Wasit University
Computer Sciences and Information Technology College

Wasit Journal
OF COMPUTER AND MATHEMATICS

A Quarterly Academic Refereed Journal
Issued by Computer Sciences and Information Technology College

Wasit Journal of computer and Mathematics

Issue 4 Volume 1

Editor by

Prof.Dr Ali Khalaf Hussain, Wasit University, Iraq

https://wjcm.uowasit.edu.iq/
Additional copies can be obtained from:
wjcm@uowasit.edu.iq
published December 2022
Printed in Iraq
Address: University of Wasit ,hay alrabee, Kut, Wasti, Iraq

Editorial Team

Table of contents

Deep Learning Based Hybrid Classifier for Analyzing Hepatitis C in Ultrasound Images

https://doi.org/10.31185/wjcm.65

Hussain k. Ibrahim(✉)
Computer Science and Information Technology, Wasit University, Iraq.
hkhudher@uowasit.edu.iq

Abstract— Although liver biopsy is the gold standard for identifying diffuse liver disorders, it is an intrusive procedure with a host of negative side effects. Physician subjectivity may affect the ultrasonography diagnosis of diffuse liver disease. As a result, there is still a clear need for an appropriate classification of liver illnesses. In this article, an unique deep classifier made up of deep convolutional neural networks (CNNs) that have already been trained is proposed to categories the liver condition. The variants of ResNet and AlexNet are a few networks that are combined with fully connected networks (FCNs). Transfer learning can be used to extract deep features that can offer adequate categorization data. Then, an FCN can depict images of the disease in its many stages, including tissue, liver hepatitis, and hepatitis. To discriminate between these liver images, three different (normal/cirrhosis, perfectly natural, and cirrhosis/hepatitis) and 3 (normal/cirrhosis/hepatitis) models were trained. A hybrid classifier is presented in order to integrate the graded odds of the classes produced by each individual classifier since two-class classifiers performed better than three-class classifiers. The class with the highest score is then chosen using a majority voting technique. The experimental results demonstrate an high accuracy when liver images were divided into three classes using ResNet50 and a hybrid classifier.

Keywords— Classifier for Hepatitis C using Hybrid Models, Deep Learning, Hepatitis C.

1 Introduction

On a worldwide basis, it has been noted that there are more fatalities from liver disease than from other serious illnesses. This is due to the fact that the most common types of jaundice do not first manifest any symptoms. Therefore, a precise prospective diagnosis for each patient is essential to creating the most personalized treatment strategy.

Cirrhosis is a disorder that worsens with time and cannot be reversed. It increases the risk of liver cancer and hepatocellular carcinoma by encouraging the growth of scar tissue in the liver (HCC). The most typical kind of primary liver cancer is HCC. Individuals who have long-term liver disorders, such as cirrhosis brought on by hepatitis B or C infection, are more likely to develop hepatocellular carcinoma [1].

2 Contribution

- On this study, a computational technique for automatically classifying diffuse liver disorders in ultrasound images is investigated
- Hepatitis, cirrhosis, and normal ultrasound liver images were distinguished using deep learning approaches.
- Classifiers for two and three classes were trained using a variety of networks, including ResNeXt, ResNets, and AlexNet.
- To increase the three-class classification's accuracy, a hybrid classifier was suggested.

3 Research Aspects

As a standard procedure, liver biopsy can occasionally advised to evaluate the liver status and assist doctors in determining the best course of therapy for patients. But in addition to being extremely costly and unpopular with patients, it is also seen to be a risky and intrusive operation [2]. Therefore, the availability of a continuous noninvasive monitoring technique, especially during the initial stages of liver disease, can save many individuals and lower their overall treatment costs.

In comparison to other imaging modalities, ultrasound offers an affordable, secure, and non-invasive imaging technique [3]. It also offers mobility and real-time capabilities. It is a global strategy that has been widely used for years in clinical settings to diagnose or engage with the treatment procedure of the illnesses among those individuals who specifically suffer from a chronic liver disease [4]. This is due to recent advancements in digital technology.

Despite the advantages already indicated, there are several limitations to ultrasound-based imaging that must be overlooked. First off, the subsequent interpretation and evaluation of the data may be influenced by the doctor's expertise with and understanding of the ultrasonography. Particularly, even a qualified person could find it challenging to visually analyse data in obese people. Second, further research is needed to compare the diagnostic capabilities of ultrasound-based imaging techniques to those of other imaging modalities, including computed tomography (CT), magnetic resonance imaging (MRI), and elastography [4].

Computer-aided diagnosis and intelligent approaches were developed to assist doctors and radiologists in making more precise and objective diagnoses in response to these difficulties.

4 Key Studies and Related Work

Key studies examining the diagnostic accuracy of ultrasound imaging for liver illness are as follows: Wavelet transform of B-scan liver images were used by Mojsilovi et al. [5] to define diffuse disorders. Using a combination of imaging characteristics,

Ogawac et al. [6] were able to determine the liver's health. Yeh et al. [7] used the support vector machine (SVM) method to classify the severity of liver fibrosis based on ultrasound images acquired in the B-mode. To distinguish between healthy liver, hepatitis, and cirrhosis, Wu Chun Ming et al. [8] used textural characteristics and a Bayes classifier, resulting in a 90.00% accuracy rate. In order to recognise ultrasound images for cirrhosis, Lei et al. [9] used the dictionary learning techniques of Local Binary Pattern (LBP), Gabor transform, and K-SVD. Classification accuracies of 93.33%, 90.00%, and 89.67% were achieved by Chen Fei et al. [10] when they retrieved statistical and fractal characteristics for normal liver, cirrhosis, and hepatoma identification. With a sensitivity of 96.00% and a specificity of 94.00%, K. Mala et al. [11] retrieved multi-resolution statistical texture characteristics using Probabilistic Neural Network (PNN) to differentiate cirrhosis from fatty liver in CT images. Our colleagues [12] proposed a scheme to classify ultrasound images of diffuse liver diseases into normal, cirrhosis, and hepatitis. The method used the Gabor wavelet transform and statistical moments to achieve a sensitivity of 85% in distinguishing normal from hepatitis liver images and 86% in distinguishing normal from cirrhosis liver images.

5 Deep Learning in Medical Analytics

Deep learning is a subfield of machine learning that has recently attracted a lot of interest due to its ability to automatically extract characteristics from unprocessed data [13]. It is possible that deep learning might be used to perform tasks like categorization, object recognition, and organ segmentation on ultrasound images [4]. The foetus [[14], [15], [16]], the heart [17], the breast [18], the prostate [19], the thyroid [20], the liver [13,21], the brain [22], the spine [23], the bone [24], the carotid [25], the intravascular [26], the lymph [27], the muscle [28], and the kidney [29] are all examples of current uses of deep learning in doppler ultrasound analysis. Several different types of deep learning network designs have been applied to medical ultrasound analysis [4], including convolutional neural networks, deep belief networks, completely convolutional networks, hybrids of numerous network architectures, recurrent neural network (rnn, and auto-encoders.

6 Research Perspectives and Methodology

The purpose of this research is to see if dynamic ultrasound images can be used to reliably classify liver state (normal, hepatitis, and cirrhosis liver) using deep learning methods. This was accomplished by training two-class (normal/cirrhosis, normal/hepatitis, and cirrhosis/hepatitis) and three-class (normal/cirrhosis/hepatitis) classifiers to differentiate between liver images. Next, a hybrid classifier is presented, which takes the weighted probabilities of the classes generated by each classifier and chooses the class with a majority voting approach.

7 Dataset for Training

Liver biopsies were utilized to identify 210 images (70 normal, 70 hepatitis, and 70 cirrhosis). The input ultrasound liver images were prepared by a radiologist with experience in this field so that the classification task could be carried out. Manual cropping and resizing of images focused on the liver was done. Before submitting the images to the network, a square window is extracted from the desired liver area to maintain resolution and aspect ratio in the lateral and axial orientations. The target region is selected so that it includes the vast majority of liver tissue. More ultrasound image instances may be acquired with the help of enhancement, as will be shown in the next sections. Some examples of classified images are displayed here

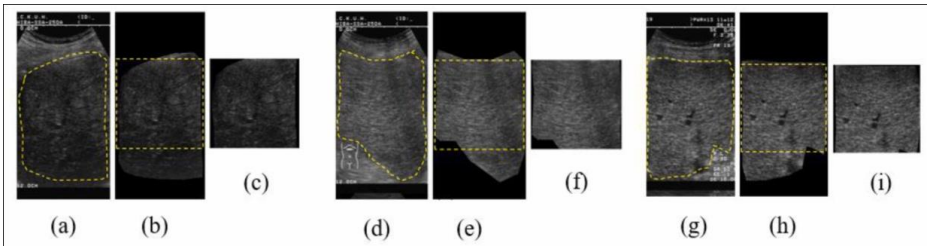


Fig. 1. Ultrasound Images for Classification and Model Building

8 Image enhancement and Augmentation

With the help of data augmentation, networks won't overfit by memorizing every nuance of the training images rather than learning to uncover the underlying patterns. The network's resilience to image data distortions is also improved by the augmentation. As an example, random rotations can be introduced to the training inputs to make the training process robust against input image rotations.

The presented work performed (1) lateral and vertical translations of 2 pixels with no padding and (2) left-right and up-down flips on each of the preprocessed images. Consequently, the original dataset now includes 1296 more images (augmented images) (consisting of 210 images).

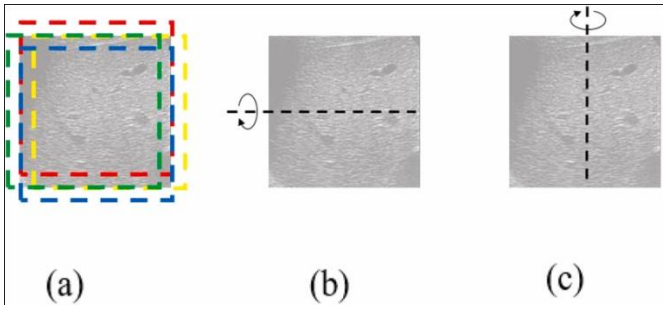


Fig. 2. Image Augmentation and Enhancement

9 Designing a neural network with a deep learning layer

The CDNN received the final modified ultrasound images detailed in the preceding sections, and the max-pooling layer down-sampled the input by splitting it into rectangular pooling areas and calculated the maximum value in each sector. The number of learnable parameters is decreased by these pooling layers, which in turn eliminates the possibility of overfitting. Next, the output consists of a single value for each ultrasound image that was used as input. Each iteration of the training process involves a both forward and backward trip across the network. The forward pass is the part of the training process when each layer uses its encoder to produce new outputs based on the preceding layer's results. Take, for example, a layer that receives X1,..., Xn from the layer below it and generates Z1,..., Zm as its outputs for the layer above it. At the end of each forward pass, the loss function L is computed between the authentic goals T and the predictions Y. In the backpropagation, each layer uses its output derivatives to calculate the input variations of the loss L with regard to its weights. The derivatives of a loss may be computed using the chain rule, which is as follows:

$$\frac{\partial L}{\partial X^{(i)}} = \sum_j \frac{\partial L}{\partial Z_j} \frac{\partial Z_j}{\partial X^{(i)}} \; i = 1, \ldots, number\ of\ inputs\ and\ j = 1, \ldots, number\ of\ outputs$$

$$\frac{\partial L}{\partial W_i} = \sum_j \frac{\partial L}{\partial Z_j} \frac{\partial Z_j}{\partial W_i} \quad i = 1, \ldots, number\ of\ learnable\ parameters\ and\ j = 1, \ldots, number\ of\ outputs$$

In convolutional deep neural networks, the Rectified Linear Unit (ReLU) layer is utilised as an activation function. Any input value that is less than zero is transformed into zero using a threshold operation. As an additional measure, a batch normalisation layer has been implemented to standardise the input of each layer throughout a mini-batch, which both accelerates training and decreases the network's sensitivity to its initialization. The iterative process of trial and error led to the selection of a learning rate of 0.0001. In the initial convolutional layers of a convolutional neural network, characteristics like colour and edges are taught to the network. By mixing the characteristics retrieved in prior convolutional layers, the network learns to recognise increasingly complex features.

10 Knowledge Transfer

It is typical practice for deep learning programmers to employ transfer learning. If a network has already been taught on one activity, it may be utilized as a foundation to learn another. For scenarios with a low number of images, training a network from start with randomly initialized weights is typically significantly slower and more complex than fine-tuning a network with transfer learning [31].

AlexNet [32], VGGNet [33], ResNet [34], and ResNeXt [35] are only few examples of pre-trained image classification networks that have learnt rich feature representations applicable to a broad variety of images. More than a million images from over a thousand item categories are used to train these networks [36,40,41-49] in the ILSVRC subset of the ImageNet database.

To facilitate transfer learning, we employed these networks. These pre-trained networks have their final layers optimized for 1000 classes. So, they need to be remolded and adjusted for the specific categorization job at hand. Figure 4 depicts the fully connected networks (FCNs) that we used to replace the last layers of these networks.

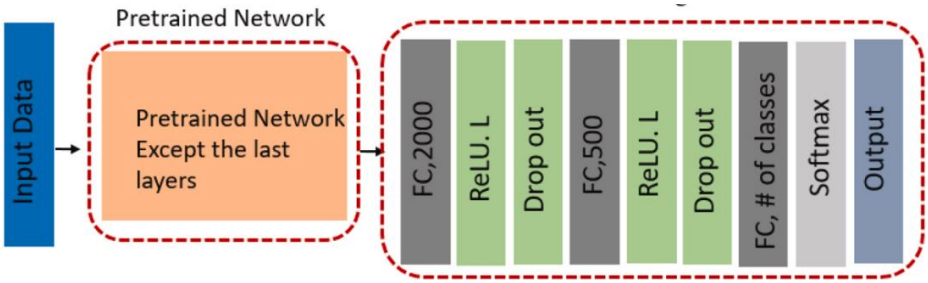


Fig. 3. Architecture of the Presented Model

11 Hybrid Classifier Based Approach

In this research, we trained four classifiers to distinguish between healthy, cirrhotic, and hepatitis-affected liver images. The first three classifications distinguished between normal and cirrhosis, normal and hepatitis, and cirrhosis and hepatitis; the last classifier separated ultrasonic liver images into these three types of liver illnesses. Based on these classifications, it is clear that two-class classifiers are superior to three-class classifiers, which do not provide enough classification power. To solve this problem, a hybrid classifier was developed [37, 38, 39] that would combine the findings of all trained classifiers by assigning different weights to the probability of the classifications that each classifier would provide. This was accomplished by using a soft - max layer in each classifier to distribute input probabilities over all classes.

A final class label was determined by averaging the weighted probabilities from all classifiers. We utilized a grid search with a step size of 0.125 to find the optimal weights for the outcome of each classifier, and then we choose the best configuration based on its classification performance. Later, the sum of all weights was divided by each ideal weight in order to standardize them.

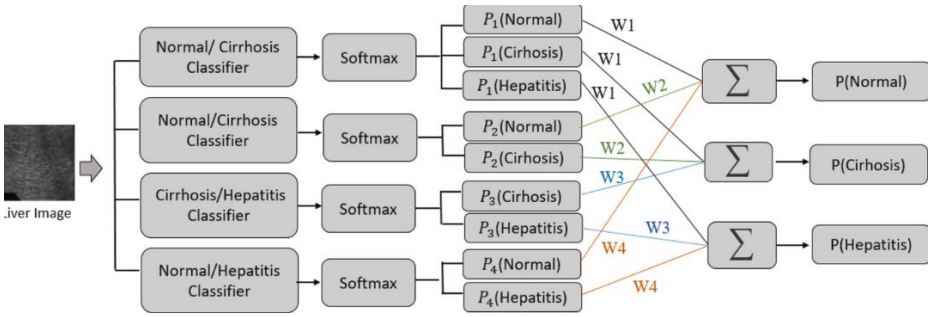


Fig. 4. Framework of the Presented Model

12 Results and Conclusiveness of Experiments

In this part, we provide the findings from a study that used dynamic ultrasound images and deep learning algorithms to evaluate the classification performance of three different liver statuses: normal, hepatitis, and cirrhosis.

A total of 216 ultrasounds were analyzed, divided evenly between three groups (normal liver ultrasound, hepatitis, and cirrhosis) based on biopsy results. We created a 70% training set and a 30% validation set at random. Using 70% of the original dataset with augmentation for training and 30% of it without augmentation for validation, ResNet50 was trained using the modified FCN. It is frequently helpful to keep tabs on the training process as we put deep learning networks through their paces. For instance, we may ascertain the rate of improvement in network accuracy and check for signs of overfitting the training data or being stuck in a local minimum.

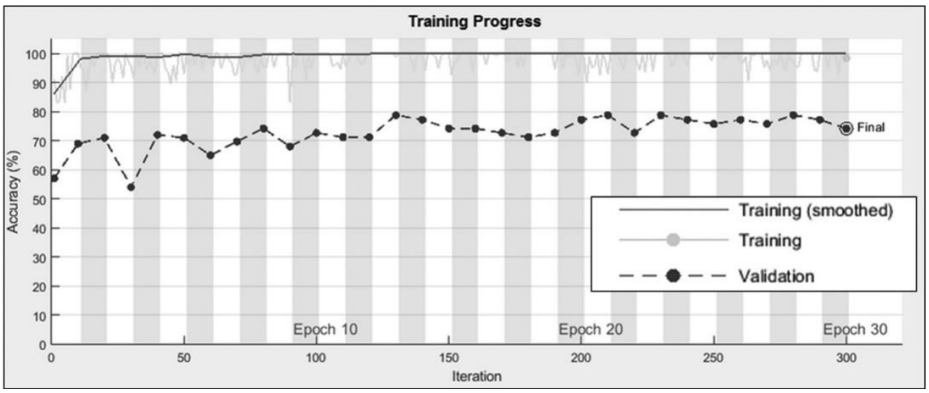


Fig. 5. Training and Validation Aspects

Accuracy of 59.09% is achieved after training the suggested CDNN from scratch for the categorization of liver images into three classes. Table 2, column 2 displays the diagnostic performance of a few well-known networks for three-class classification:

ResNet50, ResNext, ResNet18, ResNet34, and AlexNet. Table 1, column 3 displays the same diagnostic findings for two-class classifiers employing these networks. Confustion matrices for ResNet50's discrimination between normal and cirrhosis, normal and hepatitis, and cirrhosis and hepatitis are displayed in Fig. 7. Table 2 also shows the experimental outcomes of the hybrid classifier.

Table 1. Analytics of Outcomes

Models	Sensitivity	Accuracy	Specificity	Groups
Resnet50	91.6%	88.6%	86.4%	Normal (1) / Cirrhosis
	91.6%	86.4%	81.8%	Normal (1) / Hepatitis (2)
	100%	88.6%	77.2%	Cirrhosis / Hepatitis (2)
ResNext	86.4%	79.5%	72.7%	Normal (1) / Cirrhosis
	86.2%	88.6%	91.6%	Normal (1) / Hepatitis (2)
	91.6%	93.2%	95.4%	Cirrhosis / Hepatitis (2)
ResNet18	91.6%	88.6%	86.2%	Normal (1) / Cirrhosis
	77.2%	84.0%	91.6%	Normal (1) / Hepatitis (2)
	91.6%	93.2%	95.4%	Cirrhosis / Hepatitis (2)
ResNet34	81.8%	79.5%	77.2%	Normal (1) / Cirrhosis
	86.2%	86.2%	86.2%	Normal (1) / Hepatitis (2)
	77.2%	86.2%	95.4%	Cirrhosis / Hepatitis (2)
AlexNet	91.6%	84.1%	77.2%	Normal (1) / Cirrhosis
	95.5%	86.4%	77.2%	Normal (1) / Hepatitis (2)
	91.6%	84.1%	77.2%	Cirrhosis / Hepatitis (2)

However, pre-trained networks may be used as a foundation for extracting rich characteristics from liver images. The classification step may be better adapted to the job at hand via retraining the final fully-connected layers, which improves the results significantly. While the accuracy gained by using a three-class model was not satisfactory. In particular, ResNet50 outperforms its competitors in two-class classification when sensitivity requirements are taken into account.

Accuracy demonstrated by ResNeXt and ResNet18, respectively, when differentiating between cirrhosis and hepatitis. Three-class classification results showed that ResNeXt's highest achievable accuracy was less. In light of these findings and the findings for two-class classifiers, the authors settled on combining classifiers. With this goal in mind, we suggest a majority voting approach using a hybrid classifier to combine the probabilities of the predictions made by the various classifiers. Based on the outcomes, it's clear that the hybrid classifier has the potential to boost the overall precision.

Table 2. Analytics of Accuracy Levels

Model	Classical Classifier	Accuracy of Proposed Hybrid Classifier
ResNet50	76.8%	88.2%
ResNeXt	81.3%	86.5%
ResNet18	73.2%	83.8%
ResNet34	72.2%	79.3%
AlexNet	72.2%	81.3%

We conducted studies utilizing a deep neural network model to sort ultrasonic liver images into normal, hepatitis, and cirrhosis categories. The results highlight the fact

that deep features may be employed effectively for classification tasks and are replete with information. These findings suggest that a lack of sufficient data makes it impossible to successfully train a CDNN network from scratch.

Fig. 6. Training Progress and Outcomes

Segmenting the liver portions that were manually cropped as irregular polygons and feeding them into the network as binary objects ensured that they did not affect the classification results or the learning process. The network was unable to identify any significant regularities within these patterns. The use of the same dataset is necessary for a fair comparison of the classification performance to prior efforts. Because most prior research has only differentiated between normal and cirrhosis, hepatitis, or fatty liver. Quantitatively, these findings are in line with those published by Ahmadian et al. [12], who found that the cutoffs for detecting normal and cirrhosis were about 86% and 79%, respectively. They also reported results of 85% for normal and 77% for hepatitis differentiation. In comparison to their work, where a very constrained region of focus was chosen by an untrained researcher, our findings demonstrate superior categorization ability. In contrast, we employ a bigger region of tissue from liver imaging, which yields more objective and reliable results. Testing the suggested method's performance on huge datasets is essential for determining its practicality. In each matrix, the negative predictive values shown in the second row indicate how well the model can predict in typical situations. Using the model for screening rather than diagnosis is recommended due to the model's higher NPVs compared to the relevant PPVs.

13 Conclusion

The limited size of the sample is the study's biggest flaw. Better results can be achieved in future studies by utilising a big dataset and integrating deep features with textural characteristics. Effective classifiers may be built on the tiny medical datasets by fine-tuning an existing deep convolutional neural network, such as ResNeXt, ResNet18, ResNet34, ResNet50, or AlexNet. In this research, we offer a novel framework

based on a hybrid classifier for separating healthy, cirrhotic, and hepatitis-affected liver images. These liver images were used to train two-class (normal/cirrhosis, normal/hepatitis, and cirrhosis/hepatitis) and three-class (normal/cirrhosis/hepatitis) classifiers. Since two-class classifiers outperformed three-class classifiers, a hybrid classifier is developed to combine the weighted probability of the classes from each classifier. The class with the highest cumulative score is then chosen through a majority vote process. Further tweaking of the CNN and the use of a bigger dataset is required to increase performance and resilience.

14 References

[1] Liu, L., Tang, C., Li, L., Chen, P., Tan, Y., Hu, X., ... & Guo, Y. (2022). Deep learning radiomics for focal liver lesions diagnosis on long-range contrast-enhanced ultrasound and clinical factors. Quantitative Imaging in Medicine and Surgery, 12(6), 3213-3226.

[2] Li, H., Bhatt, M., Qu, Z., Zhang, S., Hartel, M. C., Khademhosseini, A., & Cloutier, G. (2022). Deep learning in ultrasound elastography imaging: A review. Medical Physics.

[3] Pasyar, P., Mahmoudi, T., Kouzehkanan, S. Z. M., Ahmadian, A., Arabalibeik, H., Soltanian, N., & Radmard, A. R. (2021). Hybrid classification of diffuse liver diseases in ultrasound images using deep convolutional neural networks. Informatics in Medicine Unlocked, 22, 100496.

[4] Li, B., Tai, D. I., Yan, K., Chen, Y. C., Huang, S. F., Hsu, T. H., ... & Harrison, A. P. (2021). Accurate and generalizable quantitative scoring of liver steatosis from ultrasound images via scalable deep learning. arXiv preprint arXiv:2110.05664.

[5] Mojsilovic, M. Popovic, S. Markovic, M. Krstic Characterization of visually similar diffuse diseases from B-scan liver images using nonseparable wavelet transform IEEE Trans Med Imag, 17 (4) (1998 Aug), pp. 541-549

[6] K. Ogawa, M. Fukushima, K. Kubota, N. Hisa Computer-aided diagnostic system for diffuse liver diseases with ultrasonography by neural networks IEEE Trans Nucl Sci, 45 (6) (1998 Dec), pp. 3069-3074

[7] W.C. Yeh, S.W. Huang, P.C. Li Liver fibrosis grade classification with B-mode ultrasound Ultrasound Med Biol, 29 (9) (2003 Sep 1), pp. 1229-1235

[8] C.M. Wu, Y.C. Chen, K.S. Hsieh Texture features for classification of ultrasonic liver images IEEE Trans Med Imag, 11 (2) (1992 Jun), pp. 141-152

[9] Y. Lei, X. Zhao, G. Wang, K. Yu, W. Guo A novel approach for cirrhosis recognition via improved LBP algorithm and dictionary learning Biomed Signal Process Contr, 38 (2017 Sep 1), pp. 281-292

[10] F. Chen Identifying ultrasonic liver image based on BP neural network Network and Information Technology, 26 (8) (2007), p. 4344

[11] K. Mala, V. Sadasivam, S. Alagappan Neural network based texture analysis of CT images for fatty and cirrhosis liver classification Appl Soft Comput, 32 (2015 Jul 1), pp. 80-86

[12] Ahmadian, A. Mostafa, M.D. Abolhassani, Y. Salimpour A texture classification method for diffused liver diseases using Gabor wavelets In2005 IEEE engineering in medicine and biology 27th annual conference, IEEE (2006 Jan 17), pp. 1567-1570

[13] D. Meng, L. Zhang, G. Cao, W. Cao, G. Zhang, B. Hu Liver fibrosis classification based on transfer learning and FCNet for ultrasound images Ieee Access, 5 (2017 Mar 30), pp. 5804-5810

[14] La Salvia, M., Secco, G., Torti, E., Florimbi, G., Guido, L., Lago, P., ... & Leporati, F. (2021). Deep learning and lung ultrasound for Covid-19 pneumonia detection and severity classification. Computers in biology and medicine, 136, 104742.

[15] Komatsu, M., Sakai, A., Komatsu, R., Matsuoka, R., Yasutomi, S., Shozu, K., ... & Hamamoto, R. (2021). Detection of cardiac structural abnormalities in fetal ultrasound videos using deep learning. Applied Sciences, 11(1), 371.

[16] Webb, J. M., Adusei, S. A., Wang, Y., Samreen, N., Adler, K., Meixner, D. D., ... & Alizad, A. (2021). Comparing deep learning-based automatic segmentation of breast masses to expert interobserver variability in ultrasound imaging. Computers in Biology and Medicine, 139, 104966.

[17] Snider, E. J., Hernandez-Torres, S. I., & Boice, E. N. (2022). An image classification deep-learning algorithm for shrapnel detection from ultrasound images. Scientific reports, 12(1), 1-12.

[18] Sun, S., Mutasa, S., Liu, M. Z., Nemer, J., Sun, M., Siddique, M., ... & Ha, R. S. (2022). Deep learning prediction of axillary lymph node status using ultrasound images. Computers in Biology and Medicine, 143, 105250.

[19] Diaz-Escobar, J., Ordóñez-Guillén, N. E., Villarreal-Reyes, S., Galaviz-Mosqueda, A., Kober, V., Rivera-Rodriguez, R., & Rizk, J. E. L. (2021). Deep-learning based detection of COVID-19 using lung ultrasound imagery. Plos one, 16(8), e0255886.

[20] Jain, P. K., Sharma, N., Giannopoulos, A. A., Saba, L., Nicolaides, A., & Suri, J. S. (2021). Hybrid deep learning segmentation models for atherosclerotic plaque in internal carotid artery B-mode ultrasound. Computers in Biology and Medicine, 136, 104721.

[21] Jain, P. K., Sharma, N., Giannopoulos, A. A., Saba, L., Nicolaides, A., & Suri, J. S. (2021). Hybrid deep learning segmentation models for atherosclerotic plaque in internal carotid artery B-mode ultrasound. Computers in Biology and Medicine, 136, 104721.

[22] Płotka, S., Klasa, A., Lisowska, A., Seliga-Siwecka, J., Lipa, M., Trzciński, T., & Sitek, A. (2022). Deep learning fetal ultrasound video model match human observers in biometric measurements. Physics in Medicine & Biology, 67(4), 045013.

[23] J. Hetherington, V. Lessoway, V. Gunka, P. Abolmaesumi, R. Rohling SLIDE: automatic spine level identification system using a deep convolutional neural network International journal of computer assisted radiology and surgery, 12 (7) (2017 Jul 1), pp. 1189-1198

[24] D. Golan, Y. Donner, C. Mansi, J. Jaremko, M. Ramachandran Fully automating Graf's method for DDH diagnosis using deep convolutional neural networks InDeep Learning and Data Labeling for Medical Applications (2016 Oct 21), pp. 130-141 [Springer, Cham]

[25] K. Lekadir, A. Galimzianova, Betriu À, M. del Mar Vila, L. Igual, D.L. Rubin, E. Fernández, P. Radeva, S. Napel A convolutional neural network for automatic characterization of plaque composition in carotid ultrasound IEEE journal of biomedical and health informatics, 21 (1) (2016 Nov 22), pp. 48-55

[26] E. Smistad, L. Løvstakken Vessel detection in ultrasound images using deep convolutional neural networks InDeep Learning and Data Labeling for Medical Applications (2016 Oct 21), pp. 30-38 [Springer, Cham]

[27] Y. Zhang, M.T. Ying, L. Yang, A.T. Ahuja, D.Z. Chen Coarse-to-fine stacked fully convolutional nets for lymph node segmentation in ultrasound images In2016 IEEE international conference on bioinformatics and biomedicine (BIBM), IEEE (2016 Dec 15), pp. 443-448

[28] P. Burlina, S. Billings, N. Joshi, J. Albayda Automated diagnosis of myositis from muscle ultrasound: exploring the use of machine learning and deep learning methods PloS One, 12 (8) (2017 Aug 30), Article e0184059

[29] Ravishankar H, Venkataramani R, Thiruvenkadam S, Sudhakar P, Vaidya V. Learning and incorporating shape models for semantic segmentation. InInternational conference on medical image computing and computer-assisted intervention 2017 sep 10 (pp. 203-211). Springer, Cham.

[30] D.P. Kingma, J. Ba Adam: a method for stochastic optimization (2014) arXiv preprint arXiv:1412.6980

[31] Y. Bengio, A. Courville, P. Vincent Representation learning: a review and new perspectives IEEE Trans Pattern Anal Mach Intell, 35 (8) (2013 Mar 7), pp. 1798-1828.

[32] H, O. Ali., N. A. Abu, and Z. Z. Abidin. "HUMAN IDENTIFICATION SYSTEM: A Review." International Journal of Computing and Business Research (IJCBR), Vol. 9. Issue 3, pp. 1-26, September 2019.

[33] Krizhevsky, I. Sutskever, G.E. Hinton Imagenet classification with deep convolutional neural networks InAdvances in neural information processing systems (2012), pp. 1097-1105

[34] K. Simonyan, A. Zisserman Very deep convolutional networks for large-scale image recognition (2014) arXiv preprint arXiv:1409.1556.

[35] Abter, S. O., Abdulhussein, A. A., Darwish, S. M., Ibrahim, Y. M., & Sheta, W. (2021). Nature-Inspired Level Set Segmentation Model for 3D-MRI Brain Tumor Detection. CMC-COMPUTERS MATERIALS & CONTINUA, 68(1), 961-981.

[36] K. He, X. Zhang, S. Ren, J. Sun Deep residual learning for image recognition IEEE conference on computer vision and pattern recognition, vol. 90, CVPR (2016)

[37] S. Xie, R. Girshick, P. Dollar, Zh Tu, K. He Aggregated residual transformations for deep neural networks. IEEE conference on computer vision and pattern recognition CVPR (2017 Nov 16)

[38] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A.C. Berg Imagenet large scale visual recognition challenge Int J Comput Vis, 115 (3) (2015 Dec 1), pp. 211-252 .

[39] Abdulhussein, Ansam A., et al. "Health monitoring catalogue based on human activity classification using machine learning." International Journal of Electrical & Computer Engineering (2088-8708) 12.4 (2022).

[40] Jena, B., Saxena, S., Nayak, G. K., Saba, L., Sharma, N., & Suri, J. S. (2021). Artificial intelligence-based hybrid deep learning models for image classification: The first narrative review. Computers in Biology and Medicine, 137, 104803.

[41] H. Al-ogaili and A. M. Shadhar, "the Finger Vein Recognition Using Deep Learning Technique," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 2, pp. 1-11, 2022.

[42] I. A. Aljazaery, J. S. Qateef, A. H. M. Alaidi, and R. a. M. Al_airaji, "Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 8, 2022.

[43] M. M. T. Al Mossawy and L. E. George, "A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System," *Wasit Journal of Computer and Mathematics Science,* vol. 1, no. 1, pp. 1-14, 2022.

[44] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022.

[45] H. Ahmed, "A Review of Hash Function Types and their Applications," *Wasit Journal of Computer and Mathematics Sciences,* vol. 1, no. 3, pp. 120-139, 2022.

[46] I. A. Aljazaery, and J. Q. Kadhim, , "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 02, 2023.
[47] B. G. Nsaif, A. H. Sallomi, and M. H. Wali, "MOBILE LOCATION PREDICTION IN CELLULAR NETWORKS by SIGNAL RECEIVED STRENGTH," *Design Engineering*, pp. 8804-8812, 2021.
[48] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," *Wasit Journal of Computer and Mathematics Sciences*, vol. 1, no. 2, pp. 12-20, 2022.
[49] Perumal, S., Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism. Wasit Journal of Computer and Mathematics Science, 2021: p. 43-51.
[50] J. Q. Kadhim, *Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT*. International Journal of Emerging Technologies in Learning (iJET), 2023. **18**(02).
[51] D. Al-Malah, H.H.K.J., *Enhancement of educational services by using the internet of things applications for talent and intelligent schools.* Periodicals of Engineering and Natural Sciences (PEN), 2020. **8**(4): p. 2358-2366.
[52] Ibrahim, H., A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 76-108.
[53] N. A. Jasim, and M.S. Farhan. Internet of Things (IoT) application in the assessment of learning process. in IOP Conference Series: Materials Science and Engineering. 2021. IOP Publishing.
[54] H.A Hassan, *Review Vehicular Ad hoc Networks Security Challenges and Future Technology*. Wasit Journal of Computer and Mathematics Science, 2022. **1**(3).
[55] S Alam, *Smart health costing system.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 70-75.
[56] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
[57] H.T. ALRikabiand , and H.T. Hazim, *Secure Chaos of 5G Wireless Communication System Based on IOT Applications.* International Journal of Online & Biomedical Engineering, 2022. **18**(12).
[58] A.S. Khairy, *The Detection of Counterfeit Banknotes Using Ensemble Learning Techniques of AdaBoost and Voting.* International Journal of Intelligent Engineering and Systems, 2021. **14**(1): p. 326-339.
[59] H. Alrikabi, H.T.H., *Enhanced Data Security of Communication System using Combined Encryption and Steganography.* International Journal of Interactive Mobile Technologies, 2021. **15**(16): p. 144-157.
[60] Akpudo, U. E., & Hur, J. W. (2021). D-dCNN: A novel hybrid deep learning-based tool for vibration-based diagnostics. Energies, 14(17), 5286.

Article submitted 15 October 2022. Published as resubmitted by the authors 17 November 2022.

Data encryption for bank management system

https://doi.org/10.31185/wjcm.83

Asst.Prof.Dr. Abdul Syukor Mohamad(✉)
Faculty of Computer Science/Universiti Teknikal Malaysia Melaka (UTEM)/Malaysia.
syuk-moh@utem.edu.my

Abstract— Data breaches are perhaps the single most significant risk that banks face today. In the financial industry. Aside from the direct costs involved in these breaches, like lost funds, increased insurance expenses and fines, and penalties, institutions also must contend with the indirect costs. Loss of reputation and consumer trust are not easy to quantitatively measure, but it's guaranteed the price is very high.

Unfortunately, banks need to face an ever-evolving set of threats because of the nature of their business. They hold sensitive financial records that bad actors are known to target, and with methods that are always shifting. Consequently, security cannot be static to meet these threats. It must be a continuous process to monitor and respond to new risks as they emerge. Also, compliance needs to be built into the overall process to meet the stringent privacy regulations for the financial industry. Data security for banks is undoubtedly a challenge, but a holistic approach may make it easier to manage.

Keywords— data encryption, bank management, database, ER.

1 Introduction

As we know the financial industry is among the most regulated in the world. There are strong data security requirements for banking and financial industries due to the sensitive and private data that they deal with.

The banking sector has been under attack for hundreds of years. First, it was the physical theft of monies. Then it was computer fraud. Today, it's not only fraud but hacks into servers to obtain a customer's personally identifiable information (PII). Hence, the reason why security in banking is of utmost importance. As individuals and companies perform most transactions computer, the risk of a data breach increases daily. This is why there's a greater emphasis to examine the importance of security in banking sector processes[1].

In today's world, banks have to think big when it comes to security. It is no longer enough to secure the system and think everything is safe. With hackers attacking major insurance companies, universities, and even the federal government, a multi-layer approach to data and system security is no longer just suggested, it's necessary[2].

Managing banking threats and monitoring data is much more complex today than it was in the past. Historically, banks only had to control access to physical paper records

by placing them in a vault and protecting their perimeter. While the digital landscape made banking much more convenient, it also opened it up to a whole host of threats. Stores of data with valuable personal information attracted the attention of cybercriminals who used a range of attacks to gain access.

Those that don't encrypt put themselves at risk for stiff government penalties, fines, lawsuits, and more.

The obvious reason for the importance of security in banking sector transactions is to protect customer assets. PII can be redirected to other locations and used for malicious activities.

Not only does this affect the customer. It also greatly harms the bank while they attempt to recover the data. When it's taken hostage, the bank might need to pay hundreds of thousands of dollars to release the information. In turn, they lose the trust of their customers and other financial institutions[3].

That's not the only thing that happens when steps for security banking aren't implemented. The customer needs to cancel all their cards and start new accounts – possibly at another bank. And though their funds are protected by the FDIC, it doesn't stop criminals from trying to use their PII[4].

2 Literature

A database is a collection of information—preferably related information and preferably organized. A database consists of the physical files you set up on a computer when installing the database software[5].

By definition, a database is a structured object. It can be a pile of papers, but most likely, in the modern world it exists on a computer system. Databases and database technology are having a major impact on the growing use of computers. It is fair to say that databases play a critical role in almost all areas where computers are used, including business, engineering, medicine, law, education, and library science, to name a few[6].

In a centralized database, all the data of an organization is stored in a single place such as a mainframe computer or a server[7]. Users in remote locations access the data through the Wide Area Network (WAN) using the application programs provided to access the data. The centralized database to the system, therefore could easily become a bottleneck. But since all the data reside in a single place it easier to maintain and back up data Furthermore, it is easier to maintain data integrity, because once data is stored in a centralized database, outdated data is no long available in other place. A centralized database is one that has all the information of the database stored in one physical location within a network[8-19].

Database design is the process of producing a detailed data model of database. This data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a data definition language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity[6] .

The process of doing database design generally consists of a number of steps which will be carried out by the database designer. Usually, the designer must :

- Determine the data to be stored in the database .
- Determine the relationships between the different data elements .
- Superimpose a logical structure upon the data on the basis of these relationship .

3 Bank database design

Database designs also include ER (entity-relationship model) diagrams. An ER diagram is a diagram that helps to design databases in an efficient way . Attributes in ER diagrams are usually modeled as an oval with the name of the attribute, linked to the entity or relationship that contains the attribute.

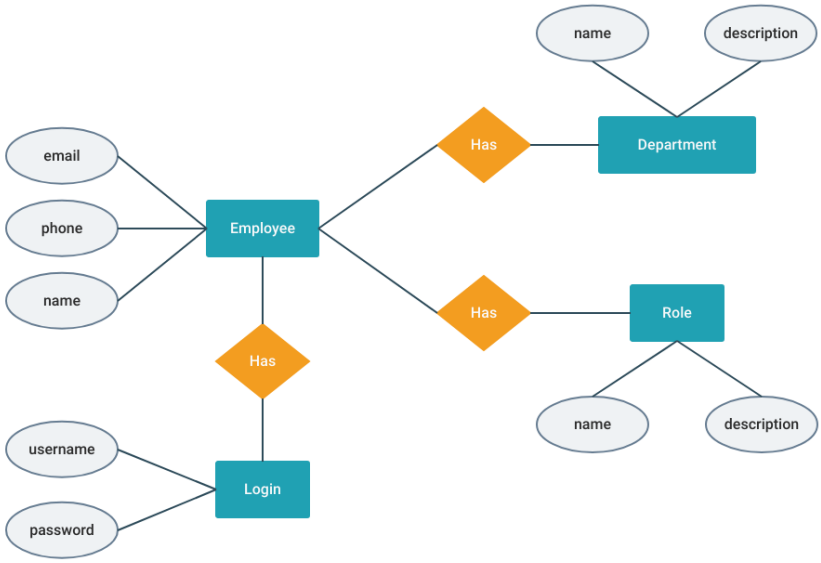


Fig. 1. bank database

4 Bank management database design

A database management system (DBMS) is a collection of programs that enables users to create and maintain databases and control all access to them. The primary goal of a DBMS is to provide an environment that is both convenient and efficient for users to retrieve 9

and store information Figure (2.2). DBMS is software designed to store and manage database to gets :-

- Data independence and efficient access .

- Reduced application development time .
- Data integrity and security .
- Uniform data administration .
- Concurrent access and recovery .

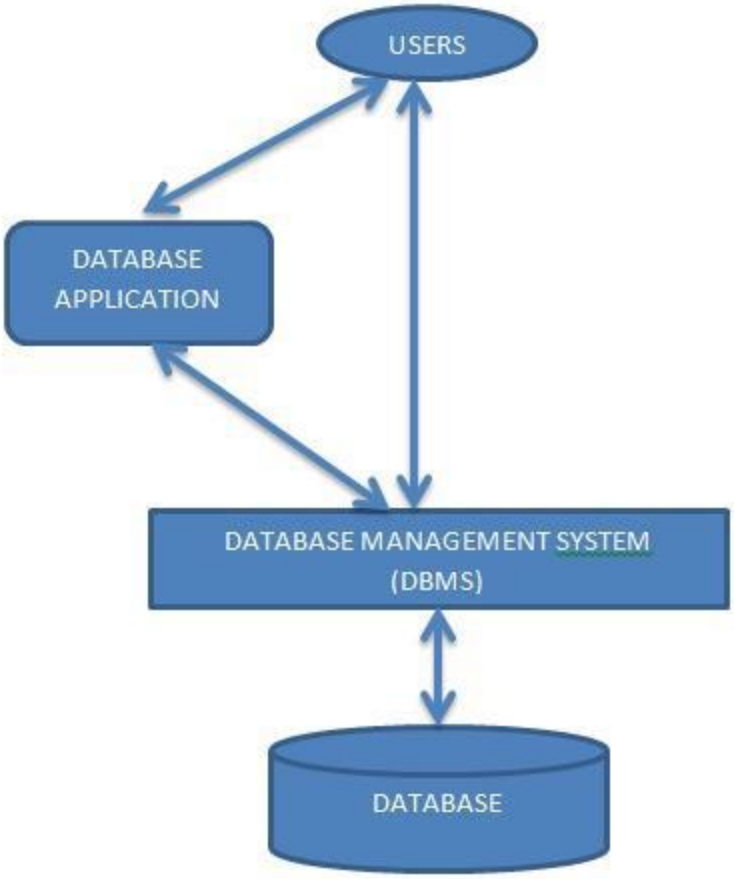
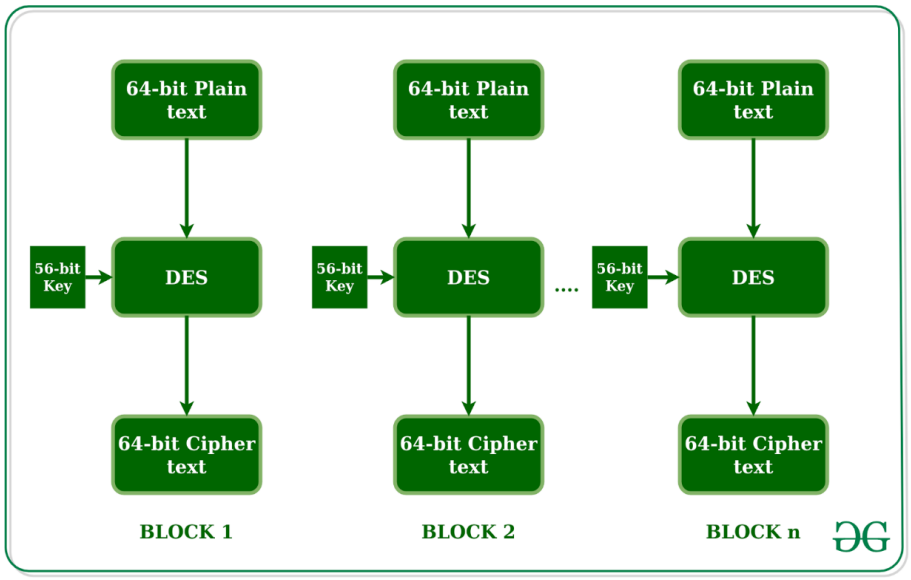


Fig. 2. bank management system

5 Data encryption standard (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The basic idea is shown in the figure



We have mentioned that DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key. DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition.

6 Bank system framework

Banking System consists of database (including several tables) and several forms connected with the tables in the database, these tables information displaying about Banking management and these entire table displaying to the admin these

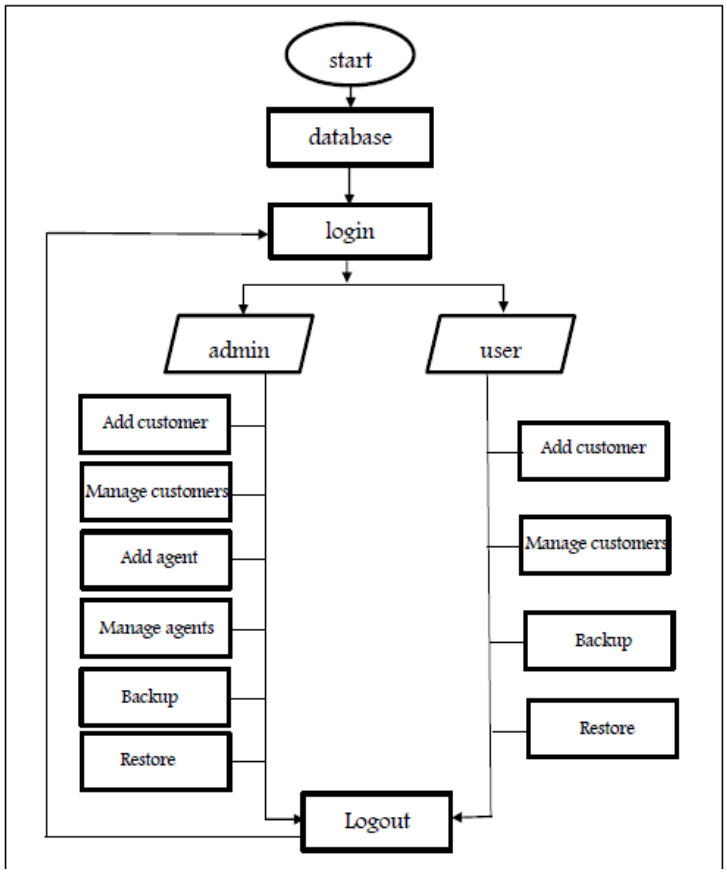


Fig. 3. bank framework

7 Conclusions

The developed system is capable of storing data and managing processes bank in bank. Encryption customers data is one of the functions of the system. The model was successfully applied by conducting an analysis of each Item, as it was part of the function of the system. The integrity and confidentiality of the customers data and passwords stored in the bank was successfully secured using DES algorithm by encrypting all the data customers and passwords in the database. Only items selected for after displayed by the data grid view will be decrypted. Main functions like adding, deleting, uploading and searching items are embedded in the system. With the developed system. Full implementation of the developed system is recommended. In order to allow for future expansion, the system has been designed in such a way that will allow possible modification as it may deem necessary by the Bank management, whenever the idea arises.

8 Reference

[1] Powell, Gavin. Beginning Database Design. s.l.: Wiley Publishing, 2006 .

[2] Connolly, Thomas .M. Database System, Design, Implementation Management. 2005 .

[3] Introduction to Database Models. TAFE NSW Sydney eLearning Moodle. https://sielearning.tafensw.edu.au

[4] Database Management System. http://slideplayer.in.th. [Online] http://slideplayer.in.th /slide/ 2049285

[5] Govind Verma ,RP Mahapatra . Database Management System 2005 .

[6] Biham, Eli and Shamir, Adi Defferential cryptanalysis of the data encryption standard, springer Verlag.

[7] Campbell, Keith W. Michael J. Wiener; DES is not a group. Crypto 1992: pp512-520.

[8] Kh-Madhloom, J., Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming. Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 21-33.

[9] Haider, .T. and H.T. Hazim, *Secure Chaos of 5G Wireless Communication System Based on IOT Applications.* International Journal of Online & Biomedical Engineering, 2022. **18**(12).

[10] Perumal, S., Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism. Wasit Journal of Computer and Mathematics Science, 2021: p. 43-51.

[11] Aljazaery, I.A., , and A.H.M. Alaidi, *Encryption of Color Image Based on DNA Strand and Exponential Factor.* International Journal of Online & Biomedical Engineering, 2022. **18**(3).

[12] Hassan, H.A., *Review Vehicular Ad hoc Networks Security Challenges and Future Technology.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(3).

[13] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.

[14] G.M.Ali .H.T.S. A Survey on The Latest FET Technology for Samsung Industry. in AIP Conference Proceedings. 2022. AIP Publishing LLC.

[15] ALRikabi, H.T., et al., *Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN.* International Journal of Interactive Mobile Technologies, 2022. **16**(8).

[16] Mohamad, R., *The Effect of Internet Marketing on External and Internal Currency of the Country.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 149-158.

[17] Hala A. Naman, N.A.H., Mohand L., *Encryption System for Hiding Information Based on Internet of Things.* International Journal of Interactive Mobile Technologies (iJIM), 2021. **15**(2).

[18] Neamah, A. F. (2020, September). Flexible Data Warehouse: Towards Building an Integrated Electronic Health Record Architecture. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1038-1042). IEEE.

[19] Diwan, S. A., Perumal, S., & Siber, D. S. (2016). Smart e-service implementation as mobile agent in a smart e-government platform. *International Journal of Applied Engineering Research*, *11*(7), 5250-5255.

Article submitted 16 November 2022. Published as resubmitted by the authors 14 December 2022.

Online translated system: DESIGN AND Implementation

https://doi.org/10.31185/wjcm.81

Prof.Dr.Sundresan perumal(✉)
Information Technology Department, Universiti Sains Islam Malaysia (USIM),Malaysia.
sundresan.perumal@usim.edu.my

Abstract— In the presence of technology and taking into account the concept of globalization, the application of chat is one of the most important aspects of our daily life to use different purposes that meet the needs of education, business and personal communication where the barrier is the language in most cases. Although we can send text using the chat app but there is still no known chat app where people can chat in different languages with the help of automatic translation system. Here the author decided to develop a mobile application with a chat and translation system in which users can chat in their preferred language for the translation system. Businessmen will help to facilitate communication with their foreign partners and students can talk to their friends abroad. It is useful to learn different languages and is useful to communicate with each other. Users only need to select the language they want to chat from the specified system. The system will use the Microsoft Translator API to translate in different languages.

Keywords— API, online translation, Microsoft translator, HTS.

1 Introduction

Chat application is a program through which messages can be transferred to a remote site or anywhere and can communicate via the Internet at the same time. Talkomatic is the first chat app developed in 1973 by Doug Brown and David R. Woolley where five users can send a message that appears on the user's screen. It was popular for the PLATO system at the University of Illinois. It is actually a transmit and receive action application with which users can interact with them. But the first online system was "chat" that was created in 1979 by Tom Walker and Fritz Thane of Dialcom [1]. Chat messages are simply short with a specific end goal to enable different members to respond quickly. Next, a tendency is created such as chat conversation, which identifies chatting from other content-based online messaging structures, for example, Internet and e-mail forums. Chat translator app is a programmed program used to convert or translate languages from one language to another. Using the translator app is to translate messages or conversations. Users copy the text from the chat application or write the text in the translator app and translate into the desired language for the user. There are thousands of languages that use people in the world but not all people are good in more than a few languages. Sometimes people need to communicate or interact with different languages that cannot be understood in all words or vocabulary. For the purpose of

being understood, unknown language users use the compiler application program. But the current chat translation process is manual. For chat translation users, they still use the copy and paste process[9]. Automatic chat translation is the federation of the chat system and the translation system. In this system, chats can be translated automatically without using copy and paste text because chat and translation systems are traditional different programs. If the user only needs to chat with another user, he can only use the chat app. If the user needs to chat and also needs to translate messages, the user needs to use both types of application but in the automatic chat application for translation the user can perform both chat and translation in the same application. Automatic conversation translation consumes more time and memory space and speeds up the process speed [2].

2 Literature Review

In the recent period, many applications for instant messaging and messaging have spread among the people, and the process of communication through e-mail between companies and between universities and between government agencies and institutions and between students and professors teaching in universities is well known, making social communication a very important thing among members of society [3]. A lot of people have used social media platforms for messaging and the issue of their social needs such as messaging, communication, and others. Recently, there have been many applications for messaging because they have become a very important thing in life and a pillar of special needs, which has facilitated our life and circumstances, and there are companies that support social communication [10-20]. And messaging programs like Telegram, Viber, Facebook with its Facebook products, WhatsApp, Instagram, and many other companies, in addition to Google, which launched the Gmail platform to send messages via e-mail, Yahoo and other important companies that contributed to the development and assistance of people's lives by facilitating their tasks [21]. However, companies in general did not provide a very important feature! However, it is the simultaneous translation of messages for a reason that everyone is ignorant of, knowing that people need this feature because it is very important in the process of understanding between people and society especially among the multilingual community. For example, there is a person in Iraq who corresponds with a person who lives in America, it is natural that the first person (Iraqi) He speaks the Arabic language, while the person who lives in (America) speaks the English language, so it is difficult for an Iraqi who speaks only one language, which is the Arabic language, to communicate the idea to the person who lives in America in the required way and this is a problem, and the person who lives in America cannot deliver the idea to The Iraqi person, simply because of the difference in language between the first parties, is fluent in English and the other is fluent in Arabic !! And from here our idea came, why don't we create a private messaging system that performs automatic translation when sending?

3 Microsoft Translator Api

Translator, part of Azure Cognitive Services, is a cloud-based machine translation service supporting more than 60 languages. Translator can be used to build applications, websites, tools, or any solution requiring multi-language support. Built for business, Translator is a proven, customizable, and scalable technology for machine translation. Translator technology powers translation features across Microsoft products, including Microsoft Translator apps for Android, iOS and Windows, Microsoft Office, Edge, SharePoint, Yammer, Visual Studio, Bing, and Skype. Simply integrate translation into web, desktop, or mobile applications, using industry standard REST technology, Translator provides a rich functionality set for any developer. Learn more about machine translation and how Translator works [4]. Translator also comes equipped with additional features to provide increased value in multilingual apps and workflows: transliteration and bilingual dictionary [5]. HTS is a web service that enables straightforward integration of Translate translation service into your corporate workflow or content manager. Your CMS calls HTS to get quotes and to place translation orders directly at our servers, exactly as a normal customer would do by clicking on our website Instant Quote widget. These translation orders will eventually be delivered back to your systems in an automatic, server to server fashion [6].
Key benefits of using HTS for your workflow are [7]:

- Cost saving: immediate reduction of administrative and management costs.
- Speed: your text is translated and posted back to your website just a few hours after the order are placed.
- Robustness: an error- free process for managing multilingual content. No more copying and pasting!
- Agility: real-time quotation and delivery planning, no more back and forth with sales to get a quote.
- You only pay for the translations you order. HTS has no setup cost and no monthly fees. Costs for human translation can be seen using our online quote.

3.1 Microsoft Translator Neural Machine Translation

Neural Machine Translation (NMT) is the new standard for high-quality AI powered machine translations. It replaces the legacy Statistical Machine Translation (SMT) technology that reached a quality plateau in the mid-2010s[8].

NMT provides better translations than SMT not only from a raw translation quality scoring standpoint but also because they will sound more fluent and human. The key reason for this fluidity is that NMT uses the full context of a sentence to translate words. SMT only took the immediate context of a few words before and after each word NMT models are at the core of the API and are not visible to end users. The only noticeable difference is improved translation quality, especially for languages such as Chinese, Japanese, and Arabic.

4 Methodology

Our project is an application that is specific to messaging between two or more people. A computer programmer. Our programming relied on the C Sharp language using the Microsoft API in the translation process, as was mentioned in previous chapters. It contains a server and a messaging application when opening in more than one device. And the connection on the server until the clients and the server are linked together so that the communication process is done in a successful way and without any mistakes, and also that the server has the process of processing that occurs in the messages sent in the language conversion if it is Arabic that converts it to the English language and then sends it to the second party Using api Microsoft or from English he converts it to Arabic then the sender if he is fluent in the Arabic language then the future must master the English language and many of the advantages

5 Conclusion

In this research of online auto translate chat system; translations were implemented using the API of Microsoft translator which avoided the formal process of copy paste using the auto translation process. This approach actively involves users to perform their chat translate smoothly which is saving the time and making easy and user friendly to communicate with different speaker with different languages. When a person is fluent in Arabic, he writes and sends the message in Arabic, and when you reach the second person who is the recipient of the message, you reach him in English, and vice versa. This is the title of our system, its details, and its beautiful idea that will benefit the community beautifully, not to mention the difficulties facing the rest of the people who have a poor translation and language, as well as this feature not found in all messaging social media programs.

6 Reference

[1] Margaret Rouse. 2007. TechTarget. [ONLINE] Available at: http://searchwindevelopment.techtarget.com/definition/C[Accessed 22 April 2017].
[2] CNET. (2017). Google Translate now serves 200 million people daily. [Online] Available at:https://www.cnet.com/news/google-translate-now-serves-200-million-people-daily/[Accessed 1 Nov. 2017].
[3] MuleSoft. (2017). what is an API? (Application Programming Interface). [Online] Available at: https://www.mulesoft.com/resources/api/what-is-an-api [Accessed 3 Nov. 2017].
[4] What is the difference between API key, S. (2017). What is the difference between API key, Secret Key and Refresh Token? - Shopify APIs & SDKs — Ecommerce University. [Online] Ecommerce.shopify.com. Available at: https://ecommerce.shopify.com/c/shopify-apisandtechnology/t/what-is-the-difference-between-api-key-secret-key-and-refresh-token221034 [Accessed 7 Nov. 2017].

[5] Architects, I., Architects, I. and Architects, I. (2017). SDLC: Seven Phases of the System Development Life Cycle. [Online] Innovativearchitects.com. Available at:https://www.innovativearchitects.com/KnowledgeCenter/basic-ITsystems/systemdevelopmentlife- cycle.aspx [Accessed 13 Nov. 2017].
[6] Anon,(2017).[Online]Availableat:1.http://www.itinfo.am/eng/softwaredevelopmentmethodologies/ [Accessed 13 Nov. 2017].
[7] [Neamah, A. F., & Salman, O. S. (2022, October). E-learning as a successful alternative: Proposing an online tests system for iraqi universities. In AIP Conference Proceedings (Vol. 2398, No. 1, p. 050034). AIP Publishing LLC.
[8] Sandrini, Peter. 2012. "Texttechnologie und Translation". In Translationswissenschaft: alte und neueArten der Translation in Theorie und Praxis/Translation Studies: old and new Types ofTranslation in Theory and Practice, ed. by Lew N. Zybatow, Alena Petrova, and MichaelUstaszewski, 21–33. Frankfurt am Main: Peter Lang.
[9] Schmitz, Klaus-Dirk, and Karl-Heinz Freigang. 2002. "Terminologieverwaltung und Sprach-datenverarbeitung". In Übersetzen und Dolmetschen, ed. by Joanna Best, and Sylvia Kalina,85–101. Tübingen: Francke Verlag.
[10] Seljan, Sanja, and Damir Pavuna. 2006a. "Why Machine-Assisted Translation (MAT) Tools forCroatian?" In Proceeding of 28th International Information Technology Interfaces Confer- ence– ITI 2006, 469–475.
[11] Kh-Madhloom, J., Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming. Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 21-33.
[12] ALRikabi, H.T. and H.T. Hazim, *Secure Chaos of 5G Wireless Communication System Based on IOT Applications.* International Journal of Online & Biomedical Engineering, 2022. **18**(12).
[13] Perumal, S., Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism. Wasit Journal of Computer and Mathematics Science, 2021: p. 43-51.
[14] Aljazaery, I.A., H.T. Salim ALRikabi, and A.H.M. Alaidi, *Encryption of Color Image Based on DNA Strand and Exponential Factor.* International Journal of Online & Biomedical Engineering, 2022. **18**(3).
[15] Hassan, H.A., *Review Vehicular Ad hoc Networks Security Challenges and Future Technology.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(3).
[16] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
[17] G.M.Ali, .H.T.S. A Survey on The Latest FET Technology for Samsung Industry. in AIP Conference Proceedings. 2022. AIP Publishing LLC.
[18] Salim, H.T., et al., *Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN.* International Journal of Interactive Mobile Technologies, 2022. **16**(8).
[19] Mohamad, R., *The Effect of Internet Marketing on External and Internal Currency of the Country.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 149-158.

[20] Jaafar Q. Kadhim, and I.A.Aljazaery, *Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT*. International Journal of Emerging Technologies in Learning (iJET), 2023. **18**(02).

[21] Seljan, Sanja, and Angelina Gašpar. 2009. "Primjena prvoditeljskih alata u EU i potreba za hrvatskimtehnologijama". In Jezična politika i jezična stvarnost, 617–625. Zagreb: Croatian AppliedLinguistics Society (PDF) The role of online translation tools in language education.Availablefrom: https://www.researchgate.net/publication/277134383_The_role_of_online_translation_tools_in_language_education [accessed Nov 13 2022].

Article submitted 16 November 2022. Published as resubmitted by the authors 17 December 2022.

An Automation system over Cloud by Using Internet of Things Applications

https://doi.org/10.31185/wjcm.88

Prof.Dr.Kevin Butler(✉)
Department of Computer Science and Information Sciences,University of Oregon,United States of America
kevin_2000@org.edu.us

Abstract— By the virtue of blooming automation industry and wireless connectivity, all the devices within the home can be connected. Today's World is moving to digitalization where everything is made easy and comfortable for people i.e., young youth as well as senior citizen. Smart Automated House Application using IOT (Internet of Thing) is a system where basic house facility can be handled by device from any place such as ON and Off of Light, Fan, AC, Water pump, Gardening of Water. One can handle all these things with help of device NodeMCU ESP8266, Android Application, Internet Connection. This paper include functionality of node esp8266 are connected with either of above given house application like fan, light, water pump, gardening with help of coding and hosting online with web server. All the functionality is handled by Mobile App created in android application, from which house application are controlled with help of internet. This paper is clarifying that monitoring of circuit devices through wireless using Node MCU and controlling using App Blynk. According to requirement of need one can connect multiple device like sensors, appliance and many more till 8.

Keywords— MCU, cloud, IOT, automation.

1 Introduction

IoT (internet of things) in recent years have become lifestyle of human being with great potential. Even it is focusing on different task that are requirement of human intelligence. In today's scenario IoT has opened doors to that cover up all requirements of human dealings in their daily life.

Example like purchasing of goods, monitoring of resources and remotely control them from any corner of the world. Think about a world were personal refrigerator will provide you list of all your stuff required for upcoming few days base on your present utilization in it. Even envisage your fridge is interactive with Home automation refers to remotely monitoring the conditions of home and performing the required actuation. Through home automation, household devices such as TV, light bulb, fan, etc. are assigned a unique address and are connected through a common home gateway. These can be remotely accessed and controlled from any PC, mobile or laptop. That can

drastically decrease energy consumption and get better the living environment as well as enhancing the indoor safety [2] [3].

Along with the quick developments in technology, the devices in the recent past are becoming smarter. The real-world appliances are being prepared with intellect and computing capability so that they can configure themselves accordingly. Sensors attached to embedded devices along with the low power wireless connectivity can facilitate to remotely monitor and control the devices. This

forms an integral component of Internet of Things (IoT) network. IoT also helps in transferring of data from sensors through wireless network, achieving recognition and informational exchange in open computing network. Things that we are using in our daily life are becoming smart with the current technologies but it isn't sufficient until we connect them to act with the dynamic environment and in addition to make their own inter-network, that is, machine-to-machine communication [4]. The Objects like electronics devices, softwares, sensors, actuators, home appliances and vehicles are connected to a wireless network.

Internet of Things is considered as a wireless network of these objects and they can exchange data through light weight protocols like MQTT, CoAP etc. There are so many types of radio modules out of which GSM, 3G, WiFi, Bluetooth, ZigBee, etc. are common. However, owing to the surging number of WiFi hotspots and range sufficient to perform the required control and monitoring, WiFi is chosen as the mode of communication in the prototype and the devices are controlled through Blynk App implemented using ESP8266 [1].

2 Literature

The ease of doing things in the most accurate, lowest cost and shortest time are what human beings have been researching since their first day on earth. The process of almost everything has been modified in a manner of which every last drop of outcome is achieved with the minimum effort possible. The technology revolution led to the information age where each activity is based on cluster of information collected via various methods. the simplest example of the importance of the role of information is shown by the fuel level reader in automobile, where change in fuel levels are sensed constantly so that drivers are aware of the fuel level all the time not mentioning the low level notification that flash on when the fuel scanted. The Information value loop as described by jonathan Holdoesky el al. [10] would describe the principle behind the fuel level example. Figure below shows the information value steps that starts with a sensor which and in according to IEEE formal definition is "a device that convert non-electrical input into electrical signal that can be sent to an electronic circuit". An action triggers the sensor that uses a network to communicate using communication standards and protocols to transmit special type of data. The information from many different sensors are aggregated by those standards and then analyzed to create an intelligent activity required upon the sensors' aggregated data [10]. Figure (2.1) shows the information value loop diagram. A 1991 definition of the "ubiquitous computing" by Mark Weiser where sensing, communicating, analyzing, and acting would be what objects of all

kinds do. The model described by Weiser was pure information value loop [10]. It is agreed that the previously mention information value loop with all stages outlined

gives the earliest identification to the Internet of things (IoT), although the term where not used until 1999 [10]. The wide spreading of the internet and the ability of connecting objects and devices of various type from different location inspired Kevin Ashton to come with an idea of connect RFID tags using the internet to decrease the human intervention in corporate supply chains [10].

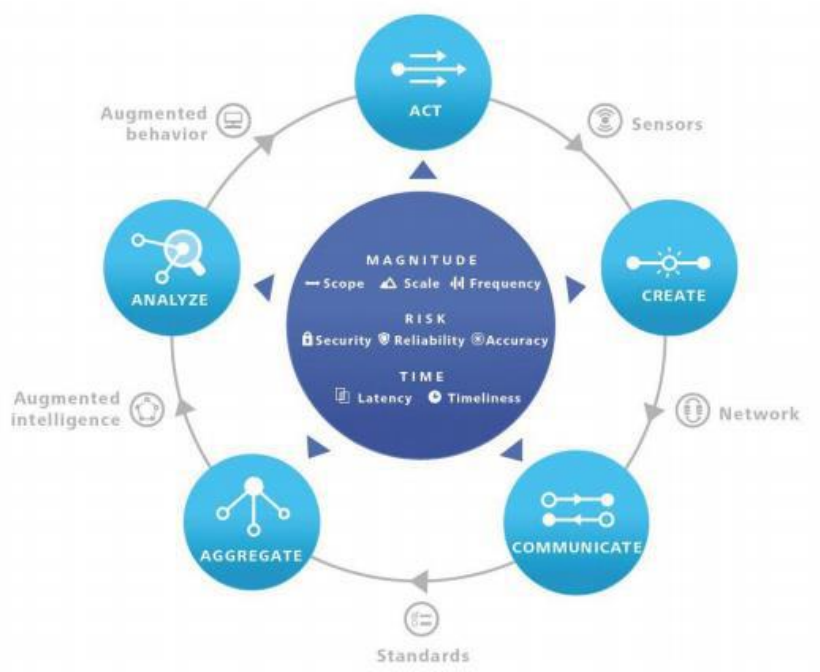


Fig. 1. information value loop diagram

IoT revolutionize the way of life in many different aspects and the technology is spreading widely over the entire world occupying almost every single detail around human being. Daily life gadgets and appliances, economic, industrial, health care, security and many other fields. Numbers of connected devices have been projected in billions within the current years. IoT connected objects will rise from 0.9 billion connected devices to nearly 26 billion devices by the 2020. Cisco figured 29 billion devices connected to the internet by the end of 2019 [13]. Figures are to be growing readily according to Morgan Stanly to reach about 75 billion devices by 2020. Yet 25 billion connections foresee by Huawei by 2025 .Surly, leveling up connected devices shall level up the global economy by about 185% by 2025 as

expected numbers shall rise up from $3.9 trillion to $11.1 trillion [1]. The numbers will hit $14.4 trillion according to Bradley, Barbier and Handler [13].

IoT influence the manufacturing and servicing industries via its impact on the availability of data related to these fields. Researches yield to a developed IoT technology, hence increased numbers of IoT connected devices as mentioned before, and this was a main reason behind firms adopting the new technology. IoT application can be classified into three main categories [13] :

1. Monitoring and Control Applications: quite wide range of exist applications fall under this category data about equipment's performance, energy using and environmental condition are to be collected and sent to either managers or automatic controllers to track the performance of different platform as per request. Smart grid is an example of a monitor and control IoT application where the collected data are used to highlight operational pattern, discover areas that need improvement, yield to the prediction of future outcome and optimize of the operation [3].

Fig. 2. smart home system applications

Verizon Home Monitoring System and control network prove to deliver property protection and energy saving for families using it. The company used special designed wireless technology to control and monitor application in home automation. Figure (2.2) shows the smart home system applications. Automobile IoT systems also classified under the same category where Ford and Intel gives the first go when special facial recognition software were used with a mobile application to personalized the user experience [13].

2. Big Data and Business Analytics: as number of connected IoT devices increases the amount of data collect shall hit a peak. The enormous amount of data collected could be used to find and correct issues in business. The collected data are transmitted what

is known as business intelligence and analytic tools where decision are made by humans. The Big data application proved customer satisfaction factors with the valuable services provided such as the health monitoring systems [11]. Many health systems have been developed to observe aggregate and analyze data related to different health conditions such diabetes and blood pressure. Health monitoring systems using wearable health sensor and back by the business analytic gather huge amount of health data of patient. IoT makes it possible to observe patient's everyday habits and health enabling caregivers to influence the patients in a better way. Elderly fall detection application is another example of this category where data from different types of sensors are collected to obtain the state of an elderly by his/her caregiver. The collected data shall give a precise prediction of the elderly state and distinguish among different pattern like, sitting, running, falling, walking and etc. [14-24].

3. Information Sharing and Collaboration: information sharing is one of the most valuable application of IoT system. The entire process starts with a predefine event sensing, and then sharing information. The sharing of information could occur in three scenarios: people sharing information other people, things sharing information to people or things sharing information to other things [14]. It comes to mind the example mentioned in the first section of this chapter where the fuel tank sensor senses the level of car fuel in the tank. Reading of the level sensor are transmitted over a known period of time to a kind of user interface. The data are shared with the main processor of the car to set the low fuel indicator once the fuel gets to its minimum accepted levels. Another example of the information sharing and collaboration applications of IoT is the one used by Macy by deploying shopkick's Shop-Beacon technology [14]. A mobile application and BLE were used as location based technology to notify customers about available deals, discount and recommendation according to their location of the market. The result of engaging such technology was clear by increasing customer engagement and promotional yields to increased revenue [14].

3 Conclusions

The home automation using Internet of Things has been experimentallyproven to work satisfactorily by connecting simple appliances to it and the applianceswere successfully controlled remotely through internet. The designed system not only monitors the sensor data, like temperature, gas, light, motion sensors,but also actuatesaprocessaccording to the requirement, for example switching on the light when it gets dark. It also stores the sensor parameters in the cloud (Gmail)in a timely manner. This will helpthe user to analyze the condition of various parameters in the home anytime anywhere

4 Reference

[1] Nodemcu, "http://www.nodemcu.com/," Nodemcu, 2017. [Online]. Available: http://www.nodemcu.com./

[2] Andi Adriansyah, Akhmad Wahyu Dani, "Design of Small Smart Home Control Systems Based on Wireless Sensor Networks and Power Line Communications," in IEEE, 2014.
[3] Kim Baraka, Marc Ghobril, Sami Malek, Rouwaida Kanj, Ayman Kayssi, " Low cost Arduino/Android-based Energy-Efficient Home Automation System with Smart Task Scheduling," in Fifth International Conference on Computational Intelligence, 2013.
[4] C. F. e. al., "The Internet of Things," in First International Conference,,
[5] D. Zeng, S. Guo, and Z. Cheng, "The Web of Things: A Survey," in *Journal of Communications*, 2011.
[6] C. F. e. a. (eds.), "The Internet of Things"," in *First International Conference, IOT*, Zurich, 20008.
[7] F. L. e. al, "Star-city: semantic traffic analytics and reasoning for city," in *Proceedings of the 19 th International Conference on Intelligent Users Interfaces*, 2014.
[8] P. B. e. al, "Citypulse: Real-time IoT Stream Processing and Largescale data analytics for smart city applicationsLarge-scale data analytics for smart city applications," in *European Semantic Web Conference*, 2014.
[9] L. S. e. al., "Smartsantander: The metting point between future internet research and experimentation and the smart cities," in *Future Network & Mobile Summit*, 2011.
[10] J. Holdowsky, M. Mahto, M. E. Raynor, M. Cooteeler, "Inside the internet of things (IoT) - A primer on the technologies building the IoT," Deloitte University Press, London, 2015.
[11] K. Rose, S. Eldridge, L. Chapin, "The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World," The Internet Society (ISOC), 2015.
[12] P. Sethi, S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, p. 25, 2016.
[13] I. Lee, K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431-440, 2015. 51
[14] S. Perumal, "Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism," Wasit Journal of Computer and Mathematics Science, pp. 43-51, 2021.
[15] J. Q. Kadhim,i, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 02, 2023.
[16] D. Al-Malah, , "Enhancement of educational services by using the internet of things applications for talent and intelligent schools," Periodicals of Engineering and Natural Sciences (PEN), vol. 8, no. 4, pp. 2358-2366, 2020.
[17] H. Ibrahim, "A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 76-108, 2022.
[18] N. A. Jasim, and M. S. Farhan, "Internet of Things (IoT) application in the assessment of learning process," in IOP Conference Series: Materials Science and Engineering, 2021, vol. 1184, no. 1: IOP Publishing, p. 012002.
[19] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," Wasit Journal of Computer and Mathematics Science, vol. 1, no. 3, 2022.
[20] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 2, pp. 12-20, 2022.
[21] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," International Journal of Interactive Mobile Technologies, vol. 16, no. 10, 2022.
[22] S. Alam, "Smart health costing system," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 70-75, 2022.

[23] S. Al-Jaff, O. Bayat, and A. H. Sallomi, "Analysis of Interference and Signal Quality in Cellular Wireless Networks," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 881, no. 1: IOP Publishing, p. 012143.
[24] K. Karimi, G. Atkinson, "What the Internet of Things (IoT) Needs to Become a Reality," Freescale Semiconductor, Inc. and ARM, Inc, 2013.

Article submitted 20 November 2022. Published as resubmitted by the authors 20 December 2022.

Lie Detection: Truth Identification from EEG Signal Using Frequency and Time Features with SVM Classifier

https://doi.org/10.31185/wjcm.78

Israa J. Mohammed(✉)
Informatics Institute for Postgraduate Studies/ Iraqi Commission for Computers & Informatics (IIPS/ICCI).
esraajalal785@gmail.com

Dr. Loay E. George
University of Information Technology and Communication.
Loayedwar57@uoitc.edu.iq

Abstract— This study investigated the approach of extracting features from single EEG channels when the minimum number of features in Electroencephalogram (EEG) channels, hence the visibility of using sets of features extracted from a single channel. The feature sets considered in previous studies are utilized to establish a combined set of features extracted from one channel. The feature is the set of statistical moments. Publicly available EEG datasets like the Dryad dataset, obtained from 15 participants, are tested into a support vector machine classifier. The 12 channels were trained separately, where each channel was divided into a different number of blocks, and the results indicated that some channels were bad. Some were very encouraging, reaching 100% in the number of blocks 16 in channels 8 and 12. In this article, the comparison of ANN algorithm test results published in a previous article with SVM algorithm test results for the same tested features and channels will be presented.

Keywords— EEG signal processing, Statistical Moments, Support vector machine.

1 Introduction

Several physiological measurements are being taken to detect a lying individual among a group of people. Heart rate [1][2], respiratory movement, blood pressure, galvanic skin response (GSR), and functional magnetic resonance imaging are some of the measures (fMRI). These approaches are vulnerable to loss, theft, or falsification.

EEG is the measurement [3] of the brain's electrical impulses produced by neuronal activation. In reaction to external environmental happenings, the human brain generates electrical potential, known as event-related potential (ERP) [4]. Unlike traditional biometrics, electroencephalogram (EEG) signals are relatively new biological features that have lately been investigated for lie detection due to their robustness against forgery and theft [5].

Different time domain features [6] and frequency domain features [7] have been utilized to investigate various aspects of EEG signals. Similarly, classification techniques

such as support vector machine (SVM) [8] and artificial neural network (ANN)[9]. There have been various proposed approaches for EEG-based lie detection. “Syed Anwar et al., 2019 [1]; have discussed employing a wearable EEG headset to detect lies using Event-Related Potential (ERP) data. Researchers explored brain activity to identify sensitive information as an alternative to the polygraph test in this study. The experiment included 14 channels and 10-20 systems in this study.

The first two principal channels produce the best findings, accounting for more than 80% of data variation. The classification method (SVM) for lie detection improves the system's accuracy using fewer EEG channels. A portable EEG recording device with a low channel commercially available EMOTIV headset is used to create an upgraded deception detection system. Frequency characteristics collected include Peak-to-Peak, Peak-to-Peak Slope, Time Window, and Amplitude and Absolute Amplitude (AAMP) (deleted the zeros). ENT and A.P., as well as several other metrics, benefit advantage vectors. The testing set was created to be as realistic as possible by using a group of kids close to each other. The system has an 83% accuracy rate. Changing the cost parameters of the SVM with a specific training sequence can give additional benefits.

“D.H. Yohan Kulasinghe, 2019 [2], has discussed using EEG technology and machine learning to detect lying. Machine learning methods that may analyze EEG data include SVM, k-Means, ANN, and Linear Classifiers. The scalp EEG is captured using the 10-20 system technology. When someone discusses a mixture of truth and lies, it may take some time, which might be beneficial. To assess EEG signals, signal amplitude, wavelength, frequency, and voltage were employed as classification model characteristics. It detected dishonesty using a frontal pole (Fp) and temporal region (T) cues. Because those areas are responsible for logical thinking, reasoning, judgment-related processes, emotional reactions, and remembering. The Fast Fourier Transform (FFT) method converts complex EEG waveforms into simple waveforms. Use the algorithm to distinguish between the truth and the falsehood. SVM performs admirably on a single data point. The approach's accuracy is 86%, according to the most convenient feature for detecting lies”.

Yijun Xiong et al., 2020 [3] compared the EEGs of the two groups during lie detection (L.D.) trials using the chaotic phase synchronization (P.S.) technique. Twenty participants' EEGs were recorded in the L.D. study using a three-stimulus approach. P.S. employed the statistical metric known as the Phase Locking Value (PLV) for a few stimuli in the L.D. investigation. A strong and larger PLV was observed in the guilty group compared to the innocent group, indicating a clear spatial and temporal difference in P.S. It was utilized to examine the interconnectedness of their frontal, temporal, central, and parietal regions to identify their tricks. The researchers did this by coordinating phase synchronization patterns across 12 EEG channels. Analyzing P.S. using the EEG data from a limited-detection L.D. experiment, we investigated the P.S. between various EEG activities recorded from different brain regions. Ten healthy college students (9 males, mean age of 22.3 years) were recruited for the study (22.3 is the average). Three unique types of stimulation were used in this method. The electrodes were arranged using the 10-20 system. In total, 14 channels were used to record horizontal and vertical EOGs. Using PLV-based characteristics, an SVM was constructed to distinguish between truthful and dishonest mental states.

However, in order to be practical, quick, and accurate, an EEG-based lie detection system needs to go through a few straightforward stages. The acquisition process should be easy and simple to avoid disturbing the user. Therefore, to reduce the system's complexity while maintaining high system accuracy, the least number of electrodes (or channels) must be linked to the user's scalp, and the minimal number of features must be checked in each channel.

In previous work, [4] discussed a method for extracting features from individual EEG channels using a minimum number of features to keep the detection system's complexity to a minimum; features were evaluated in ANN, and competitive results were obtained.

"In this work, the same approach to extracting features from EEG channels is discussed, using the same feature types proposed in previous works. This paper is organized as follows: Section 2 presents the description of used datasets and the proposed methods, Section 3 presents the description ofclassification , Section 4 discusses the experiments result, Section 5 discusses previous works related to this paper, and Section 6 presents conclusions".

2 Methodology

This study uses electroencephalogram (EEG) signals as a set of statistical features to build a lie detection system. Two approaches are adopted; the first is to extract features from a single channel (or electrode), and the second is to use the least number of features extracted from the channel. EEG-based automatic lie detection and truth-identification system apply four main stages (i.e., preprocessing, feature extraction, feature selection, and classification phase) to the input EEG. The preprocessing includes two steps, normalization, and framing. Feature extraction contains two sets of features; Spectral features and statistical moments. In feature selection, including selecting the most discriminative features. The SVM classifier is used for the classification task.

2.1 Datasets

The publicly accessible EEG Dryad dataset [4] assesses the system's performance on lie detection tasks. It is a public, free dataset that is fairly huge. It is made up of 12 EEG channels, each with 16384 samples.

2.2 Proposed System

The proposed methods in [4], which worked under the approach (using a single channel and a minimum number of features), are tested in ANN in this study under the same approach (is tested in SVM).

2.2.1 Proposed Features

Two sets of features were used for the lie detection system in the previous study; these are the Prosodic Features and statistical moments features:

2.2.2 Feature Selection

In this stage, several different feature combinations have been evaluated and compared to identify those that provide detection rates that are the highest attainable and are discussed In detail [4].

➢**Prosodic Features**

A type of measurement feature concerned with timing, articulation, duration, and zero crossing (ZCR) is the rate at which a signal changes from positive to zero to negative (ZCR) is the other way around [5] [6] used in [4]

$$\mathrm{ZCR}_{(n)} = \frac{1}{2(\mathrm{L}-1)} \sum_{\mathrm{i}=1}^{\mathrm{L}-1} |\mathrm{sgn}(\mathrm{x}_{\mathrm{i}+1}) - \mathrm{sgn}(\mathrm{x}_{\mathrm{i}})| \quad (1)$$

Where S is a signal of length and 1R<0 is an indicator function (is a function that maps elements of the subset to one and all other elements to zero).

➢**Statistical Moments Feature**

Moments refer to how much a given quantity differs from its mean or any pivot point in terms of mass, force, histogram intensity, frequency transform coefficients, and other kinds of coefficients with certain geometrical distributions [5][7].

Moments can be classified into many categories. Mathematically, moment features for a frame are calculated to characterize its behavior and extract critical features. These features are described by (1), (2),(3),(4),(5), and (6)[8][9][10][11]:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} x_i \,, \quad (2)$$

Where μ *is mean* , N denotes the total number of samples, and x_i is the sample.

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \mu)^2} \quad (3)$$

Where σ is the standard deviation, N is the total number of samples, x_i is the sample, μ is the mean.

$$Skew = \frac{\sum_{i=1}^{N} (x_i - \mu)^3}{N \sigma^3} \quad (4)$$

$$Kurt = \frac{\sum_{i=1}^{N} (x_i - \mu)^4}{N \sigma^4} \quad (5)$$

Where N is the total number of samples, xi is the sample, μ is the mean, and σ is the standard deviation.

$$\mu_5 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^5 \quad (6)$$

Where N is the total number of samples, xi is the sample, μ is the mean.

$$p = \frac{1}{N}\sum_{i=1}^{N}(|x_i|)^2 \quad (7)$$

Where P is Signal Power, N is the total number of samples, xi is the sample.

All the features mentioned above have been used in the published article [4].

2.2.3 Feature Selection

In this stage, several different feature combinations have been evaluated and compared to identify those that provide detection rates that are the highest attainable and are discussed In detail [4].

3 Classification

Classification is the process of categorizing feature extraction findings based on mental activities or supplied inputs. To obtain the desired EEG signal, it must correspond to mental tasks and motivations. The Support Vector Machine (SVM) is a popular classification technique because of its accurate results and short computing time. SVM is a classification and regression prediction algorithm [12]. SVM and ANN are both class-supervised learning methods that are comparable. SVM has been around for a long time, mixing computational techniques like margin hyperplane and kernel [10].

In the present work, the fine gaussian kernel is used with SVM. Following feature extraction, initially, data are divided into 50% and 50%. Testing data are taken as 50%. Out of the remaining 50%, training data are selected. MATLAB is used to train an SVM algorithm for the classification of detections.

SVM "is a collection of relevant supervised machine learning techniques that analyses data and identify data structures for categorization" [13]. SVM-based classification has been shown to strike the ideal balance between accuracy gained on a limited stock of training data and generalization on test data [14].

In other words, SVM "is a technique to obtain the most probable hyperplane to separate two classes" [15]. "It is done by measuring the hyperplane's margin and determining its maximum point. Margin is defined as the distance between the corresponding hyperplane and the nearest pattern from each class. Moreover, this nearest pattern is called a support vector" [16].

4 Experimental Results

This paper presents and discusses the findings of a few tests run to assess the established system's performance. The Microsoft Visual Studio 2012's C# programming language and MATLAB were used.

Dryad datasets were used to test the proposed system's accuracy with all the proposed feature extraction methods. Dryad datasets are relatively large (12 EEG channels and two EOG channels), where each set of features is extracted from a single channel. The best attained system recognition rate was 100% for some feature sets and channels for each proposed feature extraction method using all the datasets.

The training and testing results of the algorithm SVM will be displayed and compared with the results of the algorithm ANN

Table (1) This table shows the training results of some channels in the system with dataset samples tested in the SVM algorithm; it gave the best result in blocks number 16:

Table 1. The result of the train and test features in blocks number is 16 in channel 1

Table 2. The result of the train and test features in blocks number is 16 in channel 4

Channel number	Chan-nelname	Block Num	Feature number	Features set	Accuracy
1	AF3	16	7	Mean, Std, Skew, Kurt, Power, Zero, Pow5	81.2%
1	AF3	16	1	Mean	75%
1	AF3	16	1	Std	62.5%
1	AF3	16	1	Skew	56.2%
1	AF3	16	1	Kurt	62.5%
1	AF3	16	1	Power	68.8%
1	AF3	16	1	Zero	68.8%
1	AF3	16	1	Pow5	62..5%
1	AF3	16	3	Mean, Power, Zero	81.2%
1	AF3	16	2	Mean, Power	75%

Channel number	Channel name	Block Num	Feature number	Features set	Accuracy
4	FC3	16	7	**Mean, Std, Skew, Kurt, Power, Zero, Pow5**	87.5%
4	FC3	16	1	Mean	81.2%
4	FC3	16	1	Std	56.2%
4	FC3	16	1	Skew	50%
4	FC3	16	1	Kurt	56.2%
4	FC3	16	1	power	75%
4	FC3	16	1	Zero	62.5%
4	FC3	16	1	Pow5	56.2%
4	FC3	16	3	Mean, power, Zero	93.8%
4	FC3	16	2	Mean, power	75%

Table 3. The result of the train and test features in blocks number is 16 in channel 8

Channel number	Channel name	Block Num	Feature number	Features set	Accuracy
8	O2	16	7	Mean, Std, Skew, Kurt, Power, Zero, Pow5	93.8%
8	O2	16	1	Mean	100%
8	O2	16	1	Std	81.2%
8	O2	16	1	Skew	87.5%
8	O2	16	1	Kurt	75%
8	O2	16	1	power	93.8%
8	O2	16	1	Zero	68.8%
8	O2	16	1	Pow5	87.5%
8	O2	16	3	Mean, Skew, power	100%
8	O2	16	2	Mean, power	93.8%

Table 4. The result of the train and test features in blocks number is 16 in channel 9

Channel number	Channel name	Block Num	Feature number	Features set	Accuracy
9	P8	16	7	Mean, Std, Skew, Kurt, Power, Zero, Pow5	93.8%
9	P8	16	1	Mean	87.5%
9	P8	16	1	Std	75%
9	P8	16	1	Skew	68.8%
9	P8	16	1	Kurt	68.8%
9	P8	16	1	power	100
9	P8	16	1	Zero	62.5%
9	P8	16	1	Pow5	81.2%
9	P8	16	3	Mean, power, Pow5	100%
9	P8	16	2	Mean, pow5	93.8%

Table 5. The result of the train and test features in blocks number is 16 in channel 11

Channel number	Chan-nel name	Block Num	Feature number	Features set	Accuracy
11	FC6	16	7	Mean, Std, Skew, Kurt, Power, Zero, Pow5	93.8%
11	FC6	16	1	Mean	93.8%
11	FC6	16	1	Std	81.2%
11	FC6	16	1	Skew	75%
11	FC6	16	1	Kurt	81.2%
11	FC6	16	1	power	93.8%
11	FC6	16	1	Zero	100
11	FC6	16	1	Pow5	81.2%
11	FC6	16	3	Mean, power, Zero	93.8%
11	FC6	16	2	power, Zero	93.8%

Table 6. The result of the train and test features in blocks number is 16 in channel 12

Channel number	Channel name	Block Num	Feature number	Features set	Accuracy
12	F9	16	7	Mean, Std, Skew, Kurt, Power, Zero, Pow5	100%
12	F9	16	1	Mean	100%
12	F9	16	1	Std	81.2%
12	F9	16	1	Skew	93.8%
12	F9	16	1	Kurt	87.5%
12	F9	16	1	power	93.8%
12	F9	16	1	Zero	75%
12	F9	16	1	Pow5	81.2%
12	F9	16	3	Mean, Skew, power	100%
12	F9	16	2	Mean, power	93.8%

In general, the results presented in the above tables show that there are 12 channels tested separately. The test results indicate that channels 8 and 12 were the best, as their test results reached 100%, and these results are considered encouraging for using one channel.

Tables (7), (8), (9) (10) will show some of the best results of trained and tested data in the ANN algorithm discussed in the published article [4] to compare with the above results mentioned above.

Table 7. The best-attained results of training and testing samples using one feature with a blocks number are 16

Channel number	Channel name	Block number	Features number	Features set	Successful samples	Failed samples	Accuracy
11	FC6	16	1	Zero crossing	32	0	100%
11	FC6	16	1	Power	31	1	96.9%
8	O2	16	1	Mean	31	1	96.9%
9	P8	16	1	Mean& power	31	1	96.9%
12	F9	16	1	Mean	31	1	96.9%
8	O2	16	1	Power	30	2	93.8%
12	F9	16	1	Std. Dev.	30	2	93.8%

Table 8. The best-attained results of training and testing sets using two features with blocks number are 16

Channel number	Channel name	Block number	Features number	Features set	Successful samples	Failed samples	Accuracy
11	FC6	16	2	Power, Zero Crossing	32	0	100%
12	F9	16	2	Mean, Std	32	0	100%
8	O2	16	2	Mean, power	31	1	96.9%
9	P8	16	2	Mean, Power	31	1	96.9%
10	T8	16	2	Mean, Power	29	3	90.6%

Table 9. The best-attained results of training and testing samples using three features with a blocks number are 16

Channel number	Channel name	Block number	Features number	Features set	Successful samples	Failed samples	Accuracy
11	FC6	16	3	Mean, Power, Zero Crossing	32	0	100%
4	FC3	16	3	Mean, power, Zero crossing	29	3	90.6%

Table 10. The best-attained results of training and testing samples using four features with blocks number16

Channel number	Channel name	Block number	Features number	Features set	Success. samples	Failed samples	Accuracy
12	F9	16	4	Mean, StdDev, Skew, Power	32	0	100%
8	O2	16	4	Mean, power, Kurtosis, Pow5	31	1	96.9%
9	P8	16	4	Mean, Power, Kurtosis, Pow5	31	1	96.9%
10	T8	16	4	Mean, Skew, Power, pow5	30	2	93.8%

There are types in the kernel function, and several types were tried, as in the following table, and the best results were observed in the kind of function kernel in Fine Gaussian SVM.

Table 11. The best results of training and testing data in several types of kernel functions in SVM

Channel number	Channel name	Block size	Features number	Accuracy Fine Gaussian SVM	Accuracy Linear SVM	Accuracy Quadratic SVM	Accuracy Cubic SVM
8	O2	16	**7**	93.8%	93.8%	93.8%	93.8%
8	O2	16	1	93.8%	87.5%	87.5%	93.8%
8	O2	16	3	100%	93.8%	100%	87.5%
8	O2	16	1	87.5%	75%	81.2%	75%
12	F9	16	7	100%	93.8%	93.8%	93.8%
12	F9	16	1	100%	87.5%	93.8%	93.8%
12	F9	16	2	93.8%	93.8%	93.8%	93.8%
12	F9	16	3	100%	100%	100%	100%

When some of the results of the test of the algorithm SVM and the algorithm ANN were presented, it was concluded that the results of the algorithm SVM are good in the number of blocks 16. The strongest channels were 8 and 12 when compared with the results of the ANN; the results were stronger and more encouraging than the results of the SVM algorithm. The best algorithm with the data set used is the ANN algorithm.

5 Comparison with Related Works

Many published studies on EEG-based lie detection systems have shown promising results, although many utilized more than one channel or feature to detect the deceptions. Table (12) shows that this paper's results are comparable to those of other papers published on the SVM algorithm.

Table 12. Comparisons of the SVM algorithm are based on the number of channels and features employed.

Authors	No. of Channel	No. of Features	Accuracy
Syed Anwar et al., [1]	12 channels	five discriminative features are used	83%
D.H. Yohan Kulasinghe,[2]	2 Channels	four discriminative features are used	86%
Yijun Xiong et al., [3]	12 channels	Three groups of features	----
Proposed Work	Single Channel	Only one or merge (2 or 3 or 4) and all 7 Features test in some cases give	100%

6 Conclusions and Future Work

In this paper, an approach to extracting features from user EEG signals is adopted; the features proposed in previous studies are tested to check the discriminative degree of these features when tested in the SVM algorithm.

This approach has good performance in the lie detection system, but the performance of the ANN algorithm for most types of features is better than the SVM approach. This approach also keeps the computational complexity low and uses a single channel. After completing

This study showed that one or two EEG channels are enough to extract discriminate features and detect the lies when the proposed method was tested on the available datasets. A new type of statistical moment is recommended as a new feature for the EEG-lie detection system and can be tested on other data sets.

7 References

[1] S. Anwar, T. Batool, and M. Majid, “Event Related Potential (ERP) based Lie Detection using a Wearable EEG headset,” Proc. 2019 16th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2019, pp. 543–547, 2019, doi: 10.1109/IBCAST.2019.8667131.

[2] D. H. Y. Kulasinghe, “Faculty of information technology university of Moratuwa – Sri Lanka,” in Using EEG and Machine Learning to perform Lie Detection, .

[3] Y. Xiong, L. Gu, and J. Gao, “Phase synchrony and its application to lie detection,” Proc. 2020 IEEE Int. Conf. Power, Intell. Comput. Syst. ICPICS 2020, pp. 726–729, 2020, doi: 10.1109/ICPICS50287.2020.9202282.

[4] I. J. Mohammed and L. E. George, “Lie Detection and Truth Identification form EEG signals by using Frequency and Time Features,” J. Algebr. Stat., vol. 13, no. 3, pp. 4102–4121, 2022.

[5] D. Dacunha-Castelle and M. Duflo, Probability and Statistics: Volume II, vol. 2. Springer Science & Business Media, 2012.

[6] N. Zhou and L. Wang, “A modified T-test feature selection method and its application on the HapMap genotype data,” Genomics. Proteomics Bioinformatics, vol. 5, no. 3–4, pp. 242–249, 2007.

[7] S. Dodia, D. R. Edla, A. Bablani, and R. Cheruku, “Lie detection using extreme learning machine: A concealed information test based on short-time Fourier transform and binary bat optimization using a novel fitness function,” Comput. Intell., vol. 36, no. 2, pp. 637–658, 2020, doi: 10.1111/coin.12256.

[8] B. Liu, “Uncertain risk analysis and uncertain reliability analysis,” J. Uncertain Syst., vol. 4, no. 3, pp. 163–170, 2010.

[9] S. Dey, B. Al-Zahrani, and S. Basloom, “Dagum distribution: Properties and different methods of estimation,” Int. J. Stat. Probab., vol. 6, no. 2, pp. 74–92, 2017.

[10] K. P. Balanda and H. L. Macgillivray, “Kurtosis : A Critical Review,” vol. 42, no. 2, pp. 111–119, 2012.

[11] J. Cohen, “Statistical power analysis,” Curr. Dir. Psychol. Sci., vol. 1, no. 3, pp. 98–101, 1992.

[12] I. El Naqa and M. J. Murphy, “What is machine learning?,” in machine learning in radiation oncology, Springer, 2015, pp. 3–11.

[13] S. B. Maind and P. Wankar, “Research paper on basic of artificial neural network,” Int. J. Recent Innov. Trends Comput. Commun., vol. 2, no. 1, pp. 96–100, 2014.

[14] I. Steinwart and A. Christmann, Support vector machines. Springer Science & Business Media, 2008.

[15] A. Bablani, D. R. Edla, V. Kupilli, and R. Dharavath, “Lie Detection Using Fuzzy Ensemble Approach with Novel Defuzzification Method for Classification of EEG Signals,” IEEE Trans. Instrum. Meas., vol. 70, 2021, doi: 10.1109/TIM.2021.3082985.

[16] Y. Kulasinghe and D. H. Yohan Kulasinghe, “Using EEG and Machine Learning to perform Lie Detection Kinect sensor for skeleton abnormality detection View project Software Effort Estimation Model Based on Story Points for Agile Development View project Using EEG and Machine Learning to perform Lie D.” [Online]. Available: https://www.researchgate.net/publication/335095404.

Article submitted 29 October 2022. Published as resubmitted by the authors 3 December 2022.

Assorted Aspects and Implementation Patterns of Artificial Intelligence to Reduce Cyber Crimes

https://doi.org/10.31185/wjcm.86

Prof. Dr. M . Randles(✉)
School of Computing and Mathematical Sciences, Liverpool John Moores University, United kingdom.
rand-it @jmu.edu.uk

Abstract— Cyber crime was a major problem even before the epidemic, and it skyrocketed as the globe became increasingly digital after the pandemic began. It is crucial to think about how to make the web safer in the post-pandemic period, since the number of cyber scams is rising rapidly. With more people doing remote work and more people quickly embracing new technology, as well as with decreased monitoring and controls, hackers have more opportunities to attack weaknesses in the system. Individuals and businesses were rendered more vulnerable to cyber fraud as a result of each of these developments brought on by the epidemic. Since cybercriminals are just as technically savvy as their cyber security counterparts, a lot of effort and money must be spent on prevention. Professionals in the field of cyber security and cybercriminals nowadays share many of the same skills and use many of the same tools. Both cyber security experts and cybercriminals rely on them, but the former to protect their systems from the latter.

Keywords— Adoption of A.I. in Reducing Cyber Crimes, Cyber Crime, Avoidance of Cyber Crimes using A.I. Approaches.

1 Introduction

The scarcity of cyber security specialists adds to the difficulty faced by hackers. According to the ISC2 - Cyber security-Workforce-Study-2020, the global need for cyber professionals is estimated at 3 million by 2020, with 2.05 million needed in the Asia-Pacific area alone [1]. An increasing number of people throughout the globe are now able to do their jobs from home, increasing the risk of cyber assaults. Cybercriminals are a threat to businesses of all sizes and their consumers because they are continually looking for new ways to generate money. Though it's difficult to predict when and where these assaults will occur, many companies are relying on Artificial Intelligence (AI) to bolster their cyber security. We enjoy an unrestricted way of life, and the alternatives available to us in the digital sphere are almost limitless. However, the risk that our private data may be compromised due to Cyber crime is quite real [2].

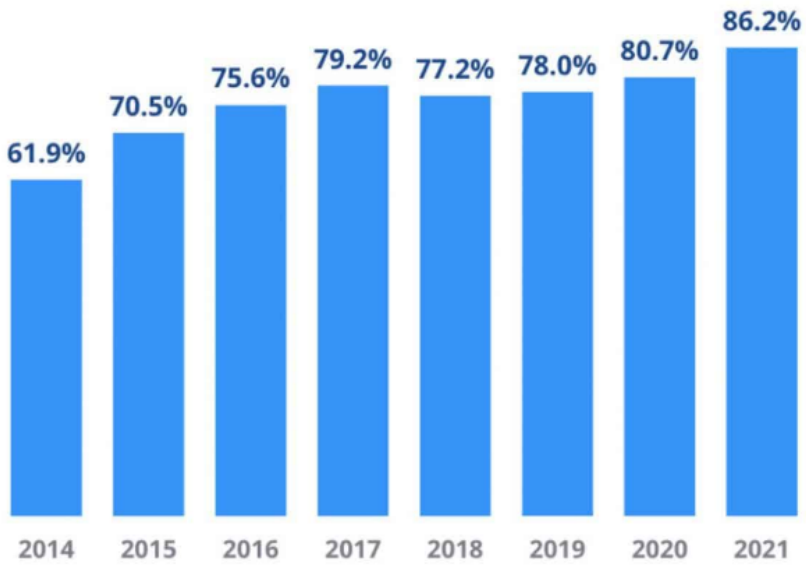


Fig. 1. Organizations compromised towards cyber attacks

The significance of cyber security has grown over the last several years. Keep in mind that cybercriminals may operate 24/7/365 from any location in the universe, and that they can use our personal information to steal our money [3, 4]. So AI and ML are becoming more and more important in the fight against Cyber crime. AI analyses patterns in data from past cyber occurrences to predict potential threats. Consequently, security officers will have more time for the tasks that really matter.

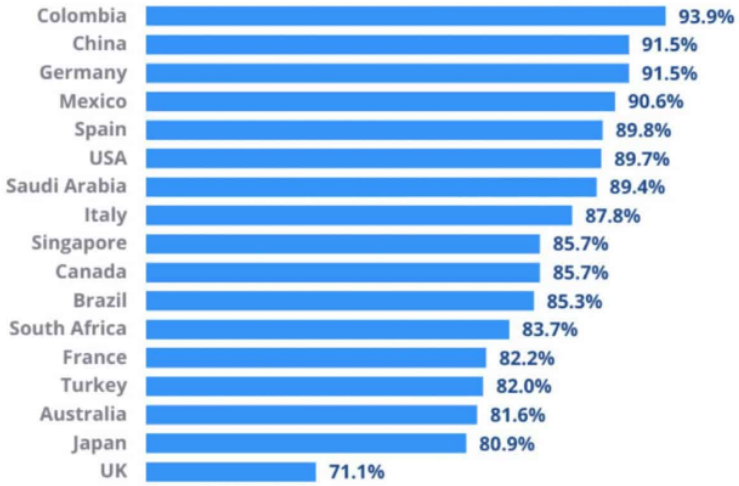


Fig. 2. Penetration Levels of Cyber Crimes in Assorted Countries

Recently, there has been a flurry of interest in using AI to improve cyber security. As was previously said, both the frequency and complexity of cyberattacks have increased. AI must be integrated with current cyber security strategies in order to provide accurate risk assessments and reduce the frequency of cyberattacks.

ZDNet reports that new security systems can identify threats like phishing schemes and new malware variants by collecting and analysing data from millions of cyber incidents [5].

There are cybercriminals that purposefully modify their malware's code so that antivirus programmes won't flag it as malicious. It's a huge challenge to find and eliminate all the many forms of malicious software. And now is the time to give thanks for artificial intelligence and machine learning systems, which provide formidable anti-malware protection.

The system may compare newly discovered malware with its database, analyse the code, and block attacks before they ever begin. This technique is effective even if the malicious code is hidden deep beneath a mountain of otherwise harmless or worthless code [6].

A monitoring system powered by AI can keep tabs on all of a user's typical activities and respond properly when it detects any out of the ordinary behaviour. To have such an edge in the present day is invaluable.

Applications aside, AI and ML are rising to prominence as key players because of their ability to prevent risks in real time without disrupting business as usual.

Data like the ever-increasing volume of communications (videos, chats, emails, etc.) may be tracked by this system even if they are not apparent to the human eye. Now that you have piqued my interest, let's examine the benefits of artificial intelligence in cyber security and see how they apply to this blog.

2 Issues Tackled by Cyber Security Tools Powered by Artificial Intelligence

All indicators of breach or exploit may be automatically analysed by AI, allowing security experts to be notified of potential threat events.

Cognitive reasoning may be used to establish connections between many types of threat entities related to real events, such as malicious entities, suspicious IP addresses, and hazardous files [7, 8].

No matter the specific implementation of AI, it's clear that technology has the potential to provide crucial insight into an incident and help a business comply and adapt.

3 Uses of Artificial Intelligence in Cyber Security

The creation of security policies and the design of the network architecture are two essential parts of network security. Traditional methods of doing these jobs took considerable time, but advancements in AI are shortening that time significantly.

This is achieved by keeping an eye on and analysing network activity and then suggesting security policies. Now that the security infrastructure is in place, experts may shift their attention to other areas of technological development [9, 10].

Up to 95% increases in detection rates are possible with the use of AI. Seeking to ascertain the source of the problem? False positives are a problem, therefore that's a yes. The best course of action here would be to combine AI with tried-and-true techniques. This integration of age-old and cutting-edge tools might increase detection rates by as much as 100 percent while also cutting down on false positives.

Danger hunting may be made better with the help of AI by including behaviour analysis. Application profiles may be developed for use inside a company's network by analysing data collected from endpoints [11].

Fig. 3. Global Market Size of A.I. in Cyber Security Market

In the field of cyber security, Cylance is among the most prominent organisations that use AI. A consumer antivirus product, Cylance Smart Antivirus, offers businesses and homes the same degree of AI security often reserved for large organizations [12].

4 Artificial intelligence and Machine Learning

Artificial intelligence and machine learning are all that is required to detect malware in legitimate data. Thus, an antivirus is developed that watches for the moment a threat is ready to be carried out and then eliminates it automatically. An enormous number of users were shielded from the Wannacry ransomware attack thanks to it.

AI and ML have the potential to enhance the vulnerability management capabilities of existing vulnerability databases. Technologies like user and event behaviour analytics (UEBA), when fueled by AI, may monitor server and endpoint activity for anomalies that might indicate an attack. Before vulnerabilities are officially publicised and remedied, this may help organisations prepare a defence [13].

Present-day internet traffic is largely generated by bots, and they could pose security risks. Account takeovers via stolen passwords, bogus account creation, and data theft are all ways in which bots could pose a serious risk.

There is no way to successfully counter automated threats with purely human responses. Understanding the distinctions between benign and malicious bots, as well as humans, in website traffic is made easier with the help of AI and machine learning.

In order to keep track of everything that has access to every system, there must be an exhaustive list of IT assets. Under the hood, an AI system aids in calculating the IT asset inventory.

Artificial intelligence (AI)-based systems can predict how and where you are most likely to be hacked, enabling you to prepare for attacks and focus your defences on the weakest points. Prescriptive insights from AI-based analysis may help you establish and fine-tune policies and processes that will increase your cyber resilience.

Artificial intelligence (AI) automates mundane cyber security tasks that may otherwise drain your staff, while also mimicking the finest qualities of humans while eliminating their shortcomings. The ability to routinely monitor for and avert even the most basic security issues is a major benefit. It also does a complete scan of your network to identify any potential security vulnerabilities.

Artificial intelligence (AI)-driven endpoint security takes a different tack, educating the endpoint to conform to a certain standard of behaviour. Artificial intelligence has the ability to recognise anomalies and respond accordingly, whether that's alerting a technician or reverting to a secure state after a ransomware attack. This allows for preventative defence against assaults, rather than reactively waiting for signature changes. You may make better prioritisation choices based on what is most likely to be utilised to attack your systems with the help of AI-based cyber security solutions, which can provide the most up-to-date information on global and industry-specific threats [14].

By 2025, the world's workforce will have lost over 85 million jobs to artificial intelligence, according to estimates. As scary as it may appear, you need not worry. There will be an additional 92.1 million employment in the world as a direct result of technological advancements, say experts. Therefore, people will need to work along with machines.

5 Negative Aspects of AI for Cyber security

One potential drawback of using AI for cyber security is the substantial investment of time, effort, and other resources required by enterprises to implement it.

In addition, hackers use AI to refine and enhance their malicious software. Malware built with artificial intelligence that can "learn" from other AI programmes is a serious threat.

Security firms need to use many data sets that include anomalies and malware codes to train the AI system. Creating reliable data sets may be a costly and time-consuming endeavour, which leaves some companies unable to do it.

Neural fuzzing is a method for finding bugs in software by testing it with massive amounts of random data. Combining neural fuzzing with neural networks allows a threat actor to learn about the target's software and its security flaws.

Cyber security firms may utilise AI to protect their customers, but the technology might also be exploited for unethical purposes. Criminals in the cyber world may utilise AI to modify their virus so that it is immune to the technology and behaves more erratically than usual.

The remedy for such flaws, After considering these drawbacks, it's evident that AI won't be the lone answer to cyber security problems anytime soon.

The most effective strategy employs a combination of both traditional methods and AI tools. Any company may improve its security by putting together a team of AI and cyber security experts that can work well together.

6 Future of Artificial Intelligence Holds for Cyber security

As more approaches to cyber resilience use AI to enable adaptive protection against dynamic threat environments, there will be a greater need for people and technology to continue to exchange knowledge and insights. CyberGraph proves that AI might be useful in the field of cyber security.

Machine learning will be included into firewalls to identify abnormalities, and artificial intelligence (AI) will be utilised to monitor security incidents.

It's possible Locating the origin of cyberattacks via the use of natural language processing (NLP) tools. In addition, RPA bots are deployed to automate rule-based processes. There is a reliance on mobile endpoints for monitoring and assessing cyber threats.

The numbers show that by the end of 2020, there will be 5.8 billion IoT-connected automobiles and business gadgets. The potential for cyber assaults increases with the number of connected devices in the Internet of Things.

Therefore, AI may be used for a variety of purposes in the field of cyber security. As cloud-based solutions grow more common, there will be a greater need for AI-powered cyber security [15-25]. With this in mind, it is projected that the value of AI cyber security will increase from $4.89 billion in 2018 to $40.61 billion in 2026, a CAGR of 30.12 percent.

7 Usage Patterns of A.I. Based Platform of OpenCV

More recent applications of computer vision and digital image processing include things like face recognition, biometric validations, the Internet of Things (IoT), criminal investigations, signature pattern detection in banking, digital document analysis, smart tag based vehicle recognition at toll plazas, and many more. All of these apps use real-time image and video processing to constantly amass a wide range of user feedback for in-depth analysis and prognostication.

Some of the many fields that benefit from HCI include: 2D and 3D image analytics; egomotion appraisal; feature points detection; human-computer interaction; facial recognition mechanism; mobile robotics; gesture control; object identification; clustering recognition; motion understanding; stereopsis scene understanding; motion tracking; structure from motion; pattern classification; augmented reality; decision making scene reconstruction; and man-machine interaction.

When it comes to computer vision jobs, nothing compares to the speed and efficiency of the open-source framework known as OpenCV. Computer vision and predictive mining are both within its capabilities because to its large set of available characteristics and algorithms. OpenCV is an AI library built by Intel; W. Garage and Itseez both use it. OpenCV was developed in response to the growing need across several sectors for efficient, real-time image analytics and recognition.

Statistical Machine Learning library used by OpenCV

- Boosting (meta-algorithm)
- Convolutional Neural Networks (CNN)
- Deep Neural Networks (DNN)
- Gradient boosting trees
- Naive Bayes classifier
- Artificial neural networks
- Random forest
- Expectation-maximization algorithm
- Decision tree learning
- k-nearest neighbor algorithm
- Support vector machine (SVM)

8 Image Forgery Analysis using OpenCV

One of the most pressing issues in the current context is determining the authenticity of user-generated content in light of the widespread usage of digital authentications across a wide range of applications. Self-attestation is becoming more commonplace, with many companies requiring applicants to provide digital versions of signed papers and certifications. This is even occurring while providing new SIM cards for mobile phones. The forgers often use digital image editing applications like Adobe PhotoShop, PaintBrush, PhotoEditors, and others to copy and paste the scanned signatures of real

people into the bogus documents. Some images may be improved by using one of the many accessible image editing software. The fresh forged copy of the document may be made using this implementation method without the target's knowledge or consent.

Here is how we see the process of identifying forged signatures in a newly created document play out.

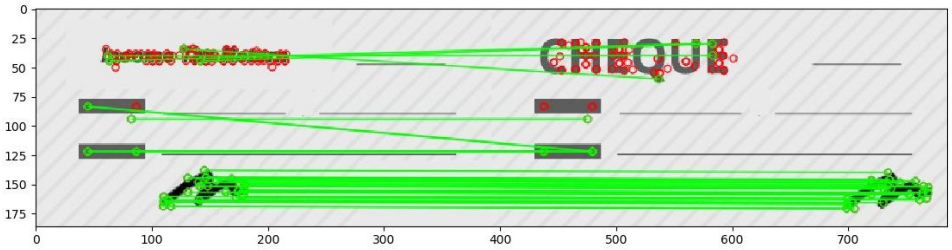


Fig. 4. Forgery Analysis using OpenCV

The pixels in the new picture with the replicated signature are easily identifiable, as shown in Figure. Methods based on machine learning and OpenCV's built-in, highly accurate prediction mechanisms are used to label pixel values. The pixels can still pinpoint the source of the picture segment, even if the individual employs sophisticated image modification techniques. We have covered the growing role of AI in cyber security, as well as how AI may aid in the fight against Cyber crimes. Implications for the future of AI in cyber security are briefly examined, as are the benefits and cons of using AI in this field.

9 Conclusion

It's become clear that AI is a reliable option for countering cyber attacks. Artificial intelligence (AI) is often used to discern "good" from "bad" in security systems. This is achieved by the comparison of one entity's behaviours with those of other entities in the same environment. More sophisticated AI security systems can analyse massive amounts of data and help piece together associated behaviours that may signify questionable activity by anonymous entities, going well beyond just detecting good or negative behaviour. Businesses are utilising models based on AI and machine learning to build up network architecture that will deter and limit Cyber crime and assaults. Artificial intelligence (AI) security features, when presented with novel or unfamiliar information/behaviors, "learn" based on previous behaviour, allowing for rapid, actionable context and insights; such as drawing logical inferences based on potentially insufficient data subsets and providing multiple solutions to a known problem, empowering security teams to select the most appropriate course of action. When conventional security solutions are proven to be too sluggish or ineffectual, artificial intelligence-based technologies are improving the entire security architecture and its performance by offering stronger protection against a growing range of complicated cyber-attacks. Companies using AI to enhance both internal and external operations have had positive

effects on business processes and financial results. Across addition, the use of AI-powered cyber security solutions has accelerated the development of data-driven security models in a variety of industries. We anticipate that artificial intelligence will soon be able to predict potential threats to cyber security systems and provide solutions to avoid them. It is also expected that countermeasures would be used extensively, giving companies peace of mind and helping them be ready for any potential cyberattacks. In addition, AI will be able to recognise sophisticated attacks, interrupt them, and prevent future efforts by hackers by establishing their identification and taking appropriate action, greatly enhancing cyber security. In addition, cutting-edge automated detection technologies will soon be available, allowing us to find attacks with a high likelihood and without the current astronomical running costs. Similarly, the arrival of automated software flaw root cause analysis — which can ascertain why a security weakness exists and how to fix it — is expected. Phishing detection neither misses a threat or issues a false alarm, and automated incident response may effectively boot an attacker from the network once they've been detected. While machine learning and artificial intelligence remain the favoured option for preventing Cyber crimes, many new breakthroughs are predicted to arise in the cyber security arena.

10 Reference

[1] MIT Technology Review, “Transforming the Energy Industry with AI”, January 21, 2021, available at: https://www.technologyreview.com/2021/01/21/1016460/transforming-the-energy-industry-with-ai/.

[2] World Health Organization (WHO), “WHO reports fivefold increase in cyberattacks, urges vigilance”, April 23, 2020, available at: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

[3] The New York Times, “Cyber Attack Suspected in German Woman’s Death”, September 18, 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

[4] Supply Chain, “Lessons Learned from the Vaccine Supply Chain Attack”, January 16, 2021, available at: https://www.supplychaindigital.com/supply-chain-risk-management/lessons-learned-vaccine-supply-chain-attack.

[5] Prakarsh and Riya Khanna, “Artificial Intelligence and Cyber crime- A curate’s Egg”, Medium, June 14, 2020, available at: https://medium.com/the-%C3%B3pinion/artificial-intelligence-and-Cyber crime-a-curates-egg-2dbaee833be1.

[6] INTSIGHTS, “The Dark Side of Latin America: Cryptocurrency, Cartels, Carding and the Rise of Cyber crime”, p.6, available at: https://wow.intsights.com/rs/071-ZWD-900/images/Dark%20Side%20of%20Latin%20America.pdf. See also, “The Next, El Chapo is Coming for your Smartphone”, June 26, 2020, available at: https://www.ozy.com/the-new-and-the-next/the-next-el-chapo-might-strike-your-smartphone-and-bank/273903/.

[7] Malwarebytes Lab, “When Artificial Intelligence goes awry: separating science fiction from fact”, without publication date, available at: https://resources.malwarebytes.com/files/2019/06/Labs-Report-AI-gone-awry.pdf.

[8] SIEMENS Energy, “Managed Detection and Response Service”, 2020, available at: https://assets.siemens-energy.com/siemens/assets/api/uuid:a95b9cd3-9f4d-4a54-8c43-77fbdb6f418f/mdr-white-paper-double-sided-200930.pdf.

[9] POLITICO, "Automated racism: How tech can entrench bias", March 2, 2021, available at: https://www.politico.eu/article/automated-racism-how-tech-can-entrench-bias/.
[10] For a discussion on discrimination caused by algorithmic decision making on AI, see ZUIDERVEEN BORGESIUS, Frederik, "Discrimination, Artificial Intelligence and Algorithmic decision making". Paper published by the Directorate General of Democracy of the Council of Europe, 2018, available at: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.
[11] See the Special Report on Facial Recognition of the Center for AI and Digital Policy (CAIDP) that contains a summary of key references on this topic contained in the 2020 Report on Artificial Intelligence and Democratic Values/ The AI Social Contract Index 2020 prepared by CAIDP, December 2020, available at: https://caidp.dukakis.org/aisci-2020/.
[12] In October 2021, the European Parliament adopted a resolution to ban the use facial recognition technologies in public spaces by law enforcement authorities to ensure the protection of fundamental rights. See European Parliament, "Use of Artificial Intelligence by the police: MEPs oppose mass surveillance". LIBE Plenary Session press release, October 6, 2021, available at: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.
[13] BBC, "What are 'bots' and how can they spread fake news, available at: https://www.bbc.co.uk/bitesize/articles/zjhg47h.
[14] FORBES, "Fake News is Rampant, Here is How Artificial Intelligence Can Help", January 21, 2021, available at: https://www.forbes.com/sites/bernardmarr/2021/01/25/fake-news-is-rampant-here-is-how-artificial-intelligence-can-help/?sh=17a6616e48e4.
[15] Kh-Madhloom, J., Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming. Wasit Journal of Computer and Mathematics Sciences, 2022. 1(2): p. 21-33.
[16] ALRikabi, H.T. and H.T. Hazim, Secure Chaos of 5G Wireless Communication System Based on IOT Applications. International Journal of Online & Biomedical Engineering, 2022. 18(12).
[17] Perumal, S., Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism. Wasit Journal of Computer and Mathematics Science, 2021: p. 43-51.
[18] Aljazaery, I.A., and A.H.M. Alaidi, Encryption of Color Image Based on DNA Strand and Exponential Factor. International Journal of Online & Biomedical Engineering, 2022. 18(3).
[19] Hassan, H.A., Review Vehicular Ad hoc Networks Security Challenges and Future Technology. Wasit Journal of Computer and Mathematics Science, 2022. 1(3).
[20] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
[21] Salim, H.T., and G.M.Ali. A Survey on The Latest FET Technology for Samsung Industry. in AIP Conference Proceedings. 2022. AIP Publishing LLC.
[22] Salim, H.T., et al., Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN. International Journal of Interactive Mobile Technologies, 2022. 16(8).
[23] Mohamad, R., The Effect of Internet Marketing on External and Internal Currency of the Country. Wasit Journal of Computer and Mathematics Sciences, 2022. 1(3): p. 149-158.
[24] Hala A. Naman, N.A.H., Mohand L. Al-dabag, Encryption System for Hiding Information Based on Internet of Things. International Journal of Interactive Mobile Technologies (iJIM), 2021. 15(2).
[25] European Commission, "Tackling online disinformation", 18 January 2021, available at: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation. For a general

review of policy implications in the UK concerning the use of AI and content moderation, see Cambridge Consultants, “Use of AI in Online Content Moderation”. 2019 Report produced on behalf of OFCOM, available at https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

Article submitted 20 November 2022. Published as resubmitted by the authors 15 December 2022.

Cheating in E-learning from the perspective of lecturers within Iraqi universities

https://doi.org/10.31185/wjcm.70

Mohammad Hasan Abd(✉)
The Students Affairs And Registration Department. University Baghdad , Iraq.
mohammed.h@uobaghdad.edu.iq

Osamah Waleed Allawi
Delta Al-Rafidain Mixed Secondary School , Baghdad,AL-Medaen Iraq.
osamah.waleed@Gmail.com

Jamal kh-madhloom
College of computer science and information technology,university of Wasit, Iraq.
Jamalkh@uowasit.edu.iq

Abstract— Online examination is an integral and vital component of online learning. Student authentication is going to be widely seen when one of these major challenges within the online assessment. This study aims to investigate potential threats to student authentication in the online examinations. Adopting cheating in E-learning in a university of Iraq brings essential security issues for e-exam . In this document, these analysts suggested a model making use of a quantitative research style to confirm the suggested aspects and create this relationship between these. The major elements that might impact universities to adopt cheating electronics were declared as Educational methods, Organizational methods, Teaching methods, Technical methods. In order to verify that the design of the questionnaire, has been followed up with two steps of verification. First of all, a approval stage within that , the list of questions examined by the section of specialists in this subject in computer technology and teaching in universities, the feedback received was implemented before proceeding in order in order to this second stage . Second of all, the pilot research has been carried out to check the dependability of the factors . The gathered data has been examined using the Cronbach's Alpha coefficient dependability test in SPSS 18 software package. This final results demonstrated this all factors are dependable as they acquired a value of 0.9126 and above inside test.

Keywords— university, e-learning, electronic exam ,e-cheating , pilot study, Cronbach's Alpha ,G Power, Iraq .

1 Introduction

E-learning and distance education have received a great attention in today's life. The key challenge in e-learning is the assessment of students in online exams. This is because, cheating in online exam is so easy. By a wide analysis on examination papers within exam cheating, we found that the main cause of test cheating is the paper and the environment which makes exam cheating possible for students . Hence online proctoring is necessary to prevent cheating in online exams .E-cheating or electronic cheating: using some form of ICT to perform academic dishonesty in or out of classrooms in order to gain unfair advantage . The benefits of E-evaluation consist of faster announcements of test results, improvement in examining assessment objectivity [1]. A lot of research is actually performed on pupils cheating actions and indicates that a university may attempt to overcome the trouble [2]. Students might select to cheat with regard to a number of psychological or cultural factors [3], like time restriction, little opportunity to be caught, a concern of failing, incompetence experience, the parent's pressure, wanting a much better score, teachers/lecturers' failure to impart information, laziness as well as indolence for the part regarding students, insufficient preparing and concern of failing... 978-1-7281-4216-6/19/$31.00 ©2019 IEEE E- Exam will be the most utilized way to assess students studying. It's several benefits[4], which includes: save printing as well as paperwork, decrease expenses, time, safeguard the environment . Additionally, this kind of assessment provides a great problem for the tutor; first, how perform we show this on the internet college students are exactly what they declare being through a test? Moreover, the way to prevent students from coming from cheating? To solve this trouble, it was suggested a recognition service platform that may confirm within real-time applicants' identities throughout the online exam. However, with regard to an e-exam the following present student's authentication in the process is usually essential[5]. Authentication could be the cosmetic foundation concerning electronic digital identity's protection. This lets to help evaluation in the event the customer could be the an individual people comments in becoming [6]. Accordingly, candidate's authentication could be the vital element inside on line assessment regulate solutions protection [7]. Authentication factors is usually labeled inside a few forms [8]: control variables (something people get hold of to be a clever card), recognizing variables (something we all assume say for example PIN NUMBER code) and biometrics (an issue we've been say for example biometric data)[9]. Sole issue authentication is in fact contingent on just a particular distinction. Nevertheless, you can use a great number of options with authentication [10] this is merged. Precisely what is identified as multiple -factor authentication like running a clever card account using connection in conjunction with some sort of PERSONAL IDENTIFICATION NUMBER code). There can be a few categories of authentication [6]: static authentication together with continuing authentication. A. Static Authentication When on this internet examination, static authentication will be done at the starting to gain access to the exam, as well as will stay valid during the session till the person closes this particular session. In this technique, for the 1st stage of security, we utilize a smart card regarding access for the assessment room [11],and also for authentication to the exam management system [12]. The solution consists of two authentication aspects ,

specifically a smart card and also a password. B. Continuous Authentication Continuous or dynamic authentication gives |one more security calculate next towards the initial authentication. It is applicable after beginning an exam session in addition to continuously inspections the student's identification (when the current student will be the identical to the one that began the exam) through the exam interval. In like a higher-risk environment (online checking platform), student's continuous authentication is extremely essential . While possession as well as knowledge authentication aspects could be stolen, borrowed or transferred into a third party. He may have exactly the same access without having the system picks up it. With this reason, those techniques aren't sufficient to verify this student's online identification. This can be a potential threat regarding an online exam [13]. Those factors are consequently vulnerable. Biometrics stays a potential solution regarding continuous authentication [14]. Because it can be depending on this natural person's confirmation and this cannot be lent or changed . III. BIOMETRICS : Biometrics may be the science regarding utilizing digital technology to recognize individuals depending on this unique physical as well as biological features of each individual [14]. Utilizing a human features may be the best method to authenticate the user[15]. In other words, the authentication aspect depending on biometrics can't be forgotten or missing contrary towards the possession and also knowledge aspects[16]. The online biometric authentication technique can be a system regarding verifying a person's identification with real time by calculating their specific features or the body's behavior [17]. Biometric devices like fingerprint readers or even eye scanning devices gather a personal biometric data as well as transform this directly into digital forms. A biometric authentication system, recognizes a person through comparing the real data to these already saved in a database utilizing algorithms [18]. A number of biometric authentication's models [19] are usually suggested some depend on physiological features for example fingerprints [20], face recognition [21] as well as iris scan [22] or even voice. As well as others provide person 's behavior aspect as the signature, the actual keyboard dynamics [23] or even mouse dynamics[24-27] . Or even a mixture of a number of characteristics within multimodal biometrics form. Generally, regardless regarding biometric indicates utilized, the rule regarding the authentication system may be the exact same: to certify this person's identification by evaluating data offered together with prerecorded ones regarding the person this claims being . Aim of the Study The aim of the study is to reduced and discover the cheating by many factors based on the lecturers s in universities within Iraq . For data collection we develop a questionnaires form for collect opinions of lecturers towards the reduced cheating electronic exam. After this. Collected data from 66 academics. The significantly of such behavior had forced institutions to employ several policies associated to cheating penalties and to use several mechanisms to detect plagiarism such as: the use of turnitin.com . The adoption of factors to reduced cheating in e-learning from the perspective of lecturers within Iraqi universities offers become one regarding the essential criteria regarding making the items required with regard to modern society. Great interest is paid to such as key |aspects for the development of an suitable developing style in different developing nations , that consequently includes understanding together with the proficiency of the use of factors to reduced e-cheating and important experiments in order to adopt them as a core component in the universities.

2 Research Model

The current study comes within the broad theoretical field. The research model proposes the adoption regarding cheating in e-learning within terms of e-exam challenges as a dependent adjustable. This may be taken the level associated with the intention which universities have got to adopt these factors to reduced e-cheating. The main factors that can affect the universities to adopt to reduced e-cheating were declared as: Educational methods, Organizational methods, Teaching methods, Technical methods. In the current study, the variables affiliated are identified based on the current review of several models and theories. After that, these parameters have conceptualized to get studied with this study. Figure1 shows the main conceptual model of this study.

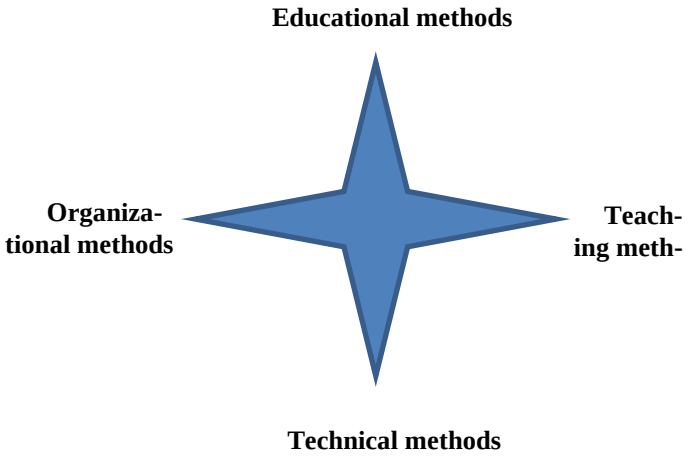


Fig. 1. The propose conceptual model

3 Material AND Method

A illustrative, study investigation style has been selected in order to research the major aspects associated in order to adopting this factors to reduced cheating in e-learning within Iraqi universities. A set of questions technique has been utilized regarding data collection within order to ascertain university staff opinions. This main cause for selecting a questionnaire returning in order to its feasibility inside simplifying this investigation from this data a lot more 'scientifically' plus objectively compared to additional types of investigation. Additionally, it might additionally assist the investigator to evaluate as well as comparison another investigation as well as might be utilized in order to calculate modify positivists think for analyzing current hypotheses (Wright, 2005). Based on this paper on Cronbach's Alpha reliability test and G Power G Power is a free, open-source program for power analysis and sample size calculations we used the method it linear multiple regression: fixed model, R^2 deviation from zero by F test Where effect size f^2 0.35, α err prob 0.05, power (1- β err prob) 0.80 for determining the total sample size.

4 Questionnaire Construction

regarding every question/item. Just about all of this items had been modified via prior research which depending on the material regarding every factor. Table 1 indicates this operationalization from this factors as well as items. Five likert scale (strongly disagree, disagree, not sure, agree, strongly agree) utilized with this research to find out the stage of agreement between the participants. Five likert scale can be one with the broadly utilized scale for supplying a clear view regarding one's proposal in certain factor. Before beginning the questionnaire, a short explanation about this investigation research as well as its objectives together with a discretion rules have got been supplied. The particular questionnaire well prepared in English as well as after this translated into Arabic, that may be this official language within Iraq .

5 Questionnaire Validation

This questionnaire validity evaluated by obtained several steps before this last submission to be able to make sure that queries /items are suitable as well as free associated with mistakes. Those types of ways involve delivering this questionnaire to six specialists within the field. These specialists are lecturers within the Iraqi universities which have experience utilizing E-learning technology. This questionnaire examined regarding language, clearness , contradiction, or even replication. Prior to the distribution, a few suggestions and remarks followed up through using suitable modifications.

6 PILOT STUDY

A variety regarding scientists suggested doing pilot research (Goodman, Meltzer, & Bailey, 1998 Smith & Studd, 1992). This goal from the pilot research would be to check the study instrument. Based on Cohen, Manion & Morrison (2013), all collected data have to be piloted within order to confirm which all questions as well as even directions are very obvious. That process enables the scientists to remove any: items which do not deliver useful data. Consequently, the perform regarding the pilot research is to create sure that the selected format regarding the study can be suitable before proceeding in order to utilize the primary tool. Therefore, the questionnaire had been allocated |between the academic staff that are using E-learning technology in different private and public universities in Baghdad-Iraq. A total of 66 replies has been obtained and that considered suitable for a pilot research as advised by (Johanson & Brooks, 2010), that announced that 66 representative members from this population of attention is a sensible minimum suggestion for pilot research . This participants' demographic foundation items are usually gender (37 males and 29 females), (2) age group (10 of these

37 years old, 26 aged 38-50 years old, 14 aged 32-35 years old, 5 aged below 32 years old , 5 aged below 29 years old ,while 6 aged over 50 years old.

7 Pilot Study Results

The most generally used check-in dependability way of measuring any kind of pilot research questionnaire will be Cronbach's Alpha (Cronbach, 1946; Sekaran & Bougie, 2010). Based on George & Mallery (2003), Cronbach's Alpha check offers values inside the selection of 0 to 1; a greater stage regarding range signifies higher value regarding dependability. Values of 0.9 as well as over are usually excellent, 0.8 as well as over are good,0.7 and over are appropriate, 0.6 and over are in question, and below 0.6 are weak. This data gathered from this pilot research happen to be examined using Statistical Package for the Social Sciences (SPSS v.18) to recognize this values of every factor in Cronbach's Alpha.

Depending on this pilot research, the test outcome demonstrated which all items are dependable since it lead in a value of about 0.9126 and over Cronbach's alpha reliability test.

Table 1: Operationalization of the factors/items and Cronbach's Alpha

Construct No.	Scale Name	CronbachAlpha value	item No.
1	Educational methods	0.887	5
2	Organizational methods	0.901	5
3	Teaching methods	0.883	8
4	Technical methods	0.931	6
5	Cheating in e-learning Adoption	0.961	14

8 Conclusion

This kind of research was suggested to examine this impacting on factors that impact this actual cheating in electronic-learning inside Iraqi universities in terms of cheating in e-exam concerns. This research was motivated through a real requirement to look at the needs, difficulties , and spaces dealing with the complete usage of e-learning technology within Iraqi universities. A questionnaire had been designed depending prior studies that check out the suggested factors. A pilot research was carried out to examine every impacting on factor as well as to check the dependability of this questionnaire. This type of study was needed to confirm this all those items will be dependable as well as free of mistakes. Cronbach's Alpha check within the pilot research discloses that all those factors get values of 0.9126 and over, which are suitable. The pilot research was performed utilizing a questionnaire that was displayed to users e-learning technology in a number of private and public universities in Iraq. A study paper follows this kind

of study to demonstrate the results from the data analysis from the main study. Future investigation will check the ideas and verify the last design .

9 Acknowledgments

We gratefully recognize all this universities and contributors in this research regarding giving us a part of their time.

10 Reference

[1] Karami, M.e.a., Advantages and Disadvantages of Electronic Assessments in Biomedical Education. IFMBE Proceedings, 2009. 25/XII:: p. p. 61-64.
[2] K. Curran, G. Middleton, et C. Doherty, « Cheating in Exams with Technology »:, International Journal of Cyber Ethics in Education, vol. 1, no 2, p. 54-62, avr. 2011.
[3] B. Keresztury et L. Cser, « New Cheating Methods in the Electronic Teaching Era », Procedia - Social and Behavioral Sciences, vol. 93, p. 1516-1520, oct. 2013.
[4] R. Bawarith, D. A. Basuhail, D. A. Fattouh, et P. D. S. GamalelDin, « E-exam Cheating Detection System », International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, n o 4, 2017.
[5] A. Ullah, H. Xiao, M. Lilley, et T. Barker, « Using Challenge Questions for Student Authentication in Online Examination », 2012
[6] P. Bours et H. Barghouthi, « Continuous Authentication using Biometric Keystroke Dynamics », p. 12, 2009.
[7] A. Moini et A. M. Madni, « Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective », IEEE Systems Journal, vol. 3, no 4, p. 469-476, déc. 2009.
[8] H. Al-Assam, H. Sellahewa, et S. Jassim, « On security of multifactor biometric authentication », in 2010 International Conference for Internet Technology and Secured Transactions, 2010, p. 1-6.
[9] I. Velásquez, A. Caro, et A. Rodríguez, « Authentication schemes and methods: A systematic literature review », Information and Software Technology, vol. 94, p. 30-37, févr. 2018.
[10] I. Velásquez, A. Caro, et A. Rodríguez, « Kontun: A Framework for recommendation of authentication schemes and methods », Information and Software Technology, vol. 96, p. 27-37, 2018.
[11] M. Ghizlane, F. H. Reda, et B. Hicham, « A Smart Card Digital Identity Check Model for University Services Access », in Proceedings of the 2Nd International Conference on Networking, Information Systems & Security, New York, NY, USA, 2019, p. 67:1–67:4.
[12] G. Moukhliss, R. F. Hilali, H. Belhadaoui, et M. Rifi, « A New Smart Cards Based Model for Securing Services », vol. 17, no 1, p. 15, 2019.
[13] K. M. Apampa, G. Wills, et D. Argles, « An approach to presence verification in summative e-assessment security », in 2010 International Conference on Information Society, 2010, p. 647-651.
[14] N. A. Mahadi, M. A. Mohamed, A. IhsanMohamad, M. Makhtar, et M. F. A. K. and M. Mamat, « A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication », Recent Advances in Cryptography and Network Security, oct. 2018.
[15] R. Saifan, A. Salem, D. Zaidan, et A. Swidan, « A Survey of behavioral authentication using keystroke dynamics: Touch screens and mobile devices », Journal of Social Sciences (COES&RJ-JSS), vol. 5, no 1, p. 29-41, 2016.

[16] P. V. Lakshmi et V. S. Susan, Biometric Authentication Using ElGamal Cryptosystem And DNA Sequence. .
[17] S. Prabhakar, S. Pankanti, et A. K. Jain, « Biometric recognition: security and privacy concerns », IEEE Security Privacy, vol. 1, no 2, p. 33-42, mars 2003.
[18] O. Enström, Authentication Using Deep Learning on User Generated Mouse Movement Images. 2019.
[19] A. C. Weaver, « Biometric authentication », Computer, vol. 39, no 2, p. 96-97, févr. 2006.
[20] « A New Fingerprint Authentication Scheme Based on SecretSplitting for Enhanced Cloud Security - Semantic Scholar ». [En ligne]. Disponible sur: https://www.semanticscholar.org/paper/ANew-Fingerprint-Authentication-Scheme-Based-on-WangKu/57f12f64a2a73cbebfc5f51014fc60075490d632.
[21] « A face recognition scheme using wavelet-based local features - IEEE Conference Publication ». Disponible sur: https://ieeexplore.ieee.org/document/5958933.
[22] « An Iris Biometric System for Public and Personal Use ». Disponible sur: https://dl.acm.org/citation.cfm?id=621411.
[23] P. Bours et S. Mondal, « Continuous Authentication with Keystroke Dynamics », in Gate to Computer Science and Research, 1st éd., vol. 2, Y. Zhong et Y. Deng, Éd. Science Gate Publishing P.C., 2015, p. 41-58.
[24] R. Asgarnezhad, S. S. A. Majeed, Z. A. Abbas, and S. S. Salman, "An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 1, pp. 27-35, 2022.
[25] R. I. Farhan, A. T. Maolood, and N. Hassan, "Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS," *Wasit Journal of Computer and Mathematics Science*, pp. 66-83, 2021.
[26] R. a. M. Al_airaji, I. A. Aljazaery, and A. H. M. Alaidi, "Automated Cheating Detection based on Video Surveillance in the Examination Classes," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 8, 2022.
[27] C. Shen, Z. Cai, X. Guan, Y. Du, et R. A. Maxion, « User Authentication Through Mouse Dynamics », IEEE Transactions on Information Forensics and Security, vol. 8, p. 16-30, 2013.

Article submitted 18 October 2022. Published as resubmitted by the authors 20 November 2022.

Questionnaire Survey

cheating in E-learning from the perspective of lecturers within Iraqi universities : PILOT STUDY

Dear Respondent

You are invited to participate in research being conducted for an academic purpose. This research aims at showing the concerns and challenges of the adoption of reduced and discover cheating in e-learning technology to develop an adoption model in Iraqi universities.

I will be obliged if you co-operate with me in completing the questionnaire. It will take approximately 20 minutes to complete the survey.

If you have any question or concern regarding this study, please feel free to contact me via mobile: (07736003453), E-mail: osamah.waleed@gmail.com or mohammed.h@uobaghdad.edu.iq .

Since the questionnaire is being used for academic purposes, the information gathered will be strictly confidential.

Thank you for your participation in this study. Your contribution is greatly appreciated.

I. Factors affecting lecturers' likelihood of Cheating in E-learning

Part I

This section collects anonymous demographic information pertaining to you. Please tick the most appropriate answer.

Kindly tick (√) as appropriate

Personal Details	
1. Gender □ Male □ Female	**2. Qualification:** □ Master □ PHD □ Others
3. Age Group □ Below 30 years □ From 31 to 40 □ From 41 to 50 □ Above 50	**4.Subject major (area of study)** □ Business □ Accounts and Finance □ Humanities □ Education □ Engineering □ Math and Science □ Others

5.Average class size (Select the box which describes the average size of the lectures you give it)	**6. Years of Experience**
□ Below 20 % □ 21 – 40 % □ 41 – 60 % □ 61 – 80 % □ 81 –100 %	□ Less than 1 year □ 1-3 years □ 4-7 years □ 8-11 years □ Over 12 years

7.In the lectures that I give it , a typical class size would be.

□ Below 20 %
□ 21 – 40 %
□ 41 – 60 %
□ 61 – 80 %
□ 81 –100 %

Academic cheating in e-learning

(The act of cases the cheating in e-learning) for each statement, indicate the extent of your agreement or disagreement based on your personal knowledge of cheating in e-learning .

In-dex	**Academic cheating cases**	**Strongly Disa-gree**	**Disa-gree**	**Neu-tral**	**Agree**	**Strongly Agree**
1	The exchange of homework and academic requirements between students electroni-cally.					
2	Quoting homework and study requirements from the Inter-net without specifying Source .					
3	Students interacted with indi-viduals or institutions via the Internet to make academic re-quirements					
4	Falsification of electronic ac-ademic documents					
5	Falsification of training cer-tificates to reduce university requirements					
6	A person to take an electronic test for a student					

7	Switching data and statistical treatments using statistical verification software					
8	Students penetrate the academic system to change grades					
9	Fill out academic forms with dishonest information					
10	Copy phrases from the Internet and put them side by side without the additions of the student.					
11	Use electronic tools (cameras, mobile phones and recording tools) at the time of the test					
12	Using technology or individuals while performing remote tests					
13	Using computer software to modify drawings and shapes and their proportions for student work					
14	One of the students snooped on his colleagues' electronic devices, and stole academic activities.					

Index	**Methods of facing academic cheating in e-learning (Educational Methods)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Developing religious discipline that contributes to distancing students from cheating					
2	Holding seminars and conferences to raise awareness and educate the regulations on the use of information technology					
3	Editing an academic ethical code that students adhere to					
4	Identify cases of fraud in the e-learning environment					

5	Announcing cases of fraud and the type of punishment on the websites without mentioning names					
Index	**Methods of facing academic cheating in e-learning(Organizational Methods)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Enforce anti-cheating policies and laws that are flexible and in line with technical changes					
2	Create a committee to follow up on academic cheating in the educational institution to present studies and proposals					
3	Determine the penal procedures for perpetrators of academic cheating in the e-learning environment					
4	Coordination between the concerned authorities of information technology at the universities level to prevent academic cheating					
5	A concerted effort and coordination among the community organizational institutions to achieve the prevention of electronic cheating					
Index	**Methods of facing academic cheating in e-learning(Teaching Methods)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Diversification of assignments, requirements and academic tests .					
2	Using student groups to do homework and study requirements .					
3	Renewal in the work of homework, requirements and academic tests .					
4	Use one calendar for students to be face to face .					
5	Connecting assessments to students ’personal experiences .					

6	The evaluation focuses on the learning process rather than the average .					
7	confirmation On specifying the sources in the academic requirements .					
8	Use a continuous evaluation based on description instead of giving value.					
Index	**Methods of facing academic cheating in e-learning(Technical Methods)**	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
1	Providing electronic systems to avoid cheating like Integrity EXAM content is DIGITALLY signed.					
2	The use of software that reveals students who practice cheating .					
3	Renewal and development in electronic learning systems.					
4	Keep all student electronic operations Encryption of stored exam content What enciphering/deciphering .					
5	Establish a technical support unit that will be in contact with the course professor to assist him .					
6	Provide anti-theft software for students Intrusion detection mechanism implemented in system to detect privilege escalation .					

registration information about the authors

Full name	**Science degree**	**Department**	**University**	**Address University**	**E-mail**	**Number of ORCID**
Mohammed Hassan Abd[1*]	Master in Computer Science	The Students Affairs And Registration Department	University Baghdad, Iraq	Iraq Baghdad,karrada	mohammed.h@uobaghdad.edu.iq	https://orcid.org/0000-0002-9294-6383

Osamah Waleed Al-lawi[*2]	Master in Computer Science	Delta Al-Rafidain Mixed Secondary School	Ministry of Education ,Iraq	Baghdad,AL-Medaen Iraq	osamah.waleed@Gmail.com	
Jamal khmadhloom[*3]	PhD in Information Technology	Computer Science	Wasit University	Wasit	[*3]Jamalkh@uowasit.edu.iq	

Thank you for your co-operation!

A Critical Review of Optimization MANET Routing Protocols

https://doi.org/10.31185/wjcm.94

Riyadh Rahef Nuiaa (✉)
College of Education for Pure Sciences, Wasit University, Iraq
riyadh@uowasit.edu.iq

Ali Hakem Alsaeedi
College of Computer Science and Information Technology, University of Al-Qadisiyah, Iraq
ali.alsaeedi@qu.edu.iq

Salam Saad Alkafagi
[3]Babylon Education Directorate, Ministry of Education, Babil, Iraq
salam.s.alkafagi@gmail.com

Ali Saeed D. Alfoudi
College of Computer Science and Information Technology, University of Al-Qadisiyah, Iraq
a.s.alfoudi@qu.edu.iq

Abstract—The main challenges in routing protocols are node mobility, resource constraints, error-prone channel states, and problems with hidden and unprotected terminals. This article provides an overview of the main protocols, their problems, and ways to improve them. The cell phone allows communication between two moving units via mobile stations (MS), mobile units, and landing units. The term "mobile ad hoc network" (MANET) refers to a group of devices connecting and communicating. The military, law enforcement, and emergency services have quickly become interested in MANETS because they provide a high quality of service. Path loss (PL), one of the biggest problems in wireless communications, can be caused by multiple reflections from an obstacle or by the source of the signal being far from the destination on the network. Multipath propagation, path loss, and interference reduce the network's quality of service (QoS). The best route is added to a router's routing table using a dynamic routing protocol, and an alternate path is chosen when the primary route is unavailable.

Keywords— Routing protocols, Optimization Network, Metaheuristics Optimization, Path loss, quality of service.

1 Introduction

The use of wireless media and radio transmission for data and voice communication inside a particular mobile network is known as mobile networks [1]. Devices made with purpose, portable, and relatively lightweight are typically referred to as "mobile.". The cell phone connects two moving units through Mobile Stations (MSs), Mobile Units,

and land units[2]. The mobile service provider has to supply three major services: locate and track the caller, assign the talking channel, and transfer the channel across base stations as the mobile moves.[3]–[5].

To enable localization, the cellular service area is divided into cells. The size of the cells depends on the population of the coverage areas. The cell center is computerized and responsible for the calls: (connecting, recording, billing) and the typical cell range (1.6 - 19.3) km[6]. Therefore, in an area with a high population density, smaller cells are required to meet traffic demands, and the transmit power of the cells must be low to avoid overlapping[7]. Figure 1 illustrates the cellular network.

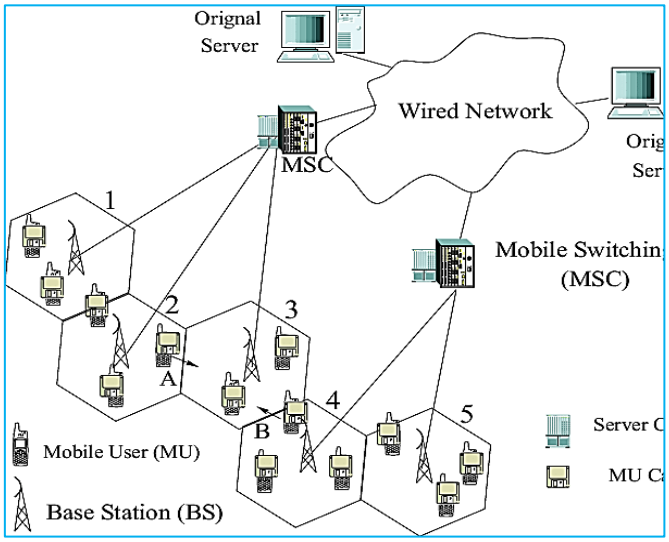


Fig. 1. Mobile network

A WSN is a group of interconnected devices, also called nodes, capable of sensing their environment and transmitting data about the monitored area (e.g., a place or a volume) to other nodes via wireless links[8]. The data is transmitted, perhaps across several hops, to a sink (also known as a controller or monitor), which can be used locally or connected to other networks (like the Internet) via a gateway. The nodes can move or stand still. It may or may not be aware of the location[9]. In either case, they may be homogeneous[10]. There are almost innumerable real-world applications for WSNs, including environmental monitoring, health care, location determination and tracking, logistics, localization, and more[11]–[13]. In this section, we offer a categorization of the possible applications. Multiple sinks in the network are a typical case. The likelihood of isolated node clusters failing to give data because of suboptimal signal propagation conditions is decreased by increasing the density of sinks per node. In theory, a WSN with multiple sinks can scale (i.e., the same performance can be obtained even if the number of nodes is increased); however, this is not true for a network with a single sink [4]. However, for the network engineer, a multi-sink WSN is not simply

an extension of the single-sink scenario. In many instances, the nodes send the data they have collected to one of the sinks they have chosen from a variety of sinks, which ultimately sends the data to the gateway for the final user [14], [15]. Figure 3 shows the two primary seniors of the WSN on both single and multi-sink sinks.

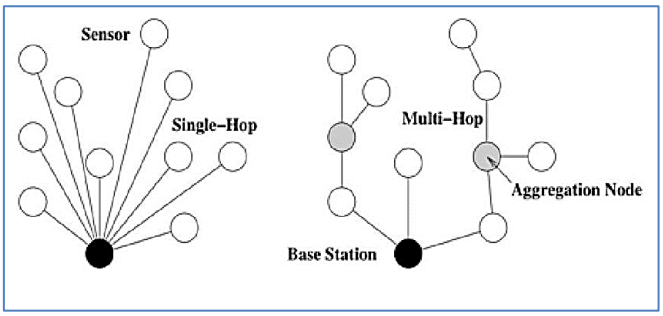


Fig. 2. Single and multi-sink of WSN.

One way to classify apps is based on the type of data that has to be collected on the network. Event detection (ED) and spatial process estimation(SPE) can be used to categorize almost every application[16]–[18]. In the first scenario, sensors detect an occurrence, such as a forest fire, earthquake, etc. A specific physical event that may be described as a two-dimensional random (usually non-stationary) process, such as ground temperature changes in a small volcanic area, or atmospheric pressure in a broad area, is what WSN in SPE seeks to estimate[19]. In this case, the main problem is to estimate the spatial process's overall behavior based on the sensors' samples, which are usually placed at random positions.

2 Mobile AD-HOC network

A mobile device group that connects and interacts without using a preexisting framework is known as a mobile ad hoc network (MANET)[11]. The uniform or focused organization is less common in MANET[20]. Instead of using permanent infrastructure, it creates connections using self-organizing, self-managing networks [1]. Each node performs the functions of a host and a router since the wireless transmission range of each node is constrained. The MANET architecture is shown in Figure 3.

MANETS may be dispatched to any site rapidly and at any time and can adapt to individual situations. These outstanding benefits sparked an immediate interest in MANETS among the military, police, and emergency services, particularly in chaotic or hostile environments[21], [22]. Before it, business applications started to appear, relying on continually developing standards like IEEE 802.11. This kind of network, which may function alone or with one or more points of attachment to cellular networks or the Internet[17], opens the door for a wide range of innovative and intriguing applications. Only a few examples of application scenarios include emergency and rescue operations, conference or university settings, vehicle networks, personal networking,

etc. Static and dynamic routing technologies are both used in MANET[9]. Technically speaking, the fixed network topology is used with the static routing protocol. The physical connection between nodes in a LAN network serves as a great illustration of a static routing system with defined destination nodes [23]. If the node and link topology exhibit mobility features, the network may be ad hoc and employ a dynamic routing system. A router can learn about routing specifics on its own and add the ideal route to its routing table by using dynamic routing. When using a dynamic routing protocol, a router adds the optimal route to its routing table and chooses an alternative path in case the primary route goes completely inaccessible.

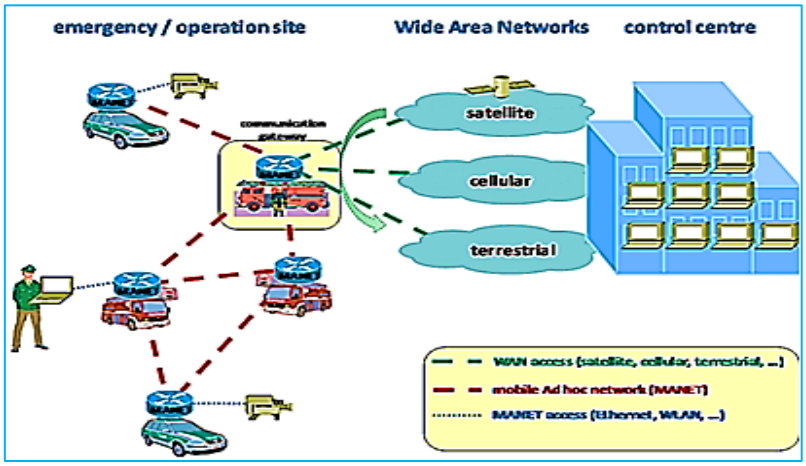


Fig. 3. General architecture of MANET

Radio frequencies are wireless media that typically transmit data between ad hoc network nodes[24], so the network often suffers from interference. Weather and the frequencies of other nearby devices or networks also cause interference. Furthermore, individual devices can obstruct the transmission of a single piece of data to the following network nodes[21]. The singles reflected from obstacles cause multipath propagation. Due to scattering of singles from hard things, it receives the same signal from multipath in delayed time. One of the major problems in wireless communication is path loss (PL)[24], [25]. It arises either because the source of the signal is far from the destination in the network or because of multiple reflections from an obstacle. The mathematical calculation of path loss depends on the ratio of the power of the transmitted signal to the received signal. Equation 1x calculates the path loss[26].

$$PL(d) = PL(d_0) + 10n \log_{10}\left(\frac{d}{d_0}\right) \qquad (1)$$

where d is the distance, d_0 is the reference point at 1 km, and n is the path loss exponent. Interference is another core problem in the management of wireless communication during the propagation of traffic in space[26]. The interference, path loss, and multipath propagation reduce the network's quality of service (QoS). The routing protocols for wireless networks should be able to link and maintain paths to other nearby

nodes and, in most situations, manage path change brought on by the dynamic behavior of nodes. Although the majority of routing protocols are available, they do not take quality of service into account. The network user's expectation of communication is satisfied by the quality of service, which offers an effective transmission service. Over the past few years, vehicular ad hoc networks (VANETs) technology has been a significant topic of research [27]. VANET is an ad-hoc network built by constructing a network of cars for a particular demand or situation. Now that VANETs have been proven to be effective networks used by vehicles on highways or in metro regions. Along with its advantages, VANET also has several drawbacks, such as the problems of providing high-quality service, high connectivity, bandwidth, vehicle security, and individual privacy. The communication between moving cars in a certain environment is handled by vehicular ad hoc networks [28]. Vehicle-to-vehicle (V2V) communication is the direct communication between two vehicles. Vehicle-to-infrastructure (V2I) communication is the direct communication between a vehicle and infrastructure, such as a Road Side Unit (RSU) (V2I). Figure 4 shows a typical VANET scenario.

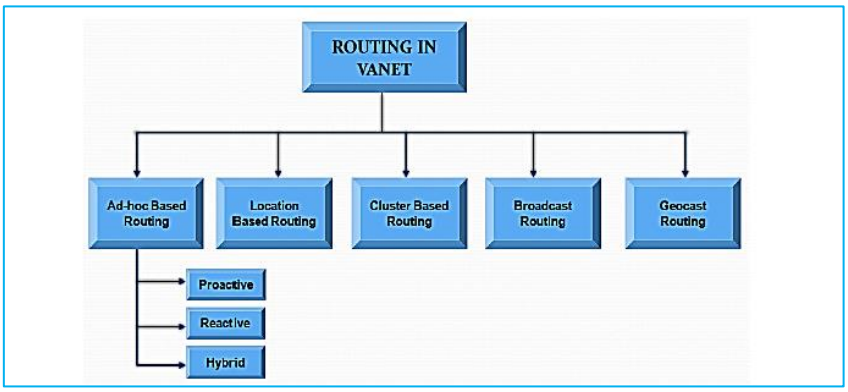


Fig. 4. Routing Types in VANET

The creation of a dynamic routing protocol that permits the transmission of information from one node (vehicle) to another is one of the major issues in the development of vehicular ad hoc networks. Because the topology of a VANET is very dynamic and continually changing, routing in a VANET differs from standard MANET routing. Some previous protocols developed for MANET environments have been tested in VANET[27]. However, there is still work to be done in order to speed up information transfer between nodes. By addressing these issues in MANET protocols, real-time applications for the VANET environment can be developed. It's important to carefully evaluate additional effects, such as reducing control overhead [1]. Given the previously mentioned dynamic properties of VANET, the routing protocol should be resilient to vehicular network architecture's unpredictable and dynamic properties. Finding and maintaining the optimum communication paths in the intended environments may be the most challenging challenge in VANET routing [6]. The performance of most routing protocols in VANET varies as the network topology changes since these protocols

are closely related to the topology utilized in the network architecture. Five broad criteria can be used to categorize routing in VANET:

- Ad-hoc or topology-driven protocols
- Location-based routing protocols
- Cluster-based
- Broadcast protocols
- Geocast protocols

3 Quality of service (QoS)

The QoS-aware routing protocol must consist of the following requirements, which must be met:

3.1 Resource estimation

Ad hoc networks allow for resource sharing between the host node and its nearby nodes. Due to the dynamic nature of MANET's architecture, it is necessary to estimate resource availability in order to improve QoS [29].

3.2 Route discovery

Reactive and proactive procedures are available for route finding in MANET [30]. In the proactive mechanism, routes are discovered and established with minimal delay, while in the reactive mechanism, the route establishment time is high but still reduces the routing overhead[31]. To obtain better QoS, route discovery must be done with lower overhead and delay. Figure 5 illustrates the discovered route in MANT.

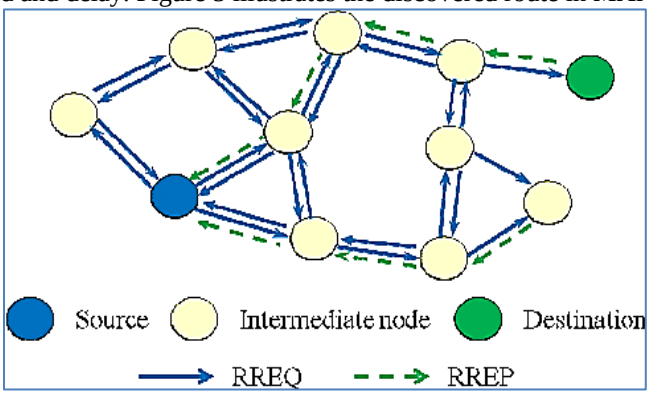


Fig. 5. discovering routes

3.3 Resource reservation QoS

Resource distribution to the nodes in dynamic topology presents a significant issue in the situation of resource scarcity. In addition to insufficiency, giving resources to nodes that participate in transmission improves quality of service [32].

3.4 Route maintenance

Due to the mobility of nodes, identified data transmission routes can sometimes get disconnected [33]. To deal with this issue, the route's nodes must be predicted, and some redundant routes must be identified for the same data transmission. This helps in better QoS. Figure 6 shows the route maintenance in MANET.

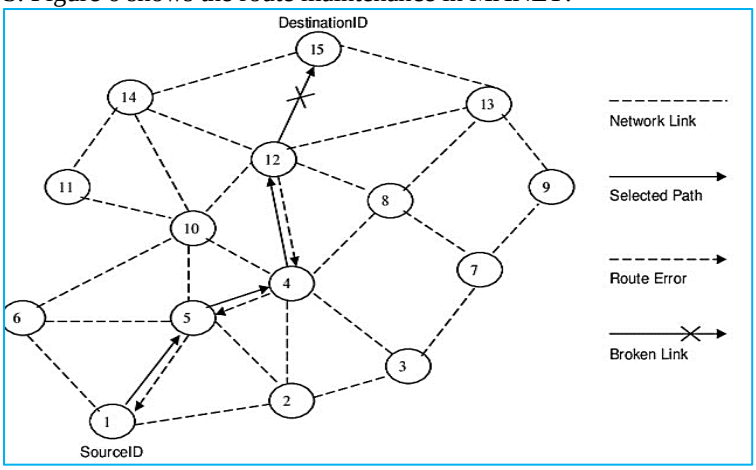


Fig. 6. Route maintenance

3.5 Route selection

Routes from source to destination must be selected from among the several existing routes based on bandwidth availability, the distance of the route, and the amount of hop counts for the route. [34]. Figure 7 shows the type of media that could be transmitted over MANT's networks and QoS.

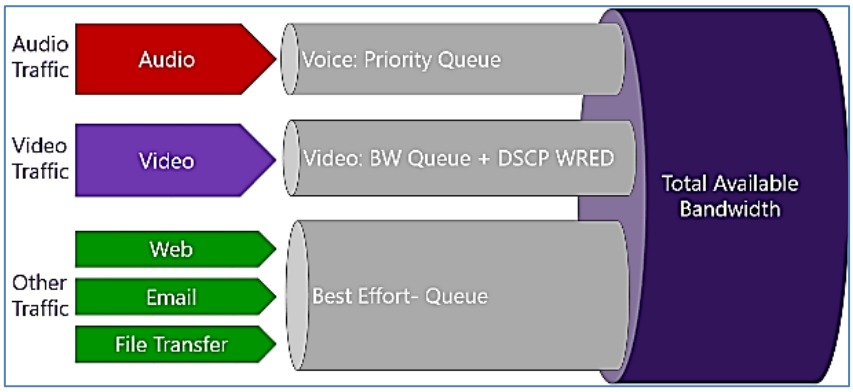


Fig. 7. Type of Media in QoS

4 Manet routing protocols

A set of systematic guidelines known as a network protocol governs how data is exchanged among various devices connected to the same network [11]. Routing, data transfer, communication, and resource sharing require network protocols. As seen in Figure 8, a mobile ad hoc network (MANET) is an autonomous group of mobile users (nodes) interacting across wireless networks with restricted bandwidth. Due to the nodes' mobility, the network topology might rapidly and unexpectedly alter over time. Because the network is decentralized, nodes must organize and exchange sms. Routing messages might be problematic in a decentralized setting where the topology fluctuates [35]. In a static network, the shortest path between two points based on a specified cost function is typically the best route, but this idea is challenging to apply in MANETs.

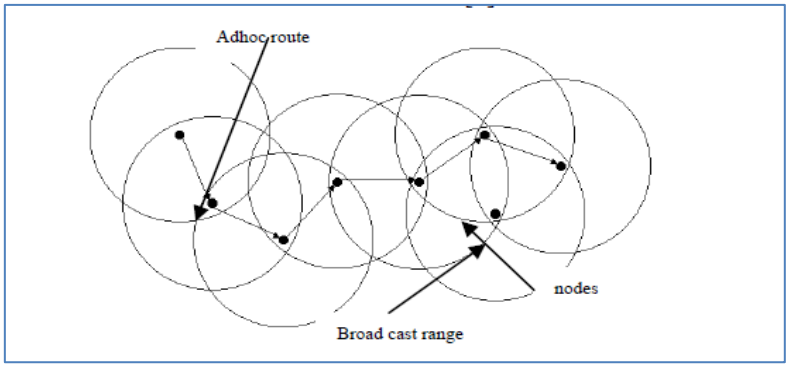


Fig. 8. Example of mobility in an Ad-hoc Network.

Reactive and proactive routing protocols are used to manage routing in the MANET network. The two reactive routing protocols that are most frequently used are Dynamic Source Routing (DSR) and the Ad Hoc On-Demand Distance Vector (ADOV) [21] [1].

The proactive routing protocol family includes the Ad Hoc On-Demand Distance Vector (ADOV). The different routing techniques based on topology are shown in Figure 9.

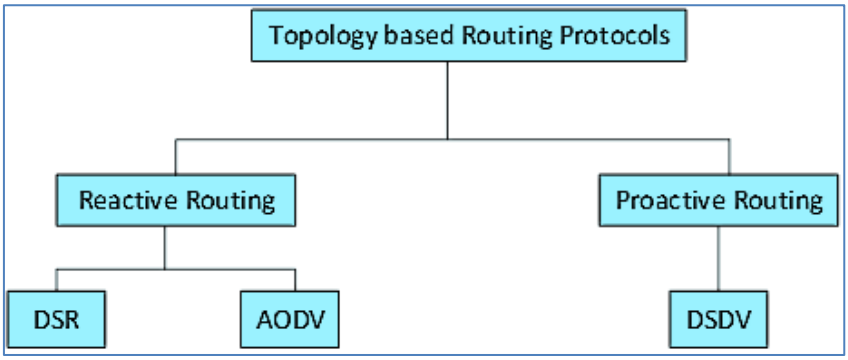


Fig. 9. Topology-based routing protocols.

Reactive routing group techniques are needed for dynamic network topologies, despite proactive routing group protocols being better suited to decrease bandwidth utilization and give faster convergence times [36]. The AODV and DSR topology-based routing protocols used more CPU, memory, bandwidth, and battery power than the DSDV routing protocol.

4.1 Ad Hoc on-demand distance vector (ADOV)

TADSV is a reactive routing protocol developed for MANET and other mobile networks [6]. It is suited for MANET networks due to a number of advantageous features, such as dynamic, self-starting multi-hop routing between mobile nodes aiming to set up and maintain an ad hoc network[37]. AODV enables the evolution of routes to specific locations without requiring nodes to maintain these routes while not communicating[38]. Using objective sequence numbers, AODV circumvents the problem of "counting to infinity." As a result, AODV is loop-free. The AODV routing protocol's routing messages contain only information about the source and destination, not the entire route path through the network[39]. The transmission of an RREQ (Route Request) packet in the MANET network can be seen in Figure 10.

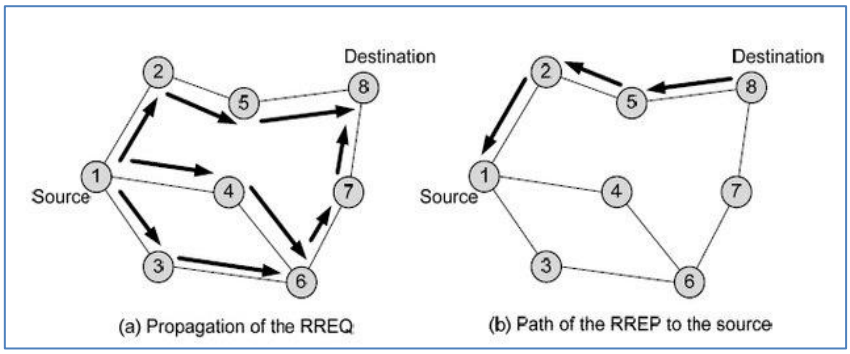


Fig. 10.AODV broadcast RREQ.

The AODV routing protocol was created for mobile ad hoc networks that contain tens to thousands of mobile nodes. AODV can manage a range of data traffic levels as well as low, moderate, and rather high mobility rates. As a result of the usage of pre-configured keys or the knowledge that there are no harmful attacker nodes, in networks where every node can trust one another AODV is intended for use [24]. AODV was developed to decrease the spread of control traffic and eliminate overhead on data traffic, hence boosting scalability and performance [29]. Formats for Messages Routing Request Message Format (RREQ) When a link breaks and some of the node's neighbors can no longer access one or more destinations, the RERR message is sent.

4.2 Dynamic source routing (DSR)

The route packets take within the MANET, from source to destination, is governed by a routing method known as TDSR. With the help of this method, nodes can locate a source route over several network hops to any desired destination node [40]. The two main aspects of the DSR routing protocol are route discovery and route maintenance. When sending packets over the DSR protocol, mobile hosts must first determine if they already have a route to the desired destination by checking their route cache[38]. A packet is sent to the host when the network contains the source-to-destination route. Imagine that the host node lacks a route. Let's say the route is still active and hasn't been discontinued. In this instance, it initiates the route discovery procedure by sending a route request packet, including the destination addresses and the mobile source host in addition to a special identifying number [40]. Each node in the network receives a packet using the DSR routing protocol to determine whether a route to the destination exists [35]. If not, it forwards the packet after adding its address to the route entry and using its routing links. When a request reaches the destination and an unclaimed route to the destination is present in the intermediate node's cache, the route of a packet is established in both cases [34]. The delivered package using DSR routing across the MANET network is shown in Figure 11.

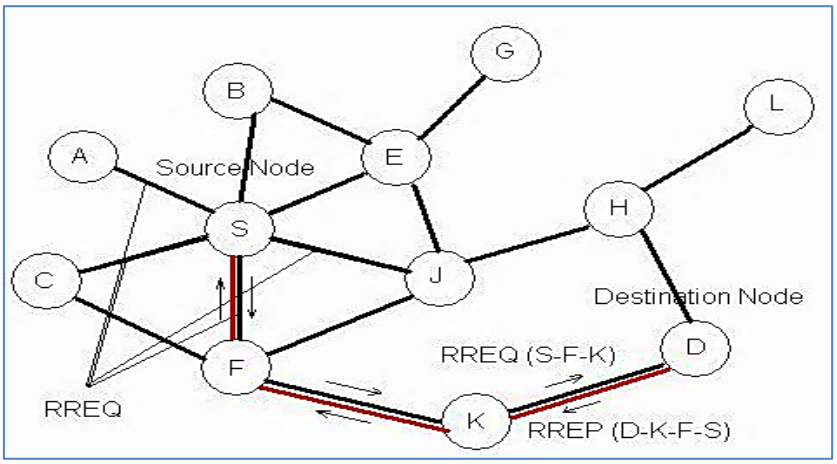


Fig. 11.DSR broadcast RREQ.

5 Optimization algorithms for enhancing routing protocols

The term meta-heuristic comes from ancient Greek. The word meta-heuristic is composed of two words: Meta means "higher level method," and heuristics means "discovering new strategies"[41]–[43]. Meta-heuristics is technically concerned with finding the best existing solution among huge and complex solutions. It obtains an approximate solution, i.e., it "guides" the search process by using the chance to find the best possible solutions[15], [44], [45]. The metaheuristic algorithms have strong properties representing flexibility, speed, and success in solving various real-world problems, making them interesting for researchers. The metaheuristic algorithms are classified into two categories according to the type of population (proposed solutions)[46]: single-solution metaheuristics and population-based metaheuristics. Single solution metaheuristics is a heuristic technique that uses iterative improvement of a single solution to find an optimal solution. S-metaheuristics can be described as a "walk" through neighborhoods to get from the current solution to another key in the search space [47]. Some examples of this approach are Hill-Clamping, Variable Neighborhood Searches (VNS), Tabu Search (TS), and Scatter Search (SS)[42]. The implementation of metaheuristic algorithms for optimizing the routing protocols in the following scenario[48-63]:

- Set the initialization parameters.
- Select optimal parameters for MANET routing protocols
- Set the route that achieves the best performance of the MANET routing protocols.
- Visualize the best-performing mobile network.
- The challenges of using metaheuristic algorithms for optimizing the routing protocols:
- In metaphoric optimization, there is stagnation in the leak.
- Improving major routing protocol parameters such as the number of connections, mobility rate, and several nodes.

- Enhancing one aspect of the MANET routing protocol and ignoring the protocol's primary parameter.
- The protocol's use of the deflate parameter F is not adaptable to each simulation scenario.
- Select optimal protocol characteristics by testing a few values to test each paragraph.
- The parameters of the routing protocol are not optimized.
- To evaluate the routing protocol's performance, use the static weight of the network.

Table 1 illustrates some of the technologies that aim to enhance the performance of MANET routing protocols

Table 1. Comparison between some of the technologies of Optimize MANET routing protocols.

Ref.	Paper name	Published year	Enhanced Protocols	Description
[64]	Enhanced-Ant-AODV for optimal route selection in a mobile ad-hoc network	2021	DSR, AODV	Using the ACO to optimize only the number of nodes and speed of nods. The proposed model did not solve time consumption and stagnation in AOC.
[21]	Performance Evaluation of Different Mobile Adhoc Network Routing Protocols in Difficult Situations	2021	DSR, AODV	The routing protocol's parameters are not optimized. Examine the performance of the routing protocol using static values from the network.
[65]	Improvisation of optimization technique and AODV routing protocol in VANET	2020	AODV	The AOC optimized initial condition to the selected node for transmitting data from source to distention. The proposed model potentially suffers from the end terminal node.
[22]	Performance analysis and enhancement of position-based routing protocols in MANETS	2019	DSR, AODV	This study's analysis concentrated on some metrics, such as power consumption, throughput, delay, and packet transmission rate. By testing a small number of values for each parameter,

				choose the best protocol characteristics.
[66]	A Stable Routing Protocol based on DSR Protocol for Mobile Ad Hoc Networks	2018	DSR	This paper aims to provide a reliable and highly effective routing protocol for these networks. Improving one component of the MANET routing protocol while ignoring its main parameter

6 Conclusion

Routing protocols govern the identification of the data path from source to destination. A collection of mobile devices connected informally forms a mobile network. It can be either a wireless ad hoc network (VANET) or a mobile ad hoc network (MANET). Self-organized, self-managed networks that MANET uses allow connections without needing a set infrastructure. Every node serves as a host and a router. The MANET routing protocol uses either proactive or reactive routing protocols. For dynamic network topologies, the routing protocol used is. Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector are two instances (ADOV). Proactive routing protocols can achieve longer convergence times with lower bandwidth consumption. Destination-sequenced distance vector routing (DSDV) serves as an illustration. The optimization multi-objective searches an optimal path from various delay, packet loss, and PDR scenarios. Finding the most effective routing for numerous protocols, including DSR, AODV, and DSDV, is the primary objective function of metaheuristics.

7 References

[1] A. S. Mustafa, M. M. Al-Heeti, M. M. Hamdi, and A. M. Shantaf, “Performance Analyzing the Effect of Network Size on Routing Protocols in MANETs,” HORA 2020 - 2nd Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc., 2020, doi: 10.1109/HORA49412.2020.9152838.

[2] A. Singh, K. Chatterjee, and S. C. Satapathy, “An edge based hybrid intrusion detection framework for mobile edge computing,” Complex Intell. Syst., 2021, doi: 10.1007/s40747-021-00498-4.

[3] J. khan, A. Abbas, and K. khan, “Cellular Handover approaches in 2.5G to 5G Technology,” Int. J. Comput. Appl., vol. 21, no. 2, pp. 28–37, 2011, doi: 10.5120/2482-2984.

[4] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, “Distributed reflection denial of service attack: A critical review,” Int. J. Electr. Comput. Eng., vol. 11, no. 6, pp. 5327–5341, 2021, doi: 10.11591/ijece.v11i6.pp5327-5341.

[5] H. M. E. MOHAMED, “Non Orthogonal Multiple Access Technique for 5G Network.” 2022.

[6] F. T. Al-Dhief, N. Sabri, M. S. Salim, S. Fouad, and S. A. Aljunid, "MANET Routing Protocols Evaluation: AODV, DSR and DSDV Perspective," MATEC Web Conf., vol. 150, pp. 1–6, 2018, doi: 10.1051/matecconf/201815006024.

[7] [7] D. Leite, I. Škrjanc, and F. Gomide, "An overview on evolving systems and learning from stream data," Evol. Syst., vol. 11, no. 2, pp. 181–198, 2020, doi: 10.1007/s12530-020-09334-5.

[8] M. S. Alsahli, M. M. Almasri, M. Al-Akhras, A. I. Al-Issa, and M. Alawairdhi, "Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 5, pp. 617–626, 2021, doi: 10.14569/IJACSA.2021.0120574.

[9] A. K. Habboush, "Ant Colony Optimization (ACO) Based MANET Routing Protocols: A Comprehensive Review," Comput. Inf. Sci., vol. 12, no. 1, p. 82, 2019, doi: 10.5539/cis.v12n1p82.

[10] T. A. N. Abdali, R. Hassan, R. C. Muniyandi, A. H. M. Aman, Q. N. Nguyen, and A. S. Al-Khaleefa, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in manet," Inf., vol. 11, no. 11, pp. 1–17, 2020, doi: 10.3390/info11110529.

[11] A. Mishra, S. Singh, and A. K. Tripathi, "Comparison of MANET routing protocols," Int. J. Comput. Sci. Mob. Comput, vol. 8, no. March, pp. 67–74, 2019, [Online]. Available: https://www.researchgate.net/profile/Shweta-Singh-35/publication/331980713_Comparison_of_Manet_Routing_Protocols/links/5c98a669299bf11169457ef3/Comparison-of-Manet-Routing-Protocols.pdf.

[12] H. M. Anwer, "A Framework for Efficient Network Anomaly Intrusion Detection with Features Selection," pp. 157–162, 2018.

[13] M. Whitney, "Teaching Accessible Design: Integrating Accessibility Principles and Practices into an Introductory Web Design Course," Proc. EDSIG Conf., vol. 18, no. February, pp. 1–10, 2019.

[14] A. K. Sangaiah, S. Rezaei, A. Javadpour, F. Miri, W. Zhang, and D. Wang, "Automatic Fault Detection and Diagnosis in Cellular Networks and Beyond 5G: Intelligent Network Management," Algorithms, vol. 15, no. 11, p. 432, 2022.

[15] R. R. Nuiaa, S. Manickam, A. H. Alsaeedi, and E. S. Alomari, "A new proactive feature selection model based on the enhanced optimization algorithms to detect DRDoS attacks," Int. J. Electr. Comput. Eng., vol. 12, no. 2, pp. 1869–1880, 2022, doi: 10.11591/ijece.v12i2.pp1869-1880.

[16] J. M. G. Hidalgo, G. C. Bringas, E. P. Sánz, and F. C. García, "Content based SMS spam filtering," Proc. 2006 ACM Symp. Doc. Eng. DocEng 2006, vol. 2006, pp. 107–114, 2006, doi: 10.1145/1166160.1166191.

[17] S. M. Hadi et al., "Trigonometric words ranking model for spam message classification," IET Networks, 2022, doi: 10.1049/ntw2.12063.

[18] S. S. Mohamed Ali, A. H. Alsaeedi, D. Al-Shammary, H. H. Alsaeedi, and H. W. Abid, "Efficient intelligent system for diagnosis pneumonia (SARSCOVID19) in X-ray images empowered with initial clustering," Indones. J. Electr. Eng. Comput. Sci., vol. 22, no. 1, pp. 241–251, 2021, doi: 10.11591/ijeecs.v22.i1.pp241-251.

[19] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks," Proc. - IEEE Symp. Comput. Commun., pp. 567–574, 2002, doi: 10.1109/ISCC.2002.1021731.

[20] M. S. Daas and S. Chikhi, "Response surface methodology for performance analysis and modeling of MANET routing protocols," Int. J. Comput. Networks Commun., vol. 10, no. 1, pp. 45–61, 2018, doi: 10.5121/ijcnc.2018.10104.

[21] S. M. Alkahtani and F. Alturki, "Performance Evaluation of Different Mobile Ad-hoc Network Routing Protocols in Difficult Situations," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 1, pp. 158–167, 2021, doi: 10.14569/IJACSA.2021.0120119.
[22] M. Alnabhan, S. Alsaraireh, B. K. Pattanayak, A. K. Habboush, and M. Hammad, "Performance analysis and enhancement of position-based routing protocols in MANETS," Int. J. Knowledge-Based Intell. Eng. Syst., vol. 23, no. 2, pp. 109–120, 2019, doi: 10.3233/KES-190404.
[23] D. J. Fehér and B. Sándor, "Log File Authentication and Storage on Blockchain Network," SISY 2018 - IEEE 16th Int. Symp. Intell. Syst. Informatics, Proc., pp. 243–247, 2018, doi: 10.1109/SISY.2018.8524848.
[24] M. Z. Zakaria, S. Mutalib, S. A. Rahman, S. J. Elias, and A. Z. Shahuddin, "Solving RFID mobile reader path problem with optimization algorithms," Indones. J. Electr. Eng. Comput. Sci., vol. 13, no. 3, pp. 1110–1116, 2019, doi: 10.11591/ijeecs.v13.i3.pp1110-1116.
[25] P. Tang et al., "Channel measurement and path loss modeling from 220 GHz to 330 GHz for 6G wireless communications," China Commun., vol. 18, no. 5, pp. 19–32, 2021.
[26] W. Tang et al., "Wireless Communications with Reconfigurable Intelligent Surface: Path Loss Modeling and Experimental Measurement," IEEE Trans. Wirel. Commun., vol. 20, no. 1, pp. 421–439, 2021, doi: 10.1109/TWC.2020.3024887.
[27] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," IEEE Access, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.
[28] M. J. N. Mahi et al., "A Review on VANET Research: Perspective of Recent Emerging Technologies," IEEE Access, vol. 10, pp. 65760–65783, 2022, doi: 10.1109/ACCESS.2022.3183605.
[29] M. Alnabhan, M. Alshuqran, M. Hammad, and M. Al Nawayseh, "Performance evaluation of unicast routing protocols in MANETs-current state and future prospects," Int. J. Interact. Mob. Technol., vol. 11, no. 1, pp. 84–97, 2017, doi: 10.3991/ijim.v11i1.6295.
[30] R. Hemalatha, R. Umamaheswari, and S. Jothi, "Optimal route maintenance based on adaptive equilibrium optimization and GTA based route discovery model in MANET," Peer-to-Peer Netw. Appl., vol. 14, no. 6, pp. 3416–3430, 2021.
[31] U. Allimuthu and K. Mahalakshmi, "Intelligent route discovery towards rushing attacks in ad hoc wireless networks," J. Ambient Intell. Humaniz. Comput., vol. 13, no. 2, pp. 921–960, 2022.
[32] S. Venkatasubramanian, A. Suhasini, and C. Vennila, "QoS Provisioning in MANET Using Fuzzy-Based Multifactor Multipath Routing Metric," in Sustainable Communication Networks and Application, Springer, 2022, pp. 555–566.
[33] A. M. Soomro et al., "Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management," J. Commun., vol. 17, no. 9, 2022.
[34] R. Ramalingam et al., "Routing Protocol for MANET Based on QoS-Aware Service Composition with Dynamic Secured Broker Selection," Electronics, vol. 11, no. 17, p. 2637, 2022.
[35] S. Manickam, R. Rahef Nuiaa, A. Hakem Alsaeedi, Z. A. A. Alyasseri, M. A. Mohammed, and M. M. Jaber, "An enhanced mechanism for detection of Domain Name System-based distributed reflection denial of service attacks depending on modified metaheuristic algorithms and adaptive thresholding techniques," IET Networks, vol. 11, no. 5, pp. 169–181, 2022, doi: 10.1049/ntw2.12043.
[36] A. S. Alfoudi et al., "Hyper clustering model for dynamic network intrusion detection," IET Commun., 2022, doi: 10.1049/cmu2.12523.

[37] H. S. Mansour et al., "Cross-Layer and Energy-Aware AODV Routing Protocol for Flying Ad-hoc Networks," sustainability, vol. 14, no. 15, p. 8980, 2022.
[38] P. Sarao, "Comparison of AODV, DSR, and DSDV routing protocols in a wireless network," J. Commun., vol. 13, no. 4, pp. 175–181, 2018, doi: 10.12720/jcm.13.4.175-181.
[39] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks," Internet of Things, vol. 20, p. 100627, 2022.
[40] M. G. K. Alabdullah, B. M. Atiyah, K. S. Khalaf, and S. H. Yadgar, "Analysis and simulation of three MANET routing protocols: A research on AODV, DSR & DSDV characteristics and their performance evaluation," Period. Eng. Nat. Sci., vol. 7, no. 3, pp. 1228–1238, 2019, doi: 10.21533/pen.v7i3.717.
[41] A. H. Jabor and A. H. Ali, "Dual Heuristic Feature Selection Based on Genetic Algorithm and Binary Particle Swarm Optimization," J. Univ. BABYLON Pure Appl. Sci., vol. 27, no. 1, pp. 171–183, 2019, doi: 10.29196/jubpas.v27i1.2106.
[42] A. H. Al-saeedi, "Binary Mean-Variance Mapping Optimization Algorithm (BMVMO)," J. Appl. Phys. Sci., vol. 2, no. 2, pp. 42–47, 2016, doi: 10.20474/japs-2.2.3.
[43] A. S. Alfoudi, A. H. Alsaeedi, M. H. Abed, A. M. Otebolaku, and Y. S. Razooqi, "Palm Vein Identification Based on Hybrid Feature Selection Model," Int. J. Intell. Eng. Syst., vol. 14, no. 5, pp. 469–478, 2021, doi: 10.22266/ijies2021.1031.41.
[44] R. R. Nuiaa, A. H. Alsaeedi, S. Manickam, and D. E. J. Al-Shammary, "Evolving Dynamic Fuzzy Clustering (EDFC) to Enhance DRDoS_DNS Attacks Detection Mechnism," Int. J. Intell. Eng. Syst., vol. 15, no. 1, pp. 509–519, 2022, doi: 10.22266/IJIES2022.0228.46.
[45] M. Mafarja, A. Qasem, A. Asghar, and I. Aljarah, "Efficient Hybrid Nature-Inspired Binary Optimizers for Feature Selection," 2019.
[46] D. Al-Shammary, A. L. Albukhnefis, A. H. Alsaeedi, and M. Al-Asfoor, "Extended particle swarm optimization for feature selection of high-dimensional biomedical data," Concurr. Comput. Pract. Exp., vol. 34, no. 10, p. e6776, 2022, doi: https://doi.org/10.1002/cpe.6776.
[47] S. Al-Janabi and A. Alkaim, "A novel optimization algorithm (Lion-AYAD) to find optimal DNA protein synthesis," Egypt. Informatics J., vol. 23, no. 2, pp. 271–290, 2022, doi: https://doi.org/10.1016/j.eij.2022.01.004.
[48] [48] N. Subramani, P. Mohan, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks," Sensors, vol. 22, no. 2, p. 415, 2022.
[49] Y. Yang, Y. Wu, H. Yuan, M. Khishe, and M. Mohammadi, "Nodes clustering and multi-hop routing protocol optimization using hybrid chimp optimization and hunger games search algorithms for sustainable energy efficient underwater wireless sensor networks," Sustain. Comput. Informatics Syst., vol. 35, p. 100731, 2022.
[50] A. A. Bahattab, "Designing ROACM routing protocol along with bandwidth allocation using seagull optimization for ad hoc wireless network," Telecommun. Syst., vol. 81, no. 3, pp. 357–372, 2022.
[51] S. Perumal, "Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism," Wasit Journal of Computer and Mathematics Science, pp. 43-51, 2021.
[52] I. A. A. Jaafar Q. Kadhim, H. ALRikabi, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 02, 2023.
[53] D. Al-Malah, and H. Salim, "Enhancement of educational services by using the internet of things applications for talent and intelligent schools," Periodicals of Engineering and Natural Sciences (PEN), vol. 8, no. 4, pp. 2358-2366, 2020.

[54] H. Ibrahim, "A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 76-108, 2022.
[55] N. A. Jasim, and M. S. Farhan, "Internet of Things (IoT) application in the assessment of learning process," in IOP Conference Series: Materials Science and Engineering, 2021, vol. 1184, no. 1: IOP Publishing, p. 012002.
[56] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," Wasit Journal of Computer and Mathematics Science, vol. 1, no. 3, 2022.
[57] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 2, pp. 12-20, 2022.
[58] R. a. M. Al_airaji , I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," International Journal of Interactive Mobile Technologies, vol. 16, no. 10, 2022.
[59] S. Alam, "Smart health costing system," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 70-75, 2022.
[60] S. Al-Jaff, O. Bayat, and A. H. Sallomi, "Analysis of Interference and Signal Quality in Cellular Wireless Networks," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 881, no. 1: IOP Publishing, p. 012143.
[61] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," International Journal of Online & Biomedical Engineering, vol. 18, no. 12, 2022.
[62] A. S. H. Rihab Salah Khairy, "The Detection of Counterfeit Banknotes Using Ensemble Learning Techniques of AdaBoost and Voting," International Journal of Intelligent Engineering and Systems, vol. 14, no. 1, pp. 326-339, 2021.
[63] H. T. Hazim . H. Alrikabi, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021.

[64] D. Sarkar, S. Choudhury, and A. Majumder, “Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network,” J. King Saud Univ. - Comput. Inf. Sci., vol. 33, no. 10, pp. 1186–1201, 2021, doi: 10.1016/j.jksuci.2018.08.013.
[65] M. Sindhwani, R. Singh, A. Sachdeva, and C. Singh, “Improvisation of optimization technique and AODV routing protocol in VANET,” Mater. Today Proc., vol. 49, pp. 3457–3461, 2020, doi: 10.1016/j.matpr.2021.03.727.
[66] G. Najafi and S. J. Gudakahriz, “A Stable Routing Protocol based on DSR Protocol for Mobile Ad Hoc Networks,” Int. J. Wirel. Microw. Technol., vol. 8, no. 3, pp. 14–22, 2018, doi: 10.5815/ijwmt.2018.03.02.

Article submitted 15 December 2022. Published as resubmitted by the authors 25 December 2022.

Smart robot using in smart homes

https://doi.org/10.31185/wjcm.84

Prof.Dr. Bellatca Naptsoksch(✉)
Computer Science Department,Moscow University, Russia.
bella.napt@mosc.edu.ru

Abstract—the smart robot is an important part of the smart homes system, in this research the Arduino Vacuum Cleaner we built is very compact and practical for potential office and home use. The developed robot is disk-shaped, equipped with vacuuming and cleaning technology and controlled by Arduino nano.

It sucks dirt via a retractable dustbin, using a fan within a motor. the device will be deployed for office and home use thereby making cleaning a fully autonomous duty. This robot will have ultrasonic sensors and an IR proximity sensor. The ultrasonic sensor will allow the robot to avoid obstacles so that it can move freely until the room is properly cleaned, and the proximity sensor will help it to avoid falling from stairs.

One of the most important features of our floor cleaning robot is that it is fast and flexible in movement, able to deal with all dirt and stains on floors without human intervention.

It is also characterized by the fact that it can be disassembled and installed with ease and simplicity, so that in the event of a malfunction, any malfunction will be repaired at the same time. It is also characterized by possessing sensors, so it can identify the .It is possible to develop this technique to become more used in various fields. Because we are in the world of technology development, it becomes very easy to develop such projects to benefit from them in daily life

Keywords—robot, smart home, smart cleaner, wireless sensor

1 Introduction

Technology is important because it is used in all areas of our working life. When you

contemplate your daily routine and count all the technical tools you consume in just one day, you will realize how important technology is, Manual work is taken over the robot technology and many of the related robot appliances are being used extensively also. Here represents the technology that proposed the working of robot for Floor cleaning. Households of today are becoming smarter and more automated. Home automation delivers convenience and creates more time for people. Domestic robots are entering the homes and people's daily lives [1], developers and companies are working everyday all over he world to develop techniques to make our daily life easier. Some movies and TV shows have depicted a future world in which robotic devices will take over routine household tasks, allowing family members to spend more time together and helping the

elderly to live independently for longer. Moreover, Robot vacuums are of great benefit in facilitating the cleaning process for patients allergic to house dust, who must clean the floors daily. These Robots have many distinctive characteristics, which make it superior to humans in many cases, including that it is easy to obtain, and it is also characterized by its small size and ease of handling, as it is made of materials that can be changed, in the event of damage to one of its parts, it thus helps in facilitating and accomplishing many household chores with ease.

[2] In a present-day scenario, we all are so busy with our work that we don't have the time for cleaning our house properly. The solution to the problem is very simple, you just need to buy a domestic vacuum cleaner robot such as irobot roomba which will clean your house with the press of a button. But such commercial products share one common issue, which is cost. So we decided to make a Floor cleaner robot, that costs very less compared to commercial products available in the market [3].

With the aim of keeping our robot as simple as possible, while able to perform the initial

goals, i.e. an autonomous vacuum cleaner robot able to randomly navigate through a room or a house with the minimum human assistance, We offer in your hands a Vacuum Robot for Autonomous floor cleaning application [4]. Vacuum cleaner Robot is designed to make the cleaning process easier rather than by using manual vacuum. This project will explore “Smart Vacuum Cleaner Robot” and discuss it.[5-15]

2 Literature

Cleaning robots are used in domestic and industrial environment .The floor cleaner available in the market requires a lot of human efforts and assistance. Manually cleaning may not wipe off the dust properly as some dust particles may remain on the floor and it can affect the human health adversely. This problem gives a fantastic idea to engineers and researchers to design a robot that can be a helping hand in this work. The smart floor cleaning robot using Arduino is designed using embedded technology. The wireless communication is implemented using Bluetooth to communicate with the robot via android application [1]. The electronic circuitry of the robot consists of the HC-05 Bluetooth module which sends the command to the microcontroller Arduino – UNO on which the software program is directly loaded. L293D chips are used as motor drivers for controlled movement of robot and moppers.

A smart floor cleaner is an electronic device that is intelligently programed to clean a specific area using Arduino based technology. Some features that are seen in smart floor cleaners include wet and dry mopping, vaccum cleaning, detection of obstacles, security cameras and UV sterilization. Some of the Smart Floor Cleaners available are: A. CLEAR [16] operates on dual modes i.e. automatic and manual. In automatic mode, decision is made on the basis of outputs of sensors being processed by Arduino and control actuators by H-Bridge driving circuitry. In manual mode, robot cleans the particular area of room by using laptop with GUI in Visual Studio via. Bluetooth Connectivity.

B. Vito M guardi [19] developed an android application for a robot driven by a microcontroller. His idea of The idea of his work is to show that android app can be operated using totally different electronic devices. He also invented a communication protocol for android smartphone and robot using Bluetooth.

3 Overview of the robot vacuum cleaner

The design of the robot requires considerations of pressure, efficiency and intelligence Choosing the geometry of the disk shape puts it at the forefront of the available conceptual designs With the shape of the disk We were able to reduce the number of robotic wheels to two rear wheels for traction and one servo front wheel The sweepers were also analytically placed in the best position, which increases From the cleaning space of the robot without increasing its overall size, the trash bin has been developed to function simultaneously as a dirt repository and a cyclone device when fully integrated with the cooling fan. Ensure that the trash is in constant contact with the floor

from which dirt is being sucked.[17] In electrical design considerations, the power bank uses the services of the Arduino and the motor shield independently because their power consumption rates vary while the motor shield drives all the motors on board the robot, the Arduino board acts as the brain that receives an impulse from the ultrasonic sensors and controls the motor shield also works An additional lithium-ion battery powers the suction fan which makes the battery work overall i.e. the frame is made of cardboard due[10].

4 Hardware design

We have 4 ultrasonic sensors that detect obstructions for that, we need to connect all the ultrasonic sensor grounds and connect them to a common ground also we connect all 4 VCC of the sensor and connect that at 5v in the Arduino port, and then we connect all the GND to the GND port of the Arduino We connect the sensor port Trigpin1 to port D3, then Trigpin2 to port D5, then Trigpin3 to port D7, then Trigpin4 to port A1, then we connect sensor ports Echopin1 to port D4, then Echopin2 to port D6, then Echopin3 to port D8, then port Echopin4 With A2 port . also connect the IR Module's the output pin of the IR sensor module goes to digital pin D2 on the Arduino. For L293D Motor Driver, we connect the enable pins to 5V and also the motor voltage pin to 5V because we are using 5V motors. the I2C module is used along with the LCD, which

only uses 4 pins where we connect VCC pin, GND with V5, common GND, SCL pin with A4 port and SDA with A5 port. The Arduino, Ultrasonic, motor driver and motors run on 5 Volt, high voltage will kill it so we use a Power Bank 10,000mAh, Lithium-Ion battery Next connect the vacuum cleaner directly to the main circuit. The Bluetooth HC-06 connects the VCC connection to 5V in the Arduino port, then the RX contact unit connects to the TX connection of the target device, the Arduino, and the TX contact connects to the RX of the device. Here a 20x4 alphanumeric LCD is connected to the Arduino using the I2C module, to display a set of words we have added in the code.

5 Mythology

At the beginning of the work, the device consists of 3 switch, where the first is responsible for operating the LCD screen, which in turn displays some of the texts that we have added, and the second is responsible for operating the Arduino and other devices associated with it, and the third and last is responsible for operating the motor installed on the draft fan. And also the robot device consists of four sensors whereby this sensor enables us to know the exact distance between it and the objects in front of it. Time x speed) and it is known that the speed of sound in air is constant and equal to 343 m/s, and using the above equation, we can calculate the distance traveled by the ultrasound wave back and forth to determine the distance of the object between the device and the barrier, where the range of these sensors measure the distance from (4 m - 7m). As for the design of this device, a distance of (15 cm) is measured. When the device is operated through the switches in the device, the Ultrasonic (sensor) gives commands to the device to measure the distance between the barriers and the device[8].

ultrasonic on the front side be No. (1), on the right side No. (2), on the left No. (3), and on the back side No. (4).For example, the front ultrasonic gives a command to measure the front distance, if the distance is less than (15cm), this means that there is a barrier

in the front direction, so the device returns to take a distance from the ultrasonic located on the Right and left sides.

6 Programming the Arduino Board

For this project we have to write a program that uses the HC-SR04 ultrasonic sensor to measure the distance of an object in front of it when the distance is about 15 cm The work is very simple first the transmitter unit sends an ultrasonic wave that travels through the air, hits an obstacle, bounces back and the receiver receives that wave By calculating the time using the Arduino so we have to turn off the motors when there is an object in front of us.

We will also use the on-board LCD display associated with the Arduino nano to display some details from the project title and the names of the work participants.

We also use an IR Module sensor, which consists of a transmitter and an infrared receiver that sends infrared radiation into the surrounding area, up to a distance of 30 cm, much less than the acoustic sensor. Then, if the radiation is reflected and the infrared receiver responds, if the distance between the device and the ground increases.

Step 1: Open the Arduino IDE and open a new window:

In this step using LCD with IC2 so we need to add two libraries "wire.h" and "Liquid CRYSTAL_I2C.h" to improve communication between Arduino and display then I configure the library with the used ports (0x27,20,4). In this part, we define a set of variables for the ultrasonic sensor (4 sensors) in addition to a port for the infrared sensor that receives the wave and sends it, then I define constants that I will need to determine

the directions (left, right, front) I know them from among the constants to give a fixed length that I need later.

Step 2:Now we need to program the setup part: First set the echo Pin from 1 to 4 as "INPUT" and from 1 to 4 as "OUTPUT" trig Pin as "OUTPUT" using the pin Mode keyword and ir pin as "INPUT" Then I configure the ports to the driver that takes port (9, 0, 11, 12) Mark it as "OUTPUT".

Here we add the Serial that is used by Bluetooth to send after that "lcd.init" These are instructions for a screen library that works on the backlight of the LCD, and the "lcd.back light" is for lighting the screen, then I prepare the column and lines to add the codes for the texts that appear on the screen, The following keywords are used: "lcd.set Cursor" Initialize the LCD screen and specify its dimensions (columns, rows), "lcd.print", print text on the display screen, "delay", delay the text, "lcd.clear" hide text from the screen

```
  #include <Wire.h>
  #include <LiquidCrystal_I2C.h>
  LiquidCrystal_I2C lcd(0x27,20,4);
  const int trigPin1 = 6; //For four sensors I know trig-
pin port and echopin
  const int echoPin1 = 8;
  void setup() {
  pinMode(trigPin1, OUTPUT); //Configuration 4 ports take
trigpin which is 1-2-3-4 because 4 sensors
  pinMode(echoPin1, INPUT); //Configuration 4 ports take
echopin which is 1-2-3-4 because 4 sensors
  pinMode(irpin, INPUT);
  pinMode(9, OUTPUT);
  pinMode(10, OUTPUT);
  pinMode(11, OUTPUT);
  pinMode(12, OUTPUT);
  lcd.init();
  lcd.backlight();
  lcd.setCursor(6,1);
  lcd.print("Welcome");
  delay(3000);
  lcd.clear();
```

Step 3:In the voice loop () we need to connect between Bluetooth and the application used in this robot (Bluetooth RC Controller). When the robot gets a certain reading, the motor moves forward and if it does not read backwards, and so on, among the conditions is to convert the movement of the broom automatically through the application mentioned above and also As the application did not get any reading stops.

7 RESULTS

We have designed and implemented an automatic smart floor cleaning robot using embedded technology. It is an effective solution with simple approach utilizing local resources while making it available in an affordable amount. The Risk Factor for this Robot is very Minimum since the water pathway is separately made so it does not Co-incide with the Electronic circuitry. Also the robot does not uses high voltage thereby reducing threat and making it more user friendly. It is of great usage to Aged Citizens.

8 Conclusions

The effectiveness of the Robot can be increased by using sensors and applying Algorithms, so that it can detect obstacles and turns into other directions without human Assistance. The Bluetooth Module HC -12 Can be used instead of HC-05 to increase the wireless communication rate. More techniques of Reducing cost of the Robot can be considered

1. Providing an overview of technology, especially artificial intelligence technology, its importance in daily life, ways to develop it to serve the community, as well as how to
2. facilitate work using a robot to clean floors in an easy and effortless way.
3. The tools that can be used to form the project and identify it in detail and how to connect it to the Arduino and know its use. These tools include ultrasonic sensors, infrared sensors, and many more tools.
4. Learn the Arduino language, how to program the Arduino piece, how to connect devices together, know the work steps in detail and provide high efficiency in work and use the device anywhere and also in the way of remote communication.
5. Learn about the benefits of the project, its applications, how to develop it, and its

importance in homes, because one of the advantages of the project can be used at any time because it does not have a lot of noise, the quiet sound, and also one of its advantages is the light size.

9 REFERENCES

[1] Subankar Roy , Tashi Rapden Wangchuk , Rajesh Bhatt , " Arduino based Bluetooth Controlled Robot'', International Journal of Engineering and Trends and Technology , Volume 32 (5) , February 2016.

[2] Abhishek Shrivastva , " Arduino based Smart Submersible Pump Controller" , International Journal of Scientific Engineering and Research , ISSN(Online): 2347-3878 , Volume 4 (8) , August 2016.

[3] Namita Shinde ,Shreya Shrivastava , Vineet Sharma , Samarth Kumar , " Paper on Arduino Controlled Arduino Based Robot Car" , International Journal of Industrial Electronics and Electrical Engineering , ISSN(p) :2347-6982 , Volume 6(3) , March 2013.

[4] Manya jain , Prakash Singh Rawat , "Automatic Floor Cleaner" , International Research Journal of Engineering and Technology , ISSN(p) : 2395-0072 , Volume 4(4) , April 2017.
[5] Arpit Sharma , Reetesh Verma , Saurabh Gupta , Sukhdeep kaur , " Android Phone Controlled Robot using Bluetooth " , International Journal of Electronic and Electrical Engineering , ISSN 0974-2174 , Volume 7(5) , 2014.
[6] Al-ogaili, H. and A.M. Shadhar, *the Finger Vein Recognition Using Deep Learning Technique.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 1-11.
[7] Salim ALRikabi, H.T., et al., *Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN.* International Journal of Interactive Mobile Technologies, 2022. **16**(8).
[8] Al Mossawy, M.M.T. and L.E. George, *A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(1): p. 1-14.
[9] Alaidi, A.H.M., et al., *Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques.* International Journal of Interactive Mobile Technologies, 2022. **16**(10).
[10] Ahmed, H., *A Review of Hash Function Types and their Applications.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 120-139.
[11] Jaafar Q. Kadhim, I.A.A., Haider TH. Salim ALRikabi, *Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT.* International Journal of Emerging Technologies in Learning (iJET), 2023. **18**(02).
[12] Nsaif, B.G., A.H. Sallomi, and M.H. Wali, *MOBILE LOCATION PREDICTION IN CELLULAR NETWORKS by SIGNAL RECEIVED STRENGTH.* Design Engineering, 2021: p. 8804-8812.
[13] Khalifa, M.A., et al., *A Novel Arabic Words Recognition System Using Hyperplane Classifier.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 12-20.
[14] Meteab, W.K., et al. Controlling and Monitoring a Robot-Car Based on Smart Phone Applications. in IOP Conference Series: Materials Science and Engineering. 2021. IOP Publishing.
[15] Nabaa Ali Jasim, H.T.S.A., *Design and Implementation of Smart City Applications Based on the Internet of Things.* International Journal of Interactive Mobile Technologies (iJIM), 2021. **15**(13): p. 4-15.
[16] Uman Khalid et al , " Smart Floor Cleaning Robot (CLEAR)'' , Ghulam Ishaq Khan Institute of Engineering Sciences and Technology , Pakistan , 2015.
[17] Neamah, A. F., & Salman, O. S. (2022, October). E-learning as a successful alternative: Proposing an online tests system for iraqi universities. In *AIP Conference Proceedings* (Vol. 2398, No. 1, p. 050034). AIP Publishing LLC..
[18] Development of a vacuum cleaner robot T.B. Asafa, T.M. Afonja, E.A. Olaniyan, H.O. Alade Mechanical Engineering Department, Ladoke Akintola University of Technology, P.M.B. 4000, Ogbomoso, Nigeria Received 20 October 2016; revised 9 March 2017; accepted 9 July 2018 Available online 14 November 2018.
[19] Hiroshi Hisahara, Yuki Ishii, Masahito Ota, Takeki Ogitsu, Hiroshi Takemura, Hiroshi Mizoguchi, Human avoidance function for robotic vacuum cleaner through use of environmental sensors: Roomba making way for humans, in:2014 5th International Conference on Intelligent Systems, Modelling and Simulation (ISMS), IEEE, 2014, pp. 64–67.

Article submitted 20 November 2022. Published as resubmitted by the authors 26 December 2022.

Detection of Deep Fake in Face Images Using Deep Learning

https://doi.org/10.31185/wjcm.92

Hanady Sabah Abdul kareem(✉)
Computer Science Department, College of Science, Al-Nahrain University, Baghdad, Iraq
hanadysabah763@gmail.com

Mohammed Sahib Mahdi Altaei
Computer Science Department, College of Science, Al-Nahrain University, Baghdad, Iraq
altaeimohamed@gmail.com

Abstract— Fake images are one of the most widespread phenomena that have a significant influence on our social life, particularly in the world of politics and celeb. Nowadays, generating fake images has become very easy due to the powerful yet simple applications in mobile devices that navigate in the social media world and with the emergence of the Generative Adversarial Network (GAN) that produces images which are indistinguishable to the human eye. Which makes fake images and fake videos easy to perform, difficult to detect, and fast to spread. As a result, image processing and artificial intelligence play an important role in solving such issues. Thus, detecting fake images is a critical problem that must be controlled and to prevent these numerous harmful effects. This research proposed utilizing the most popular algorithm in deep learning is (Convolution Neural Network) to detect the fake images.

The first steps includes a preprocessing which start with converting images from RGB to YCbCr color space, after that entering the Gamma correction. finally extract edge detection by entering the Canny filter on them. After that, utilizing two different method of detection by applying (Convolution Neural Network with Principal Component Analysis) and (Convolution Neural Network without Principal Component Analysis) as a classifiers.

The results reveal that the use of CNN with PCA in this research results in acceptable accuracy. In contrast, using CNN only gave the highest level of accuracy in detecting manipulated images.

Keywords— Deep learning, Deep fake, Generative Adversarial Network, Convolution Neural Network, Principal Component Analysis.

1 Introduction

Due to the technological development and the wide spread of programs for deep fakes on digital images with the advent of Generative Adversarial Network (GAN). Image and video editing are becoming easier and considered a cybercrime due to the fake information and images can be spread fast and widely in Internet through social

media. Thus, deepfake can be considered as the ability to automatically create, modify, or swap a person's face in videos and images using algorithms depending on Deep Learning technology, that is one of the phenomena that is expanding quickly. It is feasible to produce top-notch results by developing new multimedia materials that are difficult for the human eye to distinguish between real and fake. This term "Deepfake" refers to all multimedia items that have been synthetically modified or produced using generative machine learning models [1]. DeepFake is concerning because it combines a high level of authenticity, quick evolution and pervasiveness [2]. On Reddit, DeepFake has been widely utilized as of November 2017. due to the United States widespread manufacturing of pornographic videos that has gained a solid online reputation and attracted interest of the people from all walks of life. In January DeepFake was officially used in an application in 2018.As a result DeepFake proliferation was accelerated. The object of face swapping has also grown in popularity from celebrities and politicians to students, friends and coworkers As a result, people's panic were naturally prompted. The main IT companies have also begun to collaborate action with the academic community to avoid additional detrimental impact on the fierce discussion about whether and how to control Deepfake technology [3].

With the continuous enhancement of the computing power of computer, the ongoing reduction of hardware price and the high integration of deep learning tools like tensorflow [4] and keras [5], technicians with specific professional backgrounds can produce high-quality faked images and videos consistent with the real distribution of data through the use of convolution automatic encoder [6] and Generative adversarial networks (GAN) [7]. Deepfake image as display in Figure 1

Fig. 1. Several illustrations of DeepFake: (a) Obama, made by Buzzfeed in cooperation with Monkeypaw Studios; (b) Mark Zuckerberg, made by artists Bill Posters and Daniel Howe in association with advertising company canny ; (c) Matteo Renzi,, made by “Striscia la Notizia[8].

2 Related work

1. Y. Wang et al in 2021 presented two algorithms for detection of fakeface images. The first approach is the Local Binary Pattern (LBP)-Net using global texture features used to detect fakefaces. The second method ensemble model constructed from five models including LBP-Net, Gram-Net, ResNet and two models utilizing InceptionResnetV1 pre-trained on Casia-Webfaceare and vggface2. Results of detecting fakeface images by several image augmentation such as downsample (66.32%), brightness (81.09%), Solarize (75.04%) ,Contrast (85.42%) and color (91.06%) when using "140K Real and Fake Faces"[[9].
2. M. Taeb et al in 2022 compared the most popular state-of-the-art face-detection classifiers such as CNN, VGG19, and DenseNet-121 using an enhanced actual and fakeface dataset. Data augmentation is a technique for improving performance with conserving computing resources. When compared to other studied models, early findings show that VGG19 has the best performance and accuracy of 95%. When using "140K Real and Fake Faces"[10].
3. S. Tariq and et al. in 2018 proposed an ensemble of three different convolution neural network with different layers as a classifier after performing pre-processing represented by face cropping and noise filtering methods. Finally a fully automated end-to-end fakeface detection pipeline developed to be focused on image content with only RGB channel information in order to recognize GAN-created face images with 94% AUROC score (Area Under the Receiver Operating Characteristic curve) and recognize human-created fake face images with 74.9 % AUROC score. Where, applied on CelebA and PGGAN dataset images. [11].
4. X. Chang et al in 2020 improved VGG network termed NA-VGG, it is used to detect deepfake face images, which was based on image noise and augmentation of image. The SRM filter layer is utilized to highlight the noise features of the image and after that the image noise is acquired as the network's input. Second, the image noise map is augmented to make the face features appear weaker. Finally, the augmented noise of images are fed into the network, which is trained and used to determine whether or not the image is fake. The obtained accuracy is 85.7 % when using the Celeb-DF dataset [12].

3 The workflow of the model

This project has been performed in five steps. The broad discussion of these stages is described here. The first stage is choosing the suitable real and fake images dataset from kaggel.com and preprocessing the dataset. following that, PCA applying for selecting images features after splitting the dataset by using cross-validation (hold-out) (80:20). The next stage is using (CNN) classifiers to classify the dataset. Finally evaluate performance of model using various metrics such as (accuracy, precision, recall, and F1-score). as showed in Figure 2.

Preprocessing step **Classification step**

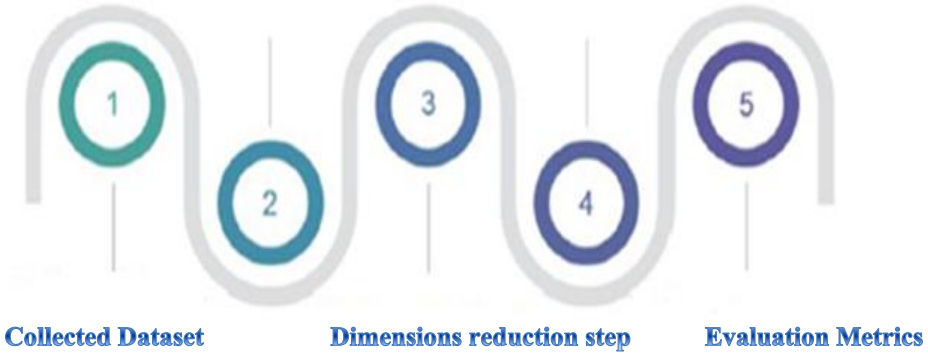


Fig. 2. Work design step of fake images detection.

The Proposed Deep Fake Detection

3.1 Dataset

Deepfake detection systems often use binary classifiers to group information into fake and real classes. This strategy needs a great quantity of high-quality authentic and manipulated data to train the models of classification. The dataset was taken from kaggle website. This dataset contains of all 70k real faces from of the Flickr dataset gathered by Nvidia, in addition 70k fake faces picked from the Bojan's 1 Million fake faces (produced using StyleGAN).

In this dataset, combined both dataset, scaled all of the images to 256px, and divided the data into three sets: train, validation and test set. also some CSV files available for convenience [13]. In this study, just two features (images and labels) are utilized to detect fake image classifiers. Label one represents fake images, whereas label zero represents true images.

Fig. 3. Samples of the dataset's real images

Fig. 4. Samples of the dataset's fake images

3.2 Pre-processing steps

In this section the results of the pre-processing of the images were reviewed, where six images were taken randomly from the dataset that was used in the proposed system.The first three represent the real images and the second three represent the fake ones, where the figure shows the results before and after the pre-processing. The first column represents the original images with RGB color space, while the second column represents the images conversion from RGB into YCbCr color space, the third column represents the images after entering the Gamma correction and finally the fourth

column represents the images after entering the Canny filter on them. As displayed in Figure 5.

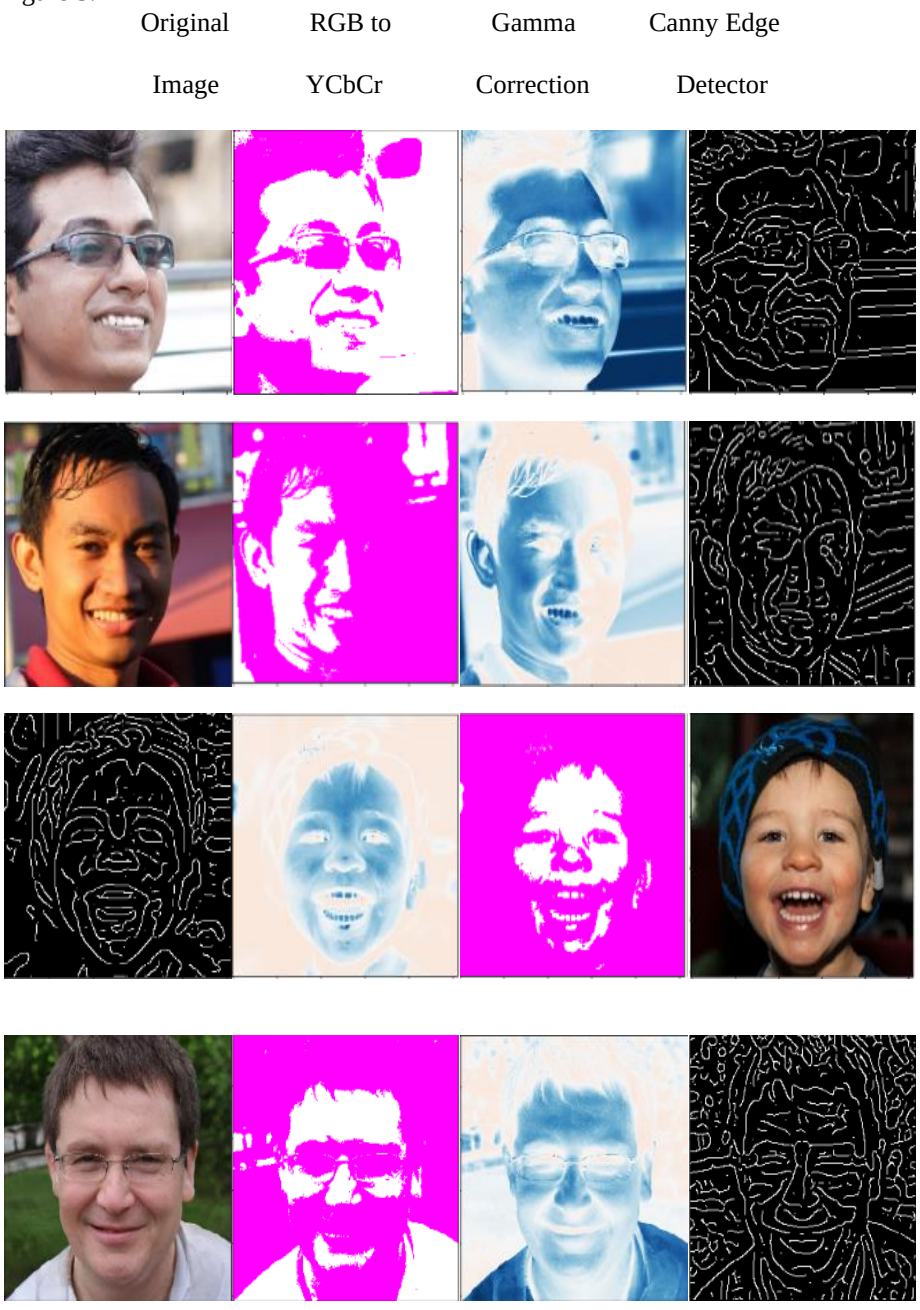


Fig. 5. Resulted of a preprocessing sample image from 140k Real and Fake Faces .

3.3 Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is one of the most widely statistical approaches used for feature selection. It has several uses in picture compression, text classification, and face recognition [14]. This is a frequently used method for reducing the dimensionality of a feature collection via a linear transformation. The main goal of PCA is to reduce the original variables to subset of variables by calculating the highest relationship of the original variables [15]. Although the resultant dataset is reduced, but the original data set's features are still retained and removed the redundancy of information [16] and [17]. The number of features in the new dataset may be equal to or lower than that in the original dataset. The principal components are computed by using the covariance matrix. The ability discriminative of the classifiers can be improved by using PCA .

The following steps summarize the process[18].

Let the training set of images {X1, X2, X3… XN}. Calculation of mean value of an image with equation:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} xi \qquad (1)$$

Information:

xi = data variable

n = numbers of data

Calculation of the mean value to reduce the dimension to be calculated in the next process.

2. Compute the covariance matrix to depict the scatter degree of all feature vectors connected to the average vector. The covariance matrix C is defined as follows:

$c = \frac{1}{n}\sum_{i=1}^{n}(xi - \bar{x})(xi - \bar{x})^T$ (2)

3. Calculate the Eigenvectors and eigenvalues from covariance matrix.

$CV = lV$ (3)

Where V is the set of eigenvectors correlated with its eigenvalue .

4. Sorts the eigenvector and eigenvalues from high to low based on the order of eigenvalues.

The main component k is the eigenvector corresponding to the largest eigenvalue.

The main component k of the vector x is observed using the equation:

$wi = vi^T(xi - \overline{x})$ *(4)*

Algorithm (1): Principal Component Analysis (PCA)
Input: Images Output: components
Begin Step 1: Form 2 dimensional matrix of independent variables X. Rows represent data items and columns represent features. The number of columns is the number of dimensions. Step 2: Subtract the mean of each column Step 3: Standardize your data Divide each value in a column by the column's standard deviation, which is the centered and standardized matrix Z. Step 4: Get Covariance of Z Estimate the covariance matrix of Z, $\text{CovMat} = \text{Z}^{\text{T}}\text{Z}$ Step 5: Calculate Eigen Vectors E and Eigen Values λ Step 6: Sort the Eigen Vectors Take the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda p$ and sort them from largest to smallest. In doing so, sort the eigenvectors in E accordingly. (For example, if λ3 is the largest eigenvalue, then take the third column of E and place it in the first column position.) Call this sorted matrix of eigenvectors E*. The columns of P* are the same as the columns of P in a different order. Note that these eigenvectors are independent of one another.

Step 7: Calculate the new features

Calculate Z* = ZE*.

Step 8: Drop unimportant features from the new set

Keep the first feature column to form (PCA).

END

3.4 Classifier

Convolutional Neural Networks is a type of Artificial Neural Net-work (ANN), also known as Conv-Nets or CNN, That is one of the most effective deep designs for classifying image data and many other applications, including audio recognition, object detection, medical image analysis and natural language processing[19]. The deep architecture of the network produces hierarchical feature extraction, wherein the trained filters of the first layer can be seen as a set of color dots or edges, of the second layer as some forms, the filter of the next layer may learn part of objects and the final layers filters may be able to recognize the objects. [20].

In the proposed method the design is carried out in two stages. Which starts first by training the model on the dataset consisting of real images and fake images. As for the second stage which is the testing stage, it is easy to distinguish the test image whether it is fake or real. One of the most common algorithms used in classification is a convolutional neural network (CNN) architecture by created a model from scratch with using six blocks in the CNN architecture. In each block utilize Conv2D with kernel size=5, Max Pooling, batch normalization=64, model = Sequential, dropout, activation = Relu, padding = same, epsilon=0.001, epochs = 100 One iteration on each training data set is represented as an epoch, verbose = 1, shuffle=True and to optimize the network using Adam optimizer = 0.001and a learning rate 0.0001. As discussed in Table 1.

Table 1. CNN architectures for deep fake detection of face image. Each row represents a block in the architecture. (Note: Conv=Conv2D, BN=BatchNormalization, DO=Dropout, MP=MaxPooling, F=Flatten, GAP=GlobalAveragePooling, D=Dense & S=Sigmoid)

Convolution Neural Network
Conv-ReLU-Padding-MP-BN
Conv-ReLU-Padding-MP-BN-DO
Conv-ReLU-Padding-MP-BN-DO
Conv-ReLU-Padding-MP-BN-DO

Conv-ReLU-Padding-MP-BN-DO
Conv-ReLU-Padding-MP-BN-DO
GAP-F-D-ReLU-DO
D- ReLU-DO-D-S

Once obtaining the features (components) the features are fed to Convolution Neural Network (CNN) layer of the deep learning model, which further selects the useful features by using their filters. The selected features are supplied to the max-pooling layer to choose the features that have the highest importance value throughout the computation. Gradients will be calculated, and the network's weights will automatically adjust.. We report our detection accuracy in result section.

3.5 Evaluation metrics

In order to evaluate the accuracy of algorithm's classification in detecting fake images, a number of evaluation metrics were used. The most commonly used measuring metric (Confusion Matrix) for detecting fake images has been applied in this part. It is possible to specify the metrics that the confusion matrix will use by defining this as a classification task. has as below [21].

$$Accuracy = \frac{TP+FP}{TP+TN+FP+FN} \quad [22]$$

$$Precision = \frac{TP}{TP+FP} \quad [23]$$

$$Recall = \frac{TP}{TP+FN} \quad [24]$$

$$F1\ Score = \frac{2* Precision*Recall}{Precision+Recal} \quad [25]$$

where TP represents (True Positive) and TN represent (True Negative). Moreover, FP is False positive, and FN is False-negative. As discussed in Table 2.

Table 2. Parameters of evaluation metrics

Parameters	Description
TP True Positive	The number of correctly classified records
TN True Negative	The number of the correctly rejected of records that have been classified
FP False Positive	The number of incorrectly classified records
FN False Negative	The number of the incorrectly rejected of records that have been classified

These measures are often used in a sequence of machine learning algorithms to evaluate the performance of a classifier from several estimations. Specifically, the accuracy measure, which quantifies the similarity between predicted and actual fake images.

Precision refers to the measuring of the fraction of the found fake images, that has been classified as fake, addressing the critical issue of the fake images classification. However, because to the dataset of fake images is typically skewed, good precision may be achieved by making a lower number of optimistic predictions, hence recall is used to assess sensitivity, or the fraction of annotated fake articles predicted as fake. It should be highlighted that higher values refers to better Recall, Precision, and Accuracy [26-29].Finally F1 score": Another term for it is the F Score or F Measure. The F1 score is a great balance of P and R [25].

4 Results and Discussion

According on the classification results showed that the accuracy of the model with pre-processing is CNN only without PCA and CNN with PCA classifier is 63.86% and 74.26%, respectively. Table 3, Table 4, Table 5, Table 6, Table 7 and Table 8 displays the resulted of confusion matrix with TP, FP, TN and FN values. Our experimental findings without preprocessing stages show that CNN only without PCA achieves 93.16% and CNN with PCA achieves 90.76%. Finally, an additional experiment was conducted by increasing the number of samples entering the CNN network (Training and Testing) which gave the highest accuracy results in image classification, so that the classification accuracy reached 98.04%.

(a) CNN without PCA with preprocessing

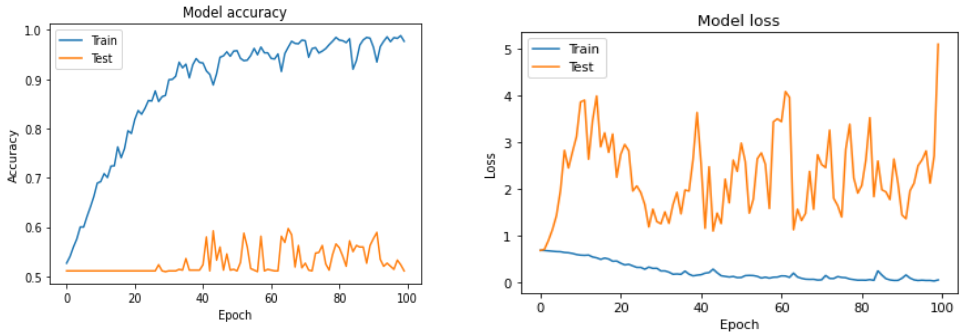


Fig. 6. The curves of the validation accuracy and loss during the training stage for the proposed CNN without PCA with preprocessing.

Table 3. Confusion matrix of the detection of deep fake on face image using CNN only without PCA with preprocessing

	Positive	Negative
Positive	1064	436
Negative	648	852

Accuracy =63.86
Precision=70.93
Recall=62.14
F1 Score=66.24

(b) CNN with PCA with preprocessing

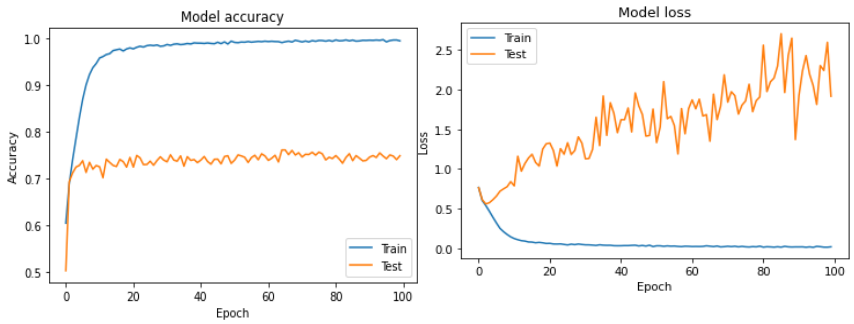


Fig. 7. The curves of the validation accuracy and loss during the training stage for the proposed CNN with PCA with preprocessing.

Table 4. Confusion matrix of the detection of deep fake on face image using CNN with PCA with preprocessing

	Positive	**Negative**
Positive	1144	356
Negative	416	1084

Accuracy =74.26
Precision=76.26
Recall=73.33
F1 Score=74.76

(c) CNN only without PCA on colored image

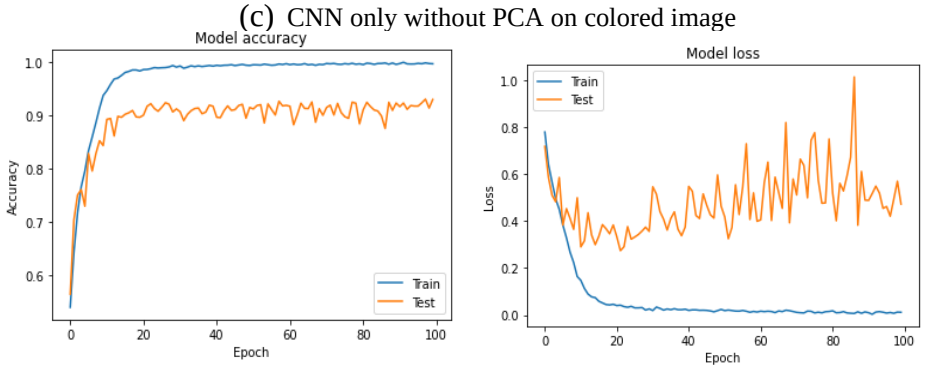


Fig. 8. The curves of the validation accuracy and loss during the training stage for the proposed CNN only.

Table 5. Confusion matrix of the detection of deep fake on face image using CNN only without PCA on colored image

	Positive	**Negative**
Positive	1414	86
Negative	119	1381

Accuracy =93.16
Precision=94.26
Recall=92.23
F1 Score=93.23

(d) CNN with PCA on colored image

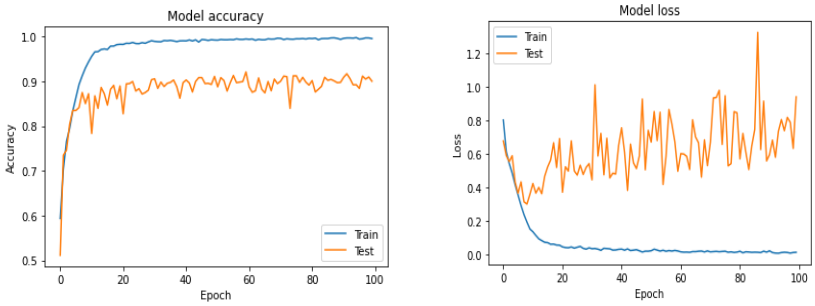


Fig. 9. The curves of the validation accuracy and loss during the training stage for the proposed CNN with PCA.

Table 6. Confusion matrix of the detection of deep fake on face image using CNN with PCA on colored image

	Positive	**Negative**
Positive	1373	127
Negative	150	1350

Accuracy =90.76
Precision=91.53
Recall=90.15
F1 Score=90.83

(e) CNN only without PCA on colored image

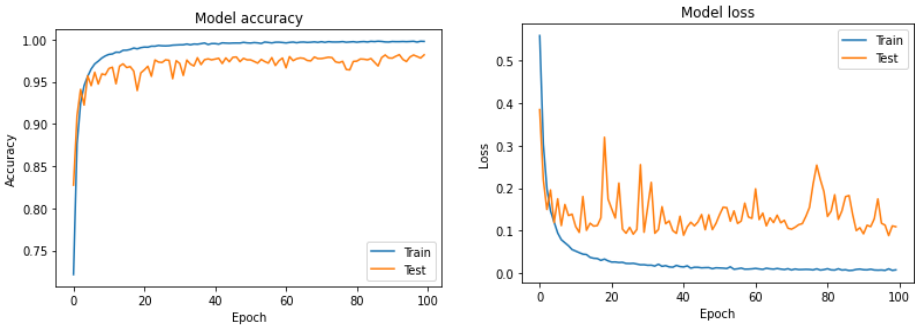


Fig. 10. The curves of the validation accuracy and loss during the training stage for the proposed CNN.

Table 7. Confusion matrix of the detection of deep fake on face image using CNN only without PCA on colored image

	Positive	**Negative**
Positive	7833	167
Negative	146	7854

Accuracy =98.04
Precision=97.91
Recall=98.17
F1 Score=98.03

(F) CNN with PCA on gray image

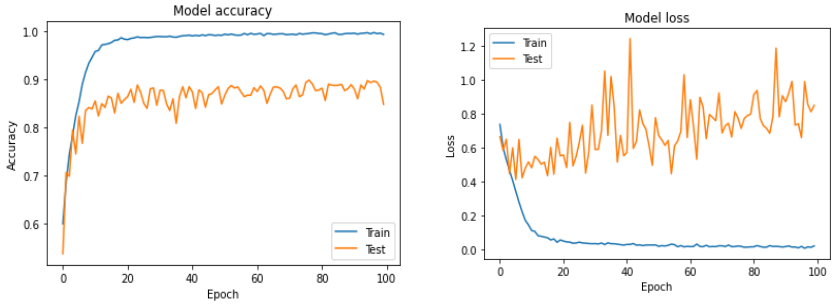


Fig. 11. proposed CNN with PCA on gray image.

Table 8. Confusion matrix of the detection of deep fake on face image using CNN with PCA on gray image

	Positive	**Negative**
Positive	1304	196

Negative	209	1291

Accuracy =86.5
Precision=86.93
Recall=86.18
F1 Score=86.55

In this section, the results were reviewed for implementing the proposed system and the results were as shown in the explanation below.

The research aims to reveal the manipulation that may be present in the images of faces, and therefore it was necessary for us to do a test stating that preserving the image entered into the system for the purpose of testing it and detecting the presence of manipulation in it first. As a result of the initial processing of the image, it may lead to the burial of some traces of manipulation in the image.

So we tested the image by using the technique involved the use of deep learning technology. In this case, we used successive steps for a simple preprocessing (determining the size of the image).

We clarified the image and reveal its edges before entering the tamper detection system.

We found that any preprocessing of the image, led to undesirable results compared to the results obtained without preprocessing.

Where the network of detection of manipulation in faces using the CNN classifier with the preprocessing and the use of canny Detection to detect edges was about 63.86

An additional experiment was used by adding the PCA method after the stage of preprocessing, which produced detection rates of 74.26% for the CNN classifier.

This indicates that the use of the PCA as a feature selector has improved the results of detection by a small percentage, but it is not high, because the work of the PCA depends on converting the data of the raw image entered into the detection system into components containing more information that spreads downward from the first component to the last component. The use of a limited set of component. Since the PCA was used in the form of a feature selector, it relied on the first components in the classification process by CNN, leaving the last components that contain information but are very weak and represent a burden on the classification process.

High classification rates and proof that any pre-processing on the image leads to changing or erasing the traces of manipulation encouraged the use of classification techniques approved by CNN, which is CNN with the PCA and without pre-processing, the detection rate of manipulation reached 90.76%., while detection rates using CNN only reached to 93.43. A new attempt was also used by inserting the CNN classifier with PCA on a gray scale image and the results were 86.5%.

Finally, CNN classifiers were used to detect forgery and applied to the images directly without using PCA and without any pre-processing, but with more data to see if the network is affected by the number of data that is trained on, and the classification results were 98.04% for the CNN classifier, which is the highest accuracy result in image classification It reached by the proposed system

This indicates that the use of PCA in the proposed system affected the accuracy of the results, and that the process of inserting direct images into the CNN classifier has

greatly benefited in the process of detecting fraud, as CNN needs a lot of information for the purpose of training and learning from it, regardless of the percentage of information contained in it. Pictures. CNN also made use of the images as more raw data. From the case that the PCA application has, that is, it made more use of the images than the components

5 Conclusion

The remarkable development of artificial intelligence and with the efficiency of the GAN in generating fake images that are closer to reality, it was necessary to find an efficient way to detect fake images. the final result of our research was to confront the phenomenon of Deepfake offered a detection model for the fake images by utilizing the most popular algorithm in deep learning is (Convolution Neural Network) to detect the fake images. The preprocessing steps start with converting images from RGB to YCbCr color space, after that entering the Gamma correction. finally extract edge detection by entering the Canny filter on them. After that, utilizing two different method of detection by applying (CNN with PCA) and (CNN without PCA) as a classifiers.

The achieved result is better than the listed related work, so utilizing this method enhances the accuracy of classification . From the above results, we conclude the following:

1. The CNN only is better than a CNN with PCA in the classification accuracy of fake images dataset.
2. CNN is more suitable for large datasets because the network efficiency increases with more data, that is, it gives better results as the training data increases
3. Preprocessing steps when using our dataset give worse results. These steps had a huge impact on decreasing classification accuracy.
4. The type of data used has a significant impact on the categorization accuracy of this work.

6 Reference

[1] Guarnera, Luca, Oliver Giudice, and Sebastiano Battiato. "Deepfake detection by analyzing convolutional traces." In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops*, pp. 666-667. 2020.

[2] Wang, L. S. "On the integrated regulation of “deep forgery”." *intelligent technology, Oriental Law*, 2019.

[3] Chang, Xu, Jian Wu, Tongfeng Yang, and Guorui Feng. "Deepfake face image detection based on improved VGG convolutional neural network." In *2020 39th chinese control conference (CCC)*, pp. 7252-7256. IEEE, 2020.

[4] Abadi, Martín, Paul Barham, Jianmin Chen, Zhifeng Chen, Andy Davis, Jeffrey Dean, Matthieu Devin et al. "{TensorFlow}: a system for {Large-Scale} machine learning." In *12th USENIX symposium on operating systems design and implementation (OSDI 16)*, pp. 265-283. 2016.

[5] Chollet, François. "keras. GitHub repository." *https://github. com/fchollet/keras>. Accessed on* 25 (2015): 2017.

[6] Tewari, Ayush, Michael Zollhofer, Hyeongwoo Kim, Pablo Garrido, Florian Bernard, Patrick Perez, and Christian Theobalt. "Mofa: Model-based deep convolutional face autoencoder for unsupervised monocular reconstruction." In *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 1274-1283. 2017.
[7] Antipov, Grigory, Moez Baccouche, and Jean-Luc Dugelay. "Face aging with conditional generative adversarial networks." In *2017 IEEE international conference on image processing (ICIP)*, pp. 2089-2093. IEEE, 2017.
[8] Guarnera, Luca, Oliver Giudice, Cristina Nastasi, and Sebastiano Battiato. "Preliminary forensics analysis of deepfake images." In *2020 AEIT international annual conference (AEIT)*, pp. 1-6. IEEE, 2020.
[9] Wang, Yonghui, Vahid Zarghami, and Suxia Cui. "Fake Face Detection using Local Binary Pattern and Ensemble Modeling." In *2021 IEEE International Conference on Image Processing (ICIP)*, pp. 3917-3921. IEEE, 2021.
[10] Taeb, Maryam, and Hongmei Chi. "Comparison of Deepfake Detection Techniques through Deep Learning." *Journal of Cybersecurity and Privacy* 2, no. 1, 2022.
[11] Tariq, Shahroz, Sangyup Lee, Hoyoung Kim, Youjin Shin, and Simon S. Woo. "Detecting both machine and human created fake face images in the wild." In *Proceedings of the 2nd international workshop on multimedia privacy and security*, pp. 81-87. 2018.
[12] Chang, Xu, Jian Wu, Tongfeng Yang, and Guorui Feng. "Deepfake face image detection based on improved VGG convolutional neural network." In *2020 39th chinese control conference (CCC)*, pp. 7252-7256. IEEE, 2020.
[13] xhlulu. 140k Real and Fake Faces [Dataset]. https://www.kaggle.com/xhlulu/140k-real-and-fake-faces 2020.
[14] Taloba, Ahmed I., Dalia A. Eisa, and Safaa SI Ismail. "A comparative study on using principle component analysis with different text classifiers." *arXiv preprint arXiv:1807.03283*, 2018.
[15] Karamizadeh, Sasan, Shahidan M. Abdullah, Azizah A. Manaf, Mazdak Zamani, and Alireza Hooman. "An overview of principal component analysis." *Journal of Signal and Information Processing* 4, 2020.
[16] Ahmad, Muhammad, Adil Mehmood Khan, Joseph Alexander Brown, Stanislav Protasov, and Asad Masood Khattak. "Gait fingerprinting-based user identification on smartphones." In *2016 International Joint Conference on Neural Networks (IJCNN)*, pp. 3060-3067. IEEE, 2016.
[17] Ahmad, Muhammad, Dr Ihsan Ul Haq, Qaisar Mushtaq, and Muhammad Sohaib. "A new statistical approach for band clustering and band selection using K-means clustering." *Int. J. Eng. Technol* 3, no. 6, 2011
[18] Arjun, V. MANE, Ramesh R. MANZA, and V. KALE Karbhari. "Human face recognition using superior principal component analysis (SPCA)." *International Journal of Computer Theory and Engineering* 2, no. 5, 2010
[19] Traore, Boukaye Boubacar, Bernard Kamsu-Foguem, and Fana Tangara. "Deep convolution neural network for image recognition." *Ecological Informatics* 48, 2018
[20] Aloysius, Neena, and M. Geetha. "A review on deep convolutional neural networks." In *2017 international conference on communication and signal processing (ICCSP)*, pp. 0588-0592. IEEE, 2017.
[21] Ali, Jehad, Rehanullah Khan, Nasir Ahmad, and Imran Maqsood. "Random forests and decision trees." *International Journal of Computer Science Issues (IJCSI)* 9, no. 5, 2012.
[22] SHAHANE, PRIYANKA, and DEIPALI GORE. "Detection of Fake Profiles on Twitter using Random Forest & Deep Convolutional Neural Network, International Journal of Management, Technology And Engineering, 2019.

[23] Allcott, Hunt, and Matthew Gentzkow. "Social media and fake news in the 2016 election." *Journal of economic perspectives* 31, no. 2, 2017.
[24] Gilda, Shlok. "Notice of violation of IEEE publication principles: Evaluating machine learning algorithms for fake news detection." In *2017 IEEE 15th student conference on research and development (SCOReD)*, pp. 110-115. IEEE, 2017.
[25] Han, J., Kamber, M. and Pei, J. "Data mining concepts and techniques third edition," *The Morgan Kaufmann Series in Data Management Systems*, 5(4), pp. 83–124 . 2011.
[26] Al-ogaili, H. and A.M. Shadhar, *the Finger Vein Recognition Using Deep Learning Technique.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 1-11.
[27] Al Mossawy, M.M.T. and L.E. George, *A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(1): p. 1-14.
[28] 5. Ahmed, H., *A Review of Hash Function Types and their Applications.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 120-139.
[29] Shu, Kai, Amy Sliva, Suhang Wang, Jiliang Tang, and Huan Liu. "Fake news detection on social media: A data mining perspective." *ACM SIGKDD explorations newsletter* 19, no. 1, 2017.

Article submitted 7 December 2022. Published as resubmitted by the authors 27 December 2022.

Data hiding by using AES Algorithm

https://doi.org/10.31185/wjcm.82

Prof. Dr.Rafidah Mohamad(✉)
Faculty of Computer Science and Information Systems, Universiti Malaya (UM),Malaysia.
rfid @um.edu.my

Abstract—Data hiding is the art of hiding data for various purposes such as; to maintain private data, secure confidential data and so on. Securely exchange the data over the internet network is very important issue. So, in order to transfer the data securely to the destination, there are many approaches like cryptography and steganography. In this research we propose an AES algorithm for embedding the data into the images which is implemented through the Microsoft .NET framework using the C#.NET.

Keywords—Data hiding, AES, encryption, decryption

1 Introduction

The growing use of Internet needs to take attention while we send and receive personal information in a secured manner. For this, there are many approaches that can transfer the data into different forms so that their resultant data can be understood if it can be returned back into its original form. This technique is known as encryption. However, a major disadvantage of this method is that the existence of data is not hidden. If someone gives enough time then the unreadable encrypted data may be converted into its original form[1]. A solution to this problem has already been achieved by using a “steganography” technique to hide data in a cover media so that other cannot notice it. The characteristics of the cover media depends on the amount of data that can be hidden, the perceptibility of the message and its robustness. In this document, I propose a new system for hiding data stands on many methods and algorithms for image hiding where I store on data file, called sink file in an image file called as container image. The primary objective is to use steganography techniques so as to provide more security and simultaneously using less storage.

This research addresses the security problem of transmitting the data over internet network, the main idea coming when we start asking that how can we send a message secretly to the destination? The science of steganography answers this question. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos and data transmissions. In this document, we proposed some methods and algorithms of an image steganography system to hide a digital text of a secret message[2].

In this project, we propose to develop a system to hiding data by using "STEGANOGRAPHY" technique as I used many methods stands on some techniques to have at the back-end a software for hiding data based on hiding algorithms[3].

After studying the data hiding algorithms, we found many ways to hiding data by using the multimedia files and the main question for me was "Where hidden data hides?" as we found by our search to know where the data hides it's important to know what is the file type of the data that it shall be hidden and the cover file type so it is possible to alter graphic or sound files slightly without losing their overall viability for the viewer and listener.

With audio, you can use bits of file that contain sound not audible to the human ear. With graphic images, you can remove redundant bits of color from the image and still produce a picture STEGANOGRAPHY USING IMAGES that looks intact to human eye and is difficult to discern from its original. It is in those bits that stego hides its data.

By the final of our research we developed a software uses an algorithm, to embed data in an image; The purposed system is called "Steganography", the aim of this research his to encrypt the data; the meaning of encrypt is to hide the data over an image using different steganographic algorithms, in this system AES is the algorithms that we use to hiding the data [4].

2 Literature

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security. It is not intended to replace cryptography but supplement it. [5] Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection.

Therefore, some Steganographic methods combine traditional Cryptography with Steganography; the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover. It has been used through the ages by ordinary people, spies, rulers, government, and armies. There are many stories about Steganography. [6] For example, ancient Greece used methods for hiding messages such as hiding In the field of Steganography, some terminology has developed. The adjectives 'cover', 'embedded', and 'stego' were defined at the information hiding workshop held in Cambridge, England. The term "cover" refers to description of the original, innocent massage, data, audio, video, and so on. Steganography is not a new science; it dates back to ancient times. [7] Hidden information in the cover data is known as the "embedded" data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content. The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret. [1] Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. This technique has recently become important in a number of application areas. For example, digital video, audio,

and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent. [8] Research in information hiding has tremendous increased during the past decade with commercial interests driving the field. Although the art of concealment “hidden information” as old as the history, but the emergence of computer and the evolution of sciences and techniques breathe life again in this art with the use of new ideas, techniques, drawing on the computer characteristics in the way representation of the data, well-known computer representation of all data including (Multimedia) is binary these representations are often the digital levels and areas and change values-aware of slight not aware or felt by Means sensual of human such as hearing, sight, the advantage use of these properties to hide data in multimedia by replace the values of these sites to the values of data to be hidden, taking into account the acceptable limits for the changeover, and not exceeded to prevent degradation media container with a change becomes aware and felt by human [9-19]. It should be noted here that although the art of hidden information come in the beginning of the computer and its techniques However, the seriousness of the work in the stenography as a stand-alone science started in 1995.

3 Methodology

In the proposed system we concentrate on finding some algorithm to hide the data inside images using steganography technique. An algorithm is designed to hide all the data inputted within the image to protect the privacy of the data. Then, the system is developed based on the new steganography algorithm.

This proposed system provides the user with two options encrypt and decrypt the data, in encryption the secret information is hiding in with image file, and on the other side the decryption is getting the hidden information from the stego image file, and also the user can show the image size after and before the encryption.

The processes of encryption and decryption of the data file consists of:

- Providing security for the data to be transmitted through network using steganography.
- Proposing an approach for hiding the data within an image using astegano graphic algorithm which provides better accuracy and quality of hiding.

Microsoft Techniques is used through the .NET framework to extensively analyze the functions of the ASE algorithm in steganography. Texts and other file formats are encrypted and embedded into an image file which is then transferred to the destination.

4 ASE Algorithms

The Advanced Encryption Standard (AES), also known by its original name Rijndael (Dutch pronunciation: [ˈrɛindaːl]),is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a variant of the Rijndael block cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001. This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see Advanced Encryption Standard process for more details).AES is included in the ISO/IEC 18033-3 standard. AES became effective as a U.S. federal government standard on May 26, 2002, after approval by the U.S. Secretary of Commerce. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the U.S. National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES, below).

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement

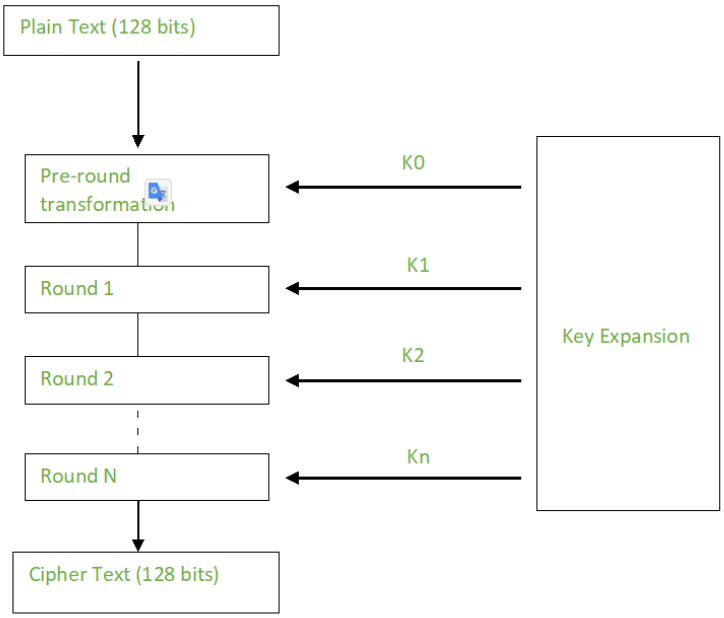
- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]

Each round comprises of 4 steps:



- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes: This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows: This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]
| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |

[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

Mix Columns:

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

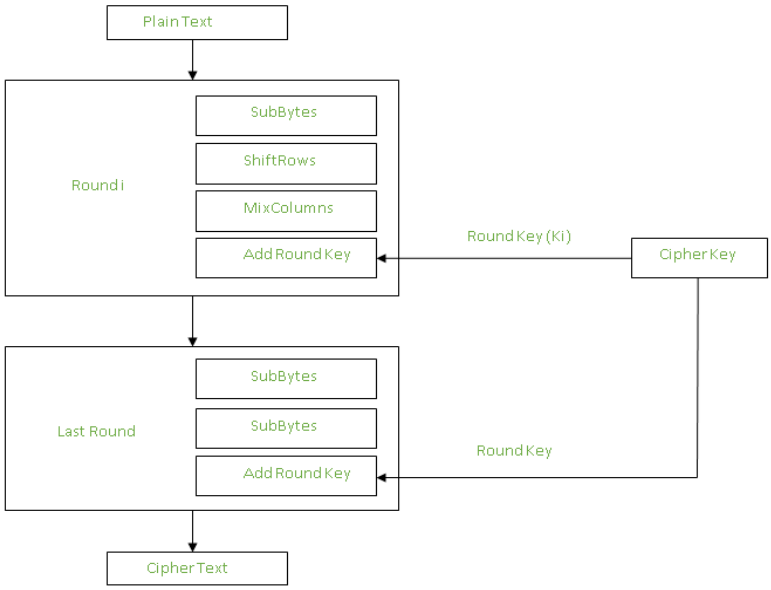
This step is skipped in the last round.

[c0] [2 3 1 1] [b0]
| c1 | = | 1 2 3 1 | | b1 |
| c2 | | 1 1 2 3 | | b2 |
[c3] [3 1 1 2] [b3]

Add Round Keys :

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.



The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse Mix Columns :

This step is similar to the Mix Columns step in encryption, but differs in the matrix used to carry out the operation.

[b0] = [14 11 13 9] [c0]
| b1 | = | 9 14 11 13 | | c1 |
| b2 | = | 13 9 14 11 | | c2 |
[b3] = [11 13 9 14] [c3]

Inverse Sub Bytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

AES instruction set is now integrated into the CPU (offers throughput of several GB/s) to improve the speed and security of applications that use AES for encryption and decryption. Even though it's been 20 years since its introduction we have failed to break the AES algorithm as it is infeasible even with the current technology. Till date the only vulnerability remains in the implementation of the algorithm.

5 CONCLUSIONS

Although only some of the main image steganographic techniques were discussed in this document, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (AES) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

The proposed approach in this research uses a new steganographic approach called image steganography. The application creates a stego image in which the personal data is embedded inside the cover file image.

Used the Advanced Encryption Standard algorithm in this research for developing the application which is faster and reliable and compression ratio is moderate compared to other algorithms.

6 References

[1] Rosziati Ibrahim and Teoh Suk Kuan, Steganography Imaging System (SIS): Hiding Secret Message inside an Image http://www.iaeng.org/publication/WCECS2010/WCECS2010_pp144-148.pdf

[2] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, Overview: Main Fundamentals for Steganography http://arxiv.org/ftp/arxiv/papers/1003/1003.4086.pd

[3] Bere Sachin Sukhadeo, User Aware Image Tag Refinement http://www.ijcsmr.org/eetecme2013/paper19.pdf

[4] Youssef Bassil , A Simulation Model for the Waterfall Software Development Life Cycle, 2011 http://arxiv.org/ftp/arxiv/papers/1205/1205.6904.pdf
[5] Neamah, A. F. (2021, March). Adoption of Data Warehouse in University Management: Wasit University Case Study. In Journal of Physics: Conference Series (Vol. 1860, No. 1, p. 012027). IOP Publishing.
[6] Neamah, A. F., & Abd Ghani, M. K. (2018). Adoption of E-Health records management model in health sector of Iraq. Indian Journal of Science and Technology, 11(30), 1-20.
[7] Donald S. Le Vie, Jr., Understanding Data Flow Diagrams http://ratandon.mysite.syr.edu/cis453/notes/DFD_over_Flowcharts.pdf
[8] B. Beizer, Software Testing Techniques. London: International Thompson Computer Press, 1990.
[9] Asgarnezhad, R., et al., An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems. Wasit Journal of Computer and Mathematics Science, 2022. 1(1): p. 27-35.
[10] Farhan, R.I., A.T. Maolood, and N. Hassan, Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS. Wasit Journal of Computer and Mathematics Science, 2021: p. 66-83.
[11] Salim, H.T., et al., Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN. International Journal of Interactive Mobile Technologies, 2022. 16(8).
[12] H.T.H., Enhanced Data Security of Communication System using Combined Encryption and Steganography. International Journal of Interactive Mobile Technologies, 2021. 15(16): p. 144-157.
[13] Al_airaji, R.a.M., et al., Automated Cheating Detection based on Video Surveillance in the Examination Classes. International Journal of Interactive Mobile Technologies, 2022. 16(8).
[14] Meteab, W.K., et al. Controlling and Monitoring a Robot-Car Based on Smart Phone Applications. in IOP Conference Series: Materials Science and Engineering. 2021. IOP Publishing.
[15] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
[16] Hassan, H.A., Review Vehicular Ad hoc Networks Security Challenges and Future Technology. Wasit Journal of Computer and Mathematics Science, 2022. 1(3).
[17] Al Mossawy, M.M.T. and L.E. George, A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System. Wasit Journal of Computer and Mathematics Science, 2022. 1(1): p. 1-14.
[18] Jaafar Q. K. , Aljazaery.I. A., Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT. International Journal of Emerging Technologies in Learning (iJET), 2023. 18(02).
[19] B. Beizer, Black Box Testing. New York: John Wiley & Sons, Inc., 1995.

Article submitted 16 November 2022. Published as resubmitted by the authors 28 December 2022.

Features and characters for distributed system

https://doi.org/10.31185/wjcm.89

Prof. Dr. Paul Mccullagh(✉)
School of Computing, Ulster University, United Kingdom.
Paul-mcc@uls.edu.uk

Abstract— The introduction of microprocessors had created a number of product options that were just not there before. These clever processors have infiltrated and dispersed themselves across every aspect of our life, whether it be in the office (fax machines, pagers, laser printers, credit card readers), living rooms (televisions, air conditioners), or kitchens (food processors, microwave ovens). The usage of an operating system has many benefits as distributed applications get more complicated. The real-time demands of the majority of distributed systems need the usage of Real Time Operating Systems (RTOS) that can fulfill the needs of distributed systems. Real-time applications can be readily built and expanded thanks to RTOS. Through the division of the application code into different files, the use of RTOS streamlines the design process.

Keywords— OS, Real time, embedded system, distributed system.

1 Introduction

A distributed system is a specialized computer system that is part of a larger system or machine. Distributed systems can also be thought of as information processing subsystems integrated in a larger system [2]. As part of a larger system, it largely determines its functionality. An distributed system usually contains an distributed processor. Many appliances that have a digital interface (microwaves, cars) utilize distributed systems. Distributed systems also can be defined as computing systems with tightly coupled hardware and software that are designed to perform a dedicated function [5]. This combination of computer hardware and software, either fixed in capability or programmable, that is specifically designed for a particular kind of application device [6]. The word distributed reflects the fact that these systems are usually an integral part of a larger system. Some distributed systems include an operating system. Others are very specialized resulting in the entire logic being implemented as a single program. These systems are distributed into some device for some specific purpose other than to provide general purpose computing. A typical distributed system is shown in figure[2].

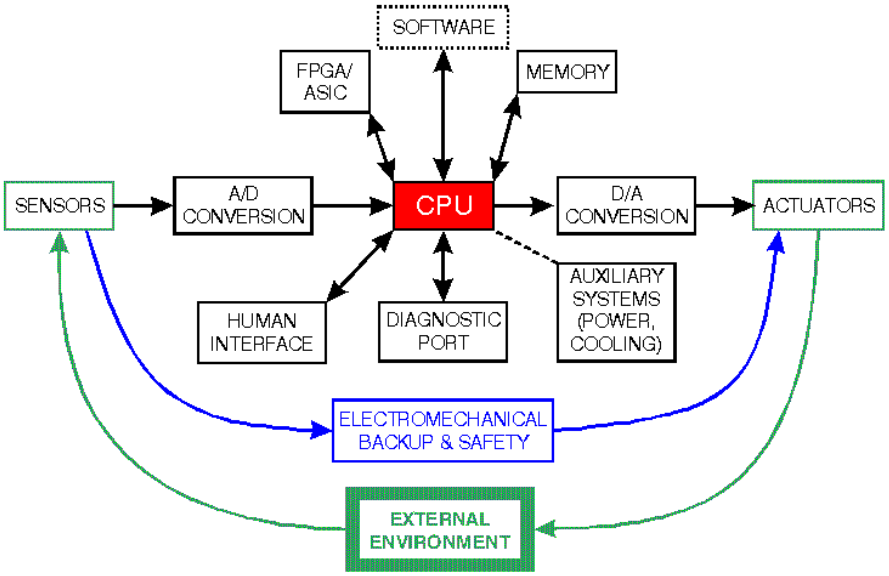


Fig. 1. A Typical Distributed System

Tracing back the history, the birth of microprocessor in 1971 marked the booming of digital era. Early distributed applications included unmanned space probes, computerized traffic lights and aircraft flight control systems. In the 1980s, distributed systems brought microprocessors into every part of our personal and professional lives. Presently there are numerous gadgets coming out to make our life easier and comfortable because of advances in distributed systems [5, 7]. Distributed systems vary considerably. Some are general-purpose computers, running standard operating systems—such as UNIX—with special-purpose applications to implement the functionality. Others are hardware devices with a special-purpose distributed operating system providing just the functionality desired. Yet others are hardware devices with application-specific integrated circuits (ASICs) that perform their tasks without an operating system [1].

There are over 3 billion distributed CPUs sold each year. Distributed CPUs are growing at a faster rate than desktop processors. A large part of this growth is in smaller (4-, 8-, and 16-bit) CPUs and digital signal processors (DSPs) [2].

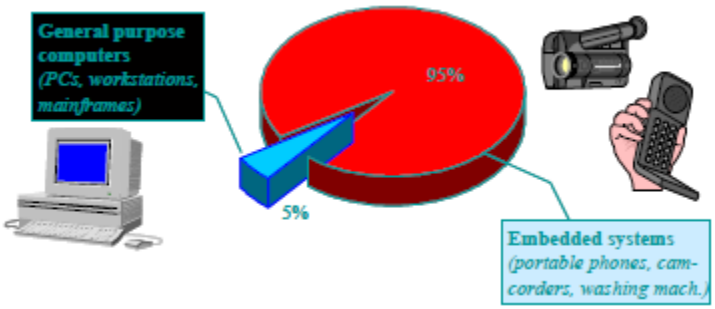


Fig. 2. Distributed systems dominate the microprocessor landscape

Distributed systems provide several functions, some of these functions are:

- **Monitor the environment;** distributed systems read data from input sensors. This data is then processed and the results displayed in some format to a user or users.
- **Control the environment;** distributed systems generate and transmit commands for actuators.
- **Transform the information;** distributed systems transform the data collected in some meaningful way, such as data compression/decompression.

Although interaction with the external world via sensors and actuators is an important aspect of distributed systems, as show in Figure, these systems also provide functionality specific to their applications. Distributed systems typically execute applications such as control laws, finite state machines, and signal processing algorithms. These systems must also detect and react to faults in both the internal computing environment as well as the surrounding electromechanical systems [2].

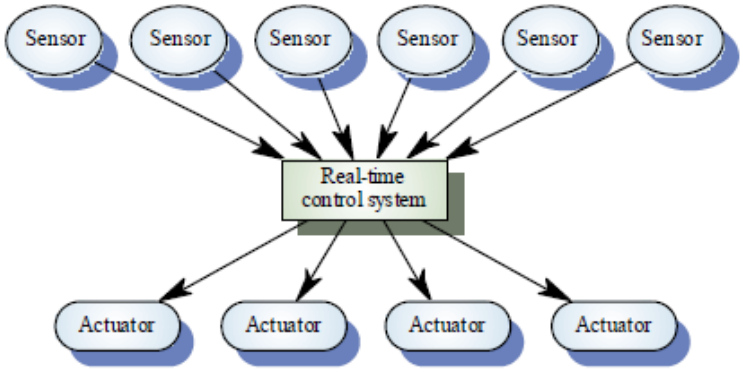


Fig. 3. Sensors and Actuators in an Distributed System

There are many categories of distributed systems, from communication devices to home appliances to control systems. Examples of distributed system include;

- Communication devices (modems, cellular phones)
- Home Appliances (CD player, microwave oven)
- Control Systems (Automobile anti-lock braking systems, robotics, and satellite control).

2 Characteristics of Distributed Systems

Distributed systems are characterized by a unique set of characteristics. Each of these characteristics imposed a specific set of design constraints on distributed systems designers. The challenge to designing distributed systems is to conform to the specific set of constraints for the application.

2.1 Application Specific Systems

Distributed systems are not general-purpose computers. Distributed system designs are optimized for a specific application. Many of the job characteristics are known before the hardware is designed. This allows the designer to focus on the specific design constraints of a well defined application. As such, there is limited user reprogram ability. Some distributed systems, however, require the flexibility of reprogram ability. Programmable DSPs are common for such applications.

2.2 Reactive *Systems*

As mentioned earlier, a typical distributed systems model responds to the environment via sensors and control the environment using actuators. This requires distributed systems to run at the speed of the environment. This characteristic of distributed system is called “reactive”. Reactive computation means that the system (primarily the software component) executes in response to external events. External events can be either periodic or aperiodic. Periodic events make it easier to schedule processing to guarantee performance. Aperiodic events are harder to schedule. The maximum event arrival rate must be estimated in order to accommodate worst case situations. Most distributed systems have a significant reactive component. One of the biggest challenges for distributed system designers is performing an accurate worst case design analysis on systems with statistical performance characteristics (e.g., cache memory on a DSP or other distributed processor). Real time system operation means that the correctness of a computation depends, in part, on the time at which it is delivered. Systems with this requirement must often design to worst case performance. But accurately predicting the worst case may be difficult on complicated architectures. This often leads to overly pessimistic estimates erring on the side of caution. Many distributed systems have a significant requirement for real time operation in order to meet external I/O and control stability requirements.

2.3 Distributed *Systems*

A common characteristic of an distributed system is one that consists of communicating processes executing on several CPUs or Application-specific integrated circuits (ASICs) which are connected by communication links. The reason for this is economy. Economical 4 8-bit microcontrollers may be cheaper than 32 bit processors. Even after adding the cost of the communication links, this approach may be preferable. In this approach, multiple processors are usually required to handle multiple time-critical tasks. Devices under control of distributed systems may also be physically distributed. ***4. Heterogeneous Architectures*** Distributed systems often are composed of heterogeneous architectures, [2].

They may contain different processors in the same system solution. They may also be mixed signal systems. The combination of I/O interfaces, local and remote memories, and sensors and actuators makes distributed system design truly unique. Distributed systems also have tight design constraints, and heterogeneity provides better design flexibility.

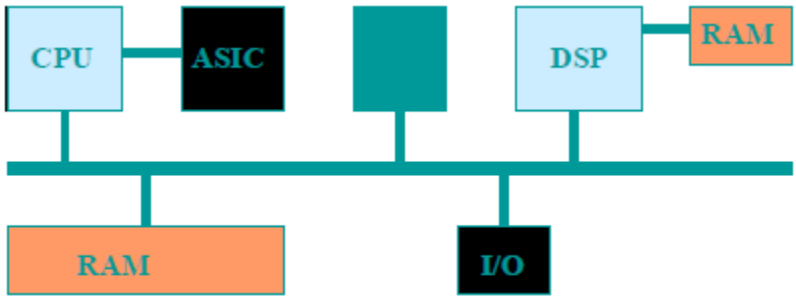


Fig. 4. Distributed Systems have Heterogeneous Architectures.

2.4 Harsh *environment*

Many distributed systems do not operate in a controlled environment. Excessive heat is often a problem, especially in applications involving combustion (e.g., many transportation applications). Additional problems can be caused for distributed computing by a need for protection from vibration, shock, lightning, power supply fluctuations, water, corrosion, fire, and general physical abuse. For example, in the Mission Critical example application the computer must function for a guaranteed, but brief, period of time even under non-survivable fire conditions. These constraints present a unique set of challenges to the distributed system designer, including accurately modeling the thermal conditions of these systems.

2.5 System *safety and reliability*

As distributed system complexity and computing power continue to grow, they are starting to control more and more of the safety aspects of the overall system. These safety measures may be in the form of software as well as hardware control. Mechanical safety backups are normally activated when the computer system loses control in order to safely shut down system operation. Software safety and reliability is a bigger issue. Software doesn't normally "break" in the sense of hardware. However software may be so complex that a set of unexpected circumstances can cause software failures leading to unsafe situations. The challenges for distributed designers include designing reliable software and building cheap, available systems using unreliable components. The main challenge for distributed system designers is to obtain low-cost reliability with minimal redundancy.

2.6 Control *of physical systems*

One of the main reasons for embedding a computer is to interact with the environment. This is often done by monitoring and controlling external machinery. Distributed computers transform the analog signals from sensors into digital form for processing. Outputs must be transformed back to analog signal levels. When controlling physical equipment, large current loads may need to be switched in order to operate motors and other actuators. To meet these needs, distributed systems may need large computer circuit boards with many non-digital components. Distributed system designers must carefully balance system tradeoffs among analog components, power, mechanical, network, and digital hardware with corresponding software.

2.7 *Small and low weight*

Many distributed computers are physically located within some larger system. The form factor for the distributed system may be dictated by aesthetics. For example, the form factor for a missile may have to fit inside the nose of the missile. One of the challenges for distributed systems designers is to develop non-rectangular geometries for certain solutions. Weight can also be a critical constraint. Distributed automobile control systems, for example, must be light weight for fuel economy. Portable CD players must be light weight for portability purposes.

2.8 *Cost sensitivity*

Cost is an issue in most systems, but the sensitivity to cost changes can vary dramatically in distributed systems. This is mainly due to the effect of computer costs have on profitability and is more a function of the proportion of cost changes compared to the total system cost.

2.9 Power management

Distributed systems have strict constraints on power. Given the portability requirements of many distributed systems, the need to conserve power is important to maintain battery life as long as possible. Minimization of heat production is another obvious concern for distributed systems.

3 Structure of *Distributed* Systems

All distributed systems contain a processor and software. The processor may be 8051 micro-controller or a Pentium-IV processor (having a clock speed of 2.4 GHz). Certainly, in order to have software there must be a place to store the executable code and temporary storage for run-time data manipulations. These take the form of ROM and RAM respectively. If memory requirement is small, it may be contained in the same chip as the processor. Otherwise one or both types of memory will reside in external memory chips. All distributed systems also contain some type of inputs and outputs, see Figure [5]. For example in a microwave oven the inputs are the buttons on the front panel and a temperature probe and the outputs are the human readable display and the microwave radiation. Inputs to the system generally take the form of sensors and probes, communication signals, or control knobs and buttons. Outputs are generally displays, communication signals, or changes to the physical world.

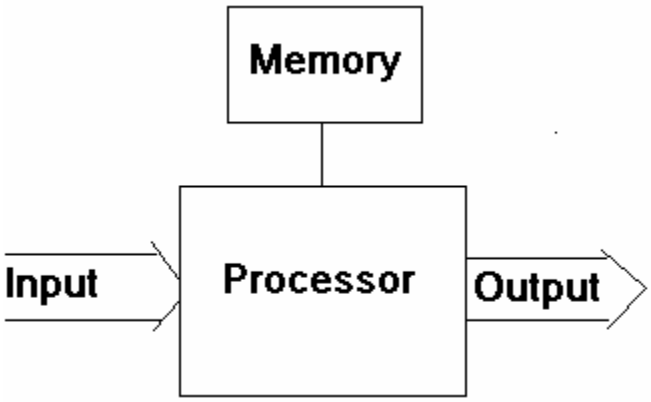


Fig. 5. Generic Distributed system.

Real-time scheduling is the process of creating start and finish times for sets of tasks such that all timing, precedence, and resource constraints are met. Real-time scheduling results in recent years have been extensive. Theoretical results have identified worst-case bounds for dynamic on-line algorithms, and complexity results have been produced for various types of assumed task-set characteristics [9-23]. Memory management capabilities are necessary in some systems to provide memory protection and

virtual memory. Special purpose interfaces are also needed to support a variety of external peripheral devices, energy consumption control, and so on. Commonly both the hardware and the software for an distributed system are developed in parallel. Constant design feedback between the two design teams should occur in this development model. The result is that each side can take advantage of what the other can do. The software component can take advantage of special hardware features to gain performance. The hardware component can simplify module design if functionality can be achieved in software that reduces overall hardware complexity and cost. As real-time distributed systems became more complex and software advanced from structured programming to object-oriented methodologies, new modeling tools were needed. Unified Modeling Language (UML) was developed in response to the need for a standardized object modeling language. UML can be adapted to design a variety of real-time systems, from small 8-bit microcontroller systems to large multi-processor networked systems. UML includes features for modeling functionality, objects, states, design patterns and extensibility features [10].

One class of distributed processors focuses on size, power consumption, and price. Therefore, some distributed processors are limited in functionality, i.e., a processor is good enough for the class of applications for which it was designed but is likely inadequate for other classes of applications. This is one reason why many distributed processors do not have fast CPU speeds. For example, the processor chosen for a personal digital assistant (PDA) device does not have a floating-point co-processor because floating-point operations are either not needed or software emulation is sufficient. The processor might have a 16-bit addressing architecture instead of 32- bit, due to its limited memory storage capacity. It might have a 200MHz CPU speed because the majority of the applications are interactive and display-intensive, rather than computation intensive. This class of PAD are small because the overall PDA device is slim and fits in the palm of your hand. The limited functionality means reduced power consumption and long-lasting battery life. The smaller size reduces the overall cost of processor fabrication. On the other hand, another class of distributed processors focuses on performance. These distributed processors are powerful and packed with advanced chip-design technologies, such as advanced pipeline and parallel processing architecture. These processors are designed to satisfy those applications with intensive computing requirements not achievable with general-purpose processors. An emerging class of highly specialized and high-performance distributed processors includes network processors developed for the network equipment and telecommunications industry. Overall, system and application speeds are the main concerns.

Yet another class of distributed processors focuses on all four requirements—performance, size, power consumption, and price. Take, for example, the distributed digital signal processor (DSP) used in cell phones. Real-time voice communication involves digital signal processing and cannot tolerate delays. A DSP has specialized arithmetic units, optimized design in the memory, and addressing and bus architectures with multiprocessing capability that allow the DSP to perform complex calculations extremely fast in real time. A DSP outperforms a general-purpose processor running at the same clock speed many times over comes to digital signal processing. These reasons are why DSPs, instead of general-purpose processors, are chosen for cell phone designs.

Even though DSPs are incredibly fast and powerful distributed processors, they are reasonably priced, which keeps the overall prices of cell phones competitive. The battery from which the DSP draws power lasts for hours and hours [10].

4 Distributed Application's features

Distributed applications have some common features such as the following [10]: ***Limited resources***: There are often strong limitations regarding available resources. Mainly due to cost and size constraints related to mass production and strong industrial competition, the system resources as CPU, memory, devices have been designed to meet these requirements. As a result of these limitations, the system has to deal with an efficient use of the computational resources. ***Real-time application requirements***: Some of the applications to be run in these devices have temporal requirements. These applications are related with process control, multimedia processing, instrumentation, and so on, where the system has to act within a specified interval. ***Distributed control systems:*** Most of the distributed systems perform control activities involving input data acquisition (sensing) and output delivery (actuation). Deterministic communications are also another important issue. ***Quality of service:*** An efficient use of the system resources is a must in distributed systems. Feedback based approaches are being used to adjust the performance or quality of service of the applications as a function of the available resources.

The challenge is how to implement applications that can execute efficiently on limited resource and that meet nonfunctional requirements such as timeliness, robustness, dependability, performance, and so on. Within the exception of these few common features, rest of the distributed hardware is usually unique and varies from application to application. Each system must meet a completely different set of requirements [9, 1]. The common critical features and design requirements of an distributed hardware include [5]: ***Processing power:*** Selection of the processor is based on the amount of processing power to get the job done and also on the basis of register width required. ***Throughput:*** The system may need to handle a lot of data in a short period of time. ***Response:*** the system has to react to events quickly. ***Memory:*** Hardware designer must make his best estimate of the memory requirement and must make provision for expansion. ***Power consumption:*** Systems generally work on battery and design of both software and hardware must take care of power saving techniques. ***Number of units:*** the no. of units expected to be produced and sold will dictate the Trade-off between production cost and development cost. ***Expected lifetime:*** Design decisions like selection of components to system development cost will depend on how long the system is expected to run. ***Program Installation:*** Installation of the software on to the distributed system needs special tools.

Testability & Debug ability: setting up test conditions and equipment will be difficult and finding out what is wrong with the software will become a difficult task without a keyboard and the usual display screen.

Reliability: is critical if it is a space shuttle or a car but in case of a toy it doesn't always have to work right.

5 Requirements for Distributed Systems

Distributed systems are unique in several ways. When designing distributed systems, there are several categories of requirements that should be considered [1, 2]:

1. Functional Requirements
2. Temporal Requirements (Timeliness)
3. Dependability Requirements

1. Functional Requirements Functional requirements describe the type of processing the system will perform. This processing varies, based on the application. Functional requirements include the following; • Data Collection requirements • Sensoring requirements • Signal conditioning requirements • Alarm monitoring requirements • Direct Digital Control requirements • Actuator control requirements • Man-Machine Interaction requirements (Informing the operator of the current state of a controlled object for example. These interfaces can be as simple as a flashing LED or a very complex GUI-based system. They include the ways that distributed systems assist the operator in controlling the object/system.

2. Temporal Requirement Distributed systems have many tasks to perform, each having its own deadline. Temporal requirements define the stringency in which these time-based tasks must complete. Examples include; • Minimal latency jitter • Minimal Error-detection latency Temporal requirements can be very tight (for example control-loops) or less stringent (for example response time in a user interface).

3. Dependability Requirements Most distributed systems also have a set of dependability requirements. Examples of dependability requirements include;

• ***Reliability***: this is a complex concept that should always be considered at the system rather than the individual component level. There are three dimensions to consider when specifying system reliability:

1. Hardware reliability; probability of a hardware component failing
2. Software reliability; probability that a software component will produce an incorrect result
3. Operator reliability; how likely that the operator of a system will make an error.

There are several metrics used to determine system reliability;

- Probability of failure on demand; likelihood that the system will fail when a service request is made.
- Rate of failure occurrence; frequency of occurrence with which unexpected behavior is likely to occur.
- Mean Time to Failure (MTTF); the average time between observed system failures.

• ***Safety***: describe the critical failure modes and what types of certification are required for the system.

• ***Maintainability***: describes constraints on the system such as type of Mean Time to Repair (MTTR).

• ***Availability***: the probability that the system is available for use at a given time. Availability is measured as; Availability = MTTF / (MTTF+MTTR)

• ***Security***: these requirements are often specified as "shall not" requirements that define unacceptable system behavior rather than required system functionality.

6 Programming Distributed Systems

A large variety of applications can be found where distributed systems play an important role, from small stand-alone systems, like a network router, to complex distributed systems supporting several operating execution environments as founded in avionic applications. This variety of applications also implies that the properties, platforms, and techniques on which distributed systems are based can be very different. The hardware needs can sometimes be achieved with the use of general purpose processors, but in many systems specific processors are required, for instance, specific DSP devices to perform fast signal processing. Memory management capabilities are necessary in some systems to provide memory protection and virtual memory. Special purpose interfaces are also needed to support a variety of external peripheral devices, energy consumption control, and so on

Every distributed system had at least one LED that could be controlled by software. The following example is designed to blink LED at a rate of 1 Hz(one complete on-off cycle per second). Typically, the code required to turn an LED on and off is limited to a few lines of C or assembly, so there is very little room for programming errors to occur. And because almost all distributed systems have LEDs, the underlying concept is extremely portable [7].

The superstructure of the Blinking LED program is shown below. This part of the program is hardware-independent. However, it relies on the hardware-dependent functions toggleLed and delay to change the state of the LED and handle the timing, respectively.

```
  /*************************************************
************* * Function: main()
  *
   * Description: Blink the green LED once a second.
  *
  * Notes: This outer loop is hardware-independent. How-
ever,
  * it depends on two hardware-dependent functions.
  *
   * Returns: This routine contains an infinite loop.
```

```
   *
   void
  main(void)
  {
  while (1)
  {
  toggleLed(LED_GREEN);          /* Change the state of
the LED. */
   delay(500);        /* Pause for 500 milliseconds. */
  }
  /* main() */
  }
```

7 Conclusion

Real-time distributed systems vary in their functions and their component. The components of simple distributed systems are usually less than of the sophisticated ones. In addition the components themselves including the hardware and software are being more complexes for the distributed systems which perform high level tasks. The software for efficient distributed systems is optimized to reduce the execution time during work. Therefore a new software is required when the hardware is upgraded to keep the high level of performance. The failure of the hardware in many cases causes shutdown in the system and usually recoding is required to bring back the system to work. On the other hand any defects in software will not damage the hardware. The following conclusions can be drowning from the current work:

1. In this report, the real-time and distributed system characteristics and there requirements have been listed and discussed thoroughly.

2. The distributed systems comprised hardware and software. The hardware should contain the processor and memory and some peripherals devices for input and output. While the suitable software is associated with every part of the hardware in order to perform the required function that the distributed system designed to do.

3. The final step of writing distributed system software is optimizing the code to make the working program run on the lower-cost production version of the hardware.

4. Code optimization can be provided by increasing code efficiency, decreasing code size, and reducing memory usage.

8 Reference

[1] Silperschatz Abraham, Galvin Peter Baer, Gagne Greg, "Operating System Concepts " , Seventh Edition, John Wiley & SONS. INC, 2005.

[2] Oshana Robert," Introduction to embedded and Real-time systems", Texas Instruments Engineering Manager.
[3] Dedicated Systems Experts, What makes a good RTOS. Brussels, Belgium: Dedicated Systems Experts, 2001.
[4] Li Qing, Yao Caroline, "Real-Time Concepts for Embedded Systems", CMP Books an imprint of CMP Media LLC.
[5] M. Tech., Agarwal Vivek, "Embedded Operating Systems for Real-Time Applications", Sagar P M, November 2002.
[6] http://searchenterpriselinux.techtarget.com/sDefinition/0, sid39_gci837507, 00.html Search EnterpriseLinux.com Definitions.
[7] Barr Michael, "Programming Embedded Systems in C and C++", O'Reilly, first edition, ISBN, 191 pages, January 1999.
[8] Feiler Peter H., Lewis Bruce, Vestal Steve," Improving Predictability in Embedded Real-Time Systems", Special Report CMU/SEI-2000-SR-011, December 2000
[9] Stankovic John A., "Real-Time and Embedded Systems", University of Massachusetts, Amherst, stankovic@cs.umass.edu.
[10] S. Perumal, "Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism," Wasit Journal of Computer and Mathematics Science, pp. 43-51, 2021.
[11] I. A. Aljazaery, and. Jaafar Q. Kadhim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 02, 2023.
[12] D. Al-Malah, and H. Salim, "Enhancement of educational services by using the internet of things applications for talent and intelligent schools," Periodicals of Engineering and Natural Sciences (PEN), vol. 8, no. 4, pp. 2358-2366, 2020.
[13] H. Ibrahim, "A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 76-108, 2022.
[14] N. A. Jasim, and M. S. Farhan, "Internet of Things (IoT) application in the assessment of learning process," in IOP Conference Series: Materials Science and Engineering, 2021, vol. 1184, no. 1: IOP Publishing, p. 012002.
[15] H. A. Hassan, "Review Vehicular Ad hoc Networks Security Challenges and Future Technology," Wasit Journal of Computer and Mathematics Science, vol. 1, no. 3, 2022.
[16] M. A. Khalifa, A. M. Ali, S. A. Alsadai, N. F. Alwan, and G. S. Mahdi, "A Novel Arabic Words Recognition System Using Hyperplane Classifier," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 2, pp. 12-20, 2022.
[17] R. a. M. Al_airaji , I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," International Journal of Interactive Mobile Technologies, vol. 16, no. 10, 2022.
[18] S. Alam, "Smart health costing system," Wasit Journal of Computer and Mathematics Sciences, vol. 1, no. 3, pp. 70-75, 2022.
[19] S. Al-Jaff, O. Bayat, and A. H. Sallomi, "Analysis of Interference and Signal Quality in Cellular Wireless Networks," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 881, no. 1: IOP Publishing, p. 012143.
[20] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," International Journal of Online & Biomedical Engineering, vol. 18, no. 12, 2022.
[21] A. S. H. Rihab Salah Khairy, "The Detection of Counterfeit Banknotes Using Ensemble Learning Techniques of AdaBoost and Voting," International Journal of Intelligent Engineering and Systems, vol. 14, no. 1, pp. 326-339, 2021.

[22] H. T. Hazim. H. Alrikabi, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021.
[23] How to Design a RealTime Embedded System Using UML | eHow.com http://www.ehow.com/how_6596645_design-embedded-system-using-uml.html#ixzz1S47rv0qc.

Article submitted 20 November 2022. Published as resubmitted by the authors 21 December 2022.

An Improved Method for Hiding Text in Image Using Header Image

https://doi.org/10.31185/wjcm.79

Nada Abdul Aziz Mustafa(✉)
University of Baghdad / College of language, Iraq.
nada@colang.uobaghdad.edu.iq

Abstract— The necessities of steganography methods for hiding secret message into images have been ascend. Thereby, this study is to generate a practical steganography procedure to hide text into image. This operation allows the user to provide the system with both text and cover image, and to find a resulting image that comprises the hidden text inside. The suggested technique is to hide a text inside the header formats of a digital image. Least Significant Bit (LSB) method to hide the message or text, in order to keep the features and characteristics of the original image are used. A new method is applied via using the whole image (header formats) to hide the image. From the experimental results, suggested technique that gives a higher embedding of several stages of complexity. Also, LSB method via using the whole image is to increase the security and robustness of the proposed method as compared to state-of the-art methods.

Keywords— Steganography, information hiding, LSB method, stego-analysis, digital image.

1 Introduction

Steganography can be defined as a procedure of hiding a secret text message into an image or hiding image within image complete secret image in the cover [1]. Consequently, the cover image must not interest any consideration as a carrier of a text message and must compare as near as potential to discover the original image via the human eye. After images are utilized as the carrier in steganography, they are normally handled through changing more than bits of the byte, which formed the pixels of the image [2]. While cryptography is indicated to like "secret writing". Cryptography is considered as a technique of sending a text message in a different form so as to the envisioned receiver could read and procedure it [3].

For the cryptography, the hidden message is named plain text and a masked text message is named cipher text. The procedure of changing a plain text into cipher text is encryption and the opposite procedure is named decryption [4]. Moreover, cryptography generates privacy potential even on an insecure channel. Recent cryptography utilizes a key if the security of a procedure depend on keeping the way the procedure mechanism secretly. This key may be a sequence of numbers, characters, or others utilized via cryptographic algorithm to change the plaintext to a cipher text or vice versa

[5]. The key could be a secret key like utilize the similar key for both plaintext and cipher text pattern [6]. Moreover, the public key that utilizes a pair of keys, one for encryption named (public key) and another one for decryption named (secret key),as described in Figure 1.

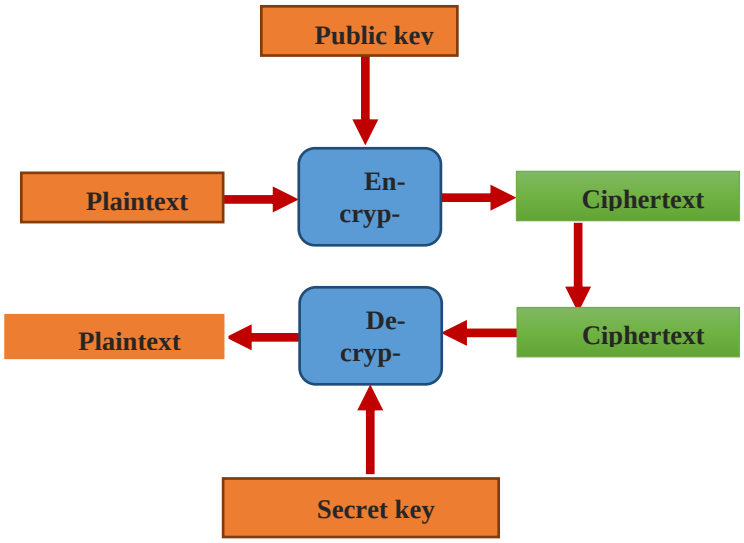


Fig. 1. The general idea of cryptography.

While for the steganography, the procedure of embedding a secret text message inside data cover is named encoding and the opposite procedure is named decoding. There was three types of steganography (pure steganography, secret key steganography and public key steganography) [7]. The first type is pure steganography that is not used to stego-key between the sender and receiver where it depends on the assumption, which no one is knowing of the secret text message [8]. The second type is secret key steganography utilizes stego-key where someone who recognizes the stego-key could reverse the procedure and read the secret text message[9], as shown in Figure 2. While the third type is the public key steganography comprises two keys where one is used for embedding procedure named (public key) and another one is used to extract the secret text message named (private key) [10].

The least significant bit (LSB) is used to encode the bits of the message. Where the LSB method can formerly read through the receiver of the stego-image and placed together [11]. The bytes is used to replicate the hidden text message that is provided the stego-key for the stego-image as shown in Figure 2.

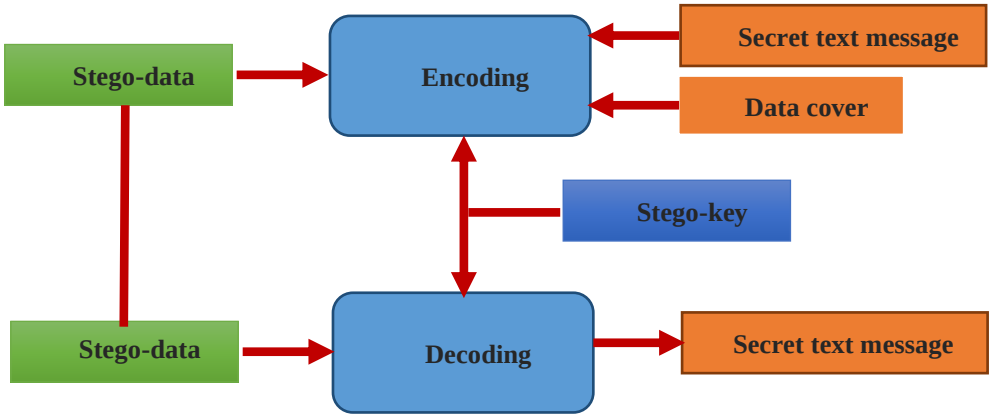


Fig. 2. The general idea of secret key steganography.

There are four main types of steganography that have been utilized to hide information on different digital mediums like text, video, image and audio [12].

1. Text Steganography: A steganography method, which utilizes text as the cover media is named a text steganography. This type is the hardest of the steganography method due to the text files take an identical small quantity of terminated data to hide a secret text message [13].
2. Video Steganography: A steganography method, which utilizes video as the cover media is named video steganography [14].
3. Image Steganography: A steganography method, which utilizes images as the cover media is named an image steganography. This type is considered as the hiding secret text messages in digital images and it is the most commonly utilized technique as it could obtain the pros of the restricted power of the human visual system (HVS). This is attributed to the images can have a huge quantity of terminated information, which could utilized to hide a secret text message [15].
4. Audio Steganography: A steganography method, which utilizes audio as the cover media is named an audio steganography. This type is regarded as the greatest challenging mission in steganography. This is attributed to the human auditory system (HAS) that has a huge dynamic domain to listen over. Therefore, even a minute modify in audio worth may be identified via the human ears [16].

2 Related work

Hiding information becomes is considered as one of the most vital keys of information technology and communication due to the great increase of the World Wide Web. Cryptography method was used for hiding information [17]. However, it is sometimes not sufficient to save the contents of a text message secret, it can be required to save the presence of the text message secret that called steganography [18]. Several data hiding structures take pros of human perceptual weaknesses [19]. The chief pros

of steganography technique is due to its basic security mechanism. Due to the steganographic text message is combined invisibly and covered within other innocent sources, it is very hard to discover the text message without knowing the presence and the suitable encoding pattern [20]. There was found different steganography techniques utilized for hiding data like least significant bits (LSB), batch steganography, permutation steganography, and bit-plane complexity segmentation (BPCS). a new technique that is used to hide data inside the audiovisual files proposed by [21]. In steganography technique, to hide text, the secret text has to be hidden in a cover message. A steganography method to hide a large amount of data with high security. Steganography method is based on hiding a large amount of data (image, audio, text) file inside a color bitmap (bmp) image was introduced by [22]. The image filtered and segmented that bits replacement is utilized on the suitable pixels. The pixels are nominated randomly instead of sequentially. A new modified method via using the side match method. They focused on hiding the text in the edge parts of the image was presented by [23]. A new technique using pixel-value differencing by dividing the original image into non-overlapping blocks of two successive pixels was introduced by [24].

3 Systematic Proposed Approach

The suggested approach can be divided into three main phases: Hiding text in image and extracting secret text message from colored image and performance evaluation as shown in Figure 3. For hiding text in image, the text is used as a collection of characters where each character has code number (ASCII). The proposed approach is presented a new technique via processing the text as image rather than the (ASCII) code. For hiding text in image, it uses a new technique via using the header formats of the whole distribution of secret image file randomly among the contents of cover image as well as using LSB algorithm to hide the key. Furthermore, there are several complexity stages to avoid the stego-analysis from the attackers who must know many keys to reach the secret text message (plaintext).

This study deals with text is being an image, it is not considered as group of letters due to the procedure of hiding image. Several embedding of several stages of complexity is done, it combines the secret message in a collection of characters where each character has code number (ASCII) to the corresponding values of it. The proposed technique is to use the first byte segment length of header formats as the number of bits to decode position and the second byte segment uses the last two byte number of segment and so on. This value is treated on base that represents color value via storing in BMP value. Consequently, it has randomly colored image much bigger than the secret text as a specific stage of complexity operation. Hiding text into within image it can be in one of the all contents like image data, files information and colors index via dividing it to a group of values hidden in segments inside the cover (image file). The position of these values is indicated to the beginning each segment via using LSB algorithm that it used to encode hidden data position rather than a tool for hiding text in image. A key that helps to crypt secret text process is hidden in the cover that it used to be sure not to be discovered.

4 Hiding Text in Image

Hiding text embeds a secret text message inside a cover image in a hidden method to secure trust information. Presently, hiding text in the process of steganography has found varied areas like covert communication, content authentication and so on. Text stego-analysis is considered as the process of identify in a given carrier text message has hidden information inside it as well as the process of extracting implanted hidden information.

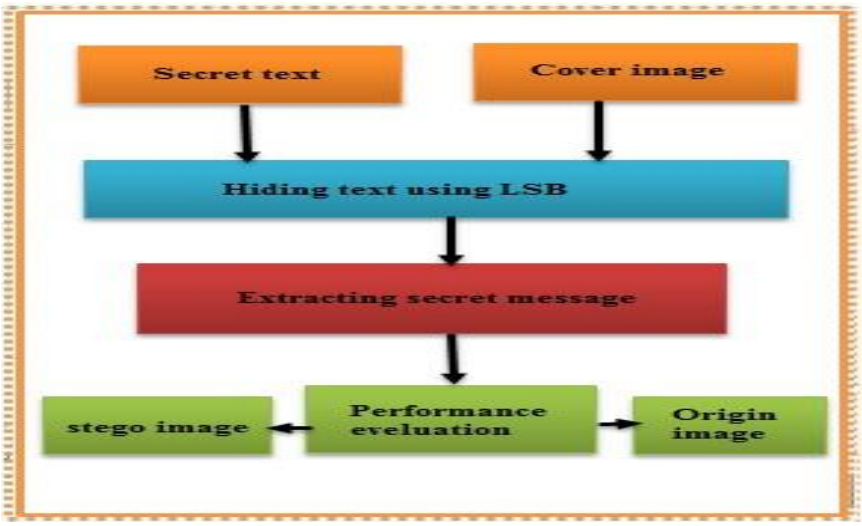


Fig. 3. The framework of proposed systematic approach.

5 Converting Text to Image

To increase the complexity, the contiguous eight pixels of the binary image that will be combined together, to produce a file having one byte per pixel. The new BMP image file scan and counting the number of contiguous bytes with the same value until the value is changed (counting does not exceed than 255 bits to allow representing it in one byte). The two bytes (count and value) that will be stored in this file (24) bit color and counting the other values starts until it reaches to different value where this procedures continues until all images are fully scanned.

The result file consists of sequence byte-pairs, where the first number with one value represents the number of repetition of the value of the second number byte.

The size of the original secret message image is (926) byte, while the random color image is (1.01) KB. From the comparative between both of them the second file is larger than the first due to convert the image from one byte color to 24-bit BMP image as displayed in Figure 4.

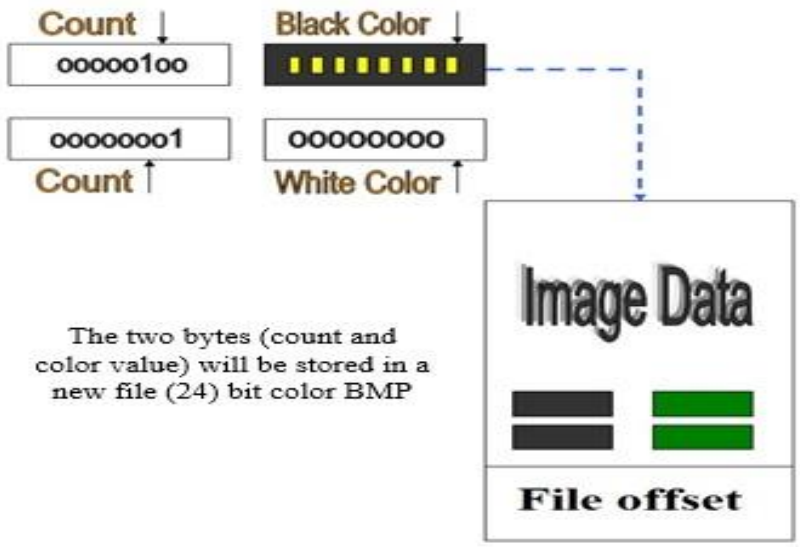


Fig. 4. Block diagram of converting one color byte.BMP to 24- bit BMP

6 Selecting of Cover Image

Choose an image to use it as a cover for hiding the secret text message (image) by using basic database as shown in Figure 5.

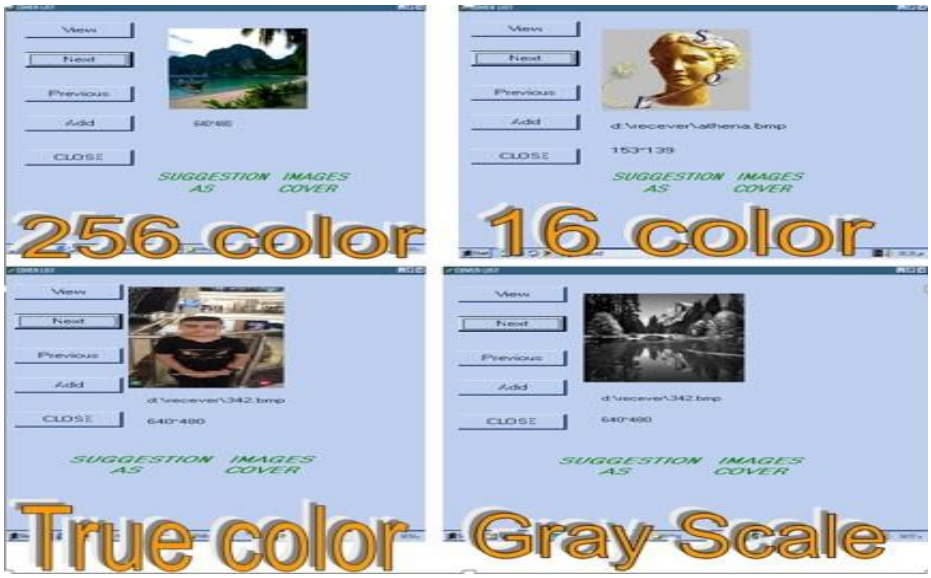


Fig. 5. Database images of colored image or gray scale image.

7 Hiding the Secret Text Message in Cover Image

The hiding procedure starts to hide text into image as follows:

1. The secret text message file (header and data) can be divided into two blocks each one with two bytes.
2. Divided the cover excluding the header of image file to a segments such that the number of segments depend on number of blocks and the size of each segment depends on the number of segments as given in Equation 1.

$$\text{Number of segments(M)} = \frac{(\text{secret message})}{2} \quad (1)$$

where M=secret key number 2.

The 256 bytes is enough for representing segment length to hide (2) bytes and when the size of secret message required to indicate the secret message with than 256 bytes as given in Equation 2.

$$\text{Length of segments(L)} = \frac{(\text{Total image size(cover)})}{\text{Number of segments required}} \quad (2)$$

where L= Public key steganography

3. Each block of secret message (2) bytes should be hidden in one segment.
   According to segment length determines the number of bits required to code this length, which means the number of bits required to code the position of secret message in the segment (that it does not exceed to segment length). This represented the maximum number of bits are used at beginning of each segment to code position of secret message block in which the segment by using the LSB algorithm.
4. To hide a block of secret message in one segment, the value of this block will be compared with the value of each contiguous two bytes in that segment. After scanning all segments bytes, the result should be either two bytes identical to block or the nearest value to that block.
5. Change the two bytes in segment with the two equal bytes of secret message block.
6. The position of these blocks will be coded at the beginning of segment using (LSB) method.
7. Repeat steps (4) to (6) until all secret message blocks are hidden in cover file. See figure 6.

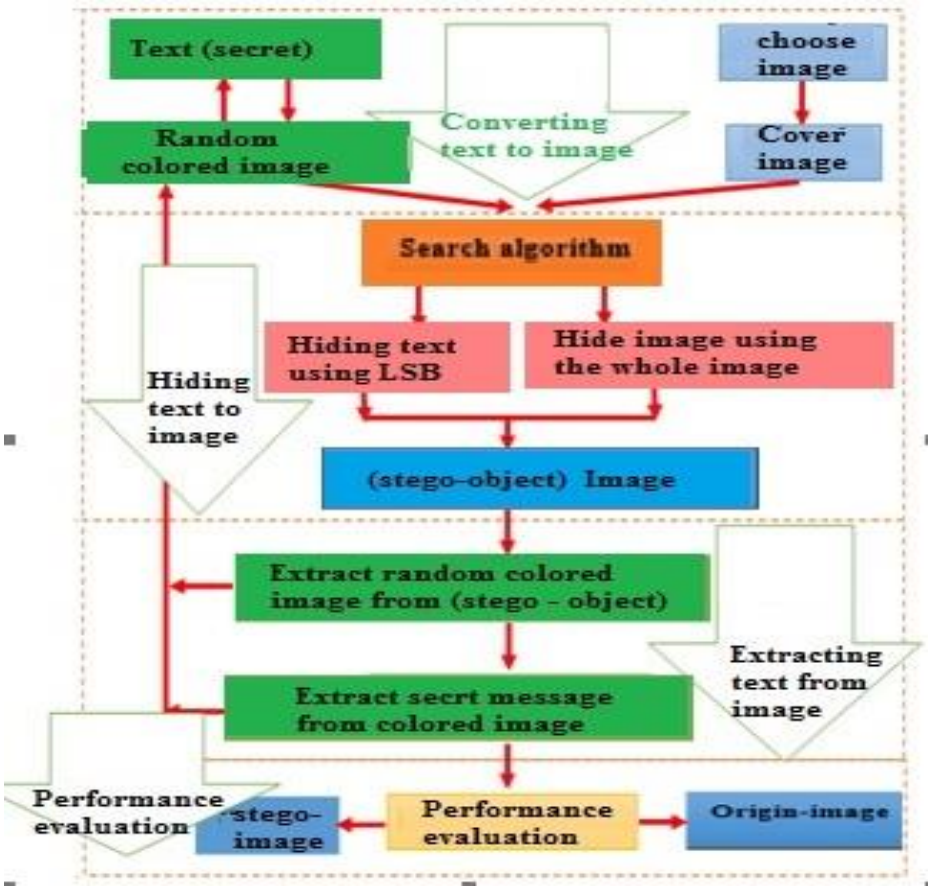


Fig. 6. Hiding the Secret Text Message in Cover Image

8 Hiding Keys

This study introduced the secret message is hidden in a random position in cover file by using two techniques. The first technique is to change the byte value and (LSB) method while the second technique is to extract the secret message by the authorized (receiver). The receiver that was required to key to reach the secret message (two types of key).

The hiding keys are known between sender and receiver. There are two keys as follows:

1. Public key: This key is considered as the first byte of cover image (bitmap data). Where it holds the segment length.
2. Secret key (1): The last byte of the first segment decoded to contain the number of bits required to decode the position of secret message in each segment.

3. Secret key (2): The last two bytes in the second segment are decoded to contain the number of segments that required to hide all secret message blocks. The listed keys is scheduled in Table 1.

Table 1. The structures of the stego-object cover file.

File Offset		
First byte segment length	*A. Segment 1*	Last byte (number of bits to decode position)
Second segment	Last two byte number of segment	*B. Segment 3*
Segment 4	Segment 5	Segment 6
.....etc	.....	.....
EOF		

9 Hiding Text Within Image Using Complete Image

Hiding text within image using steganography is the most important topic due to the challenge of the complexity to avoid the attacker software [7]. Instead of using the piece, which constitutes image data where there are other complex techniques of covering data within the image. The principle of steganography is based on noise area and other techniques that depend upon spreading data within the image by using Hoping technique.

This study is hiding text within image complete secret image in the cover (header and indexing formats). This technique is based on dividing the image into group of values hidden in segments inside the cover (image file). Where it dealing with the position of these values are indicated to the beginning of each segment via using LSB method to encode hidden data position. The idea is using LSB as the secret key for helping to crypt secret text process is hidden in the cover in which generates it without any suspicious from the attacker.

10 Extracting the Stego-Object

The extracting phase is planned to recover the hidden text message from the stego-object [25]. It comprised two steps (extracting random colored image from the stego-object image and extracting secret text message from colored image). Moreover, it is referred to the opposite of hiding process. The overall extracting phase is utilized to find the secret text message that sent by image from sender to receiver. This study is

presented as the extracting text is implemented by using the key that was stored into the first byte after the file offset and representing the segment length of hiding. The position of the secret key number (1), which represents in the last byte of the byte the first segment and the position of the secret key number (2) represents in the last two bytes of the second segment while the secret text message that was stored at the beginning of the third and so on until the key text message is completed. Figure 7 shows the flow chart of the extracting text message from stego-object.

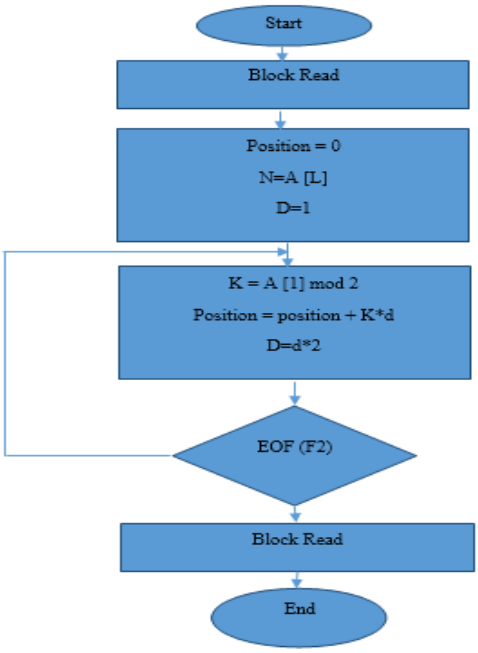


Fig. 7. Flow chart of extracting text from image.

11 Performance Evaluation

The prefect steganography is getting stego-image that was similar to the original cover by both perceptually and computer accessing. This may be impossible to reach, the cover when it changes to stego-image give the closest criteria for original cover. The standard metrics that should be used to measure for both cover image and stego-object as follows:

1. Variance: This metric that measured about the contrast between the cover and stego-object, it describes the spread in the data so a great constant image is given by [26], as shown in Equation 3 as follows:

$$v(g) = \sqrt{\sum_{g=0}^{L-1}(g - \dot{g})p(g)} \quad (3)$$

where:

$\bar{g}$ = The mean of colors value increasing the different of stego-image and the original image.

L = The number of colors in image.

g = color image.

P(g)= probability of color image.

2. Entropy: This metric that it displayed how many bits, which required to code the image data is given by [27], as shown in Equation 4 as bellows:

$$\text{Entropy} = -\sum_{g=0}^{L-1} p(g) * \log p(g) \quad (4)$$

where:

L = number of colors in image.

g = color.

P (g) = probability of color.

3. Energy: This metric is used to find the distribution of colors in image is given by [28], as shown in Equation 5 as follows:

$$Energy = \sum_{g=0}^{L-1} p(g)^2 \quad (5)$$

where:

L= The number of colors in image.

g = color.

P(g)= probability of color.

4. Similarity: The embedding process is defined in a way which cover and the corresponding stego-image are perceptually similar formally perceptual similarity can be defined via similarity function as follows:

Let c be nonempty set. Function

Sim: c2>[-∞ ,1] is called similarity function on c,

If for (x,y) ∈ c

Sim (x,y) = 1↔x= y

For x # y, sim (x,y) < 1

Perfect similarity ≠ 1

Sim (cover, stego) ≠ 1

In the case of digital images the correlation between two images can be used as similarity function therefore most practical steganographic systems try to fulfill the condition.

Sim (Cover, Stego) = 1.

5. Secrecy: This metric is considered as the most significant criteria. Where it is the a ability to hide information in cover image and is determined by[26], as shown in Equation 6 as follows:

$$Secrecy = \sum_{g=0}^{L-1} p_c(g) log_2 p_c(g)/p_s(g) \quad (6)$$

where:
P(g)=probability of color.
g= color.
L= number of colors.
c= cover image.
s =stego – image

6. Average: This metric that is used to find how the brightness of the image, it is given by [26], as shown in Equation 7 as bellows:

$$Average(\bar{g}) = \sum_{r=0}^{N-1} \sum_{c=0}^{N-1} I(r,c)/m \quad (7)$$

where
I(r, c): color value at coordinate r, c.
m= Thetotal number of pixels in image.

7. Probability: This metric is used to provide information about the characteristics of the colors level distribution for the image is given by [26], as shown in Equation 8 as follows:

$$p(g) = N(g)/m \quad (8)$$

where
N (g)= number of pixels with color (g).
m= The total number of pixels in image

8. Signal to noise ratio (SNR): The SNR serves as a measure of delectability, the cover image is viewed as noise contrary to typical communication scenarios where a high SNR is desired, a very low SNR for stego system corresponds to lower perceptibility and therefore it is greater success than when concealing the embedding signal is given by [29-32], as shown in Equation 9 as follows:

$$\mathrm{SNR} = \sum_{r=0}^{N-1} \sum_{c=0}^{N-1} \hat{I}(r,c)^2 / \sum_{r=0}^{N-1} \sum_{c=0}^{N-1} [\hat{I}(r,c)^2 - I(r,c)]^2 \quad (9)$$

where:
I (r,c) = The original image.
I ́(r,c)= The stego Image.

Hiding the secret text message in image at the first by using LSB algorithm. Where the LSB algorithm is based on utilizing the lower bit within the byte and replacing it by the value of the one of bits that constitutes the message. This text message must be converted to image by using paint software. Table 2 displays the performance evaluation findings with hidden data when utilizing stego-object.

Table 2. The performance evaluation findings with hidden data when utilizing stego-object.

Metric	Origin – cover	Stego- image	Different
Average	1.678	2.154	0.476

Variance	9.655	9.788	0.133
Energy	9.581E-7	9.639E-7	0.158
Entropy	1.709	1.806	0.097
Similarity	**99.992**		
Secrecy	2.669		
SNR	1.954		

Moreover, it can be clearly exhibited that the comparison findings of performance metrics between the origin - cover and the stego-image is matched. Thus, it indicated that the attacker could not recognized the hidden procedure. Consequently, the variant average score between the origin–cover and stego-image is (0.476), the different variance score between the origin–cover and stego-image is (0.133), and the similarity score between the origin–cover and stego-image is (99.992). The whole findings are very corresponding between both of them. That is, the whole findings were specified via comparing encouraging findings utilizing LSB with header and ordering formats hiding algorithms that produces to supply variant levels of complexity when sending and receiving text messages. All levels are used different keys for sender and receiver in order to prevent any suspicion is introduced in Figure 8.

Fig. 8. The comparison between the origin cover with the stego-object.

12 Conclusion

Hiding text in image procedure utilizing steganography presents well-organized method because of all previous researchers are depended on the utilize of the concepts of the LSB method. This study is improved the LSB method with header formats and ordering formats hiding that leads to supply variant levels of complexity when sending

and receiving text messages. The suggested approach is changed the text to image and improved the related of bits to create a color image, which is considered as the first level of complexity. Moreover, it utilized the Least Significant Bit method to hide the text message to keep the whole features of the original image. The header formats of the whole image that used to hide the text proved several different levels of complexity to prevent the attackers to notice the hidden procedures.

13 References

[1] D. Rawat and V. Bhandari, "A steganography technique for hiding image in an image using lsb method for 24 bit color image," International Journal of Computer Applications, vol. 64, 2013.

[2] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, "Text in Image Hiding using Developed LSB and Random Method," International Journal of Electrical & Computer Engineering (2088-8708), vol. 8, 2018.

[3] M. A. Pathak, B. Raj, S. D. Rane, and P. Smaragdis, "Privacy-preserving speech processing: cryptographic and string-matching frameworks show promise," IEEE signal processing magazine, vol. 30, pp. 62-74, 2013.

[4] S. Hamad, A. Khalifa, A. Elhadad, and S. Rida, "A modified playfair cipher for encrypting digital images," Mod. Sci, pp. 76-81, 2013.

[5] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher:(Vigenère-Affine cipher)," 2019.

[6] J. T. Harmening, "Virtual private networks," in Computer and Information Security Handbook, ed: Elsevier, 2017, pp. 843-856.

[7] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," Multimedia Tools and Applications, vol. 77, pp. 17333-17373, 2018.

[8] G. C. Kessler and C. Hosmer, "An overview of steganography," in Advances in Computers. vol. 83, ed: Elsevier, 2011, pp. 51-107.

[9] M. A. F. Al-Husainy and D. M. Uliyan, "A Secret-Key Image Steganography Technique using Random Chain Codes," International Journal of Technology, vol. 10, pp. 731-740, 2019.

[10] M. Mishra, G. Tiwari, and A. K. Yadav, "Secret communication using public key steganography," in International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014, pp. 1-5.

[11] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," International Journal of Electrical and Computer Engineering, vol. 9, p. 5218, 2019.

[12] R. Din, M. Mahmuddin, and A. J. Qasim, "Review on steganography methods in multimedia domain," International Journal of Engineering & Technology, vol. 8, pp. 288-292, 2019.

[13] S. Roy and M. Manasmita, "A novel approach to format based text steganography," in Proceedings of the 2011 International Conference on Communication, Computing & Security, 2011, pp. 511-516.

[14] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: A review," Neurocomputing, vol. 335, pp. 238-250, 2019.

[15] E. Zielińska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," Communications of the ACM, vol. 57, pp. 86-95, 2014.

[16] M. Verma and H. S. Saini, "Analysis of Various Techniques for Audio Steganography in Data Security," International Journal of Scientific Research in Network Security and Communication, vol. 7, pp. 1-5, 2019.
[17] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial Internet of Things," Entropy, vol. 22, p. 175, 2020.
[18] A. Behura, "Congruence of deep learning in biomedical engineering: Future prospects and challenges," in Handbook of Deep Learning in Biomedical Engineering, ed: Elsevier, 2021, pp. 1-24.
[19] N. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," International journal of engineering trends and technology, vol. 11, pp. 388-392, 2014.
[20] N. Akhtar, S. Khan, and P. Johri, "An improved inverted LSB image steganography," in 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 749-755.
[21] R. Ibrahim and T. S. Kuan, "Steganography algorithm to hide secret message inside an image," arXiv preprint arXiv:1112.2809, 2011.
[22] N. S. Terkawi, L. Berriche, A. A. Alamar, M. Ibrahim, and W. S. Alsaffar, "Comparative Study of Three DNA-based Information Hiding Methods," International Journal of Computer Science and Security (IJCSS), vol. 15, p. 45, 2021.
[23] S. N. Bhuiyan, N. A. Malek, O. O. Khalifa, and F. A. Rahman, "An improved image steganography algorithm based on PVD," Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, pp. 569-577, 2018.
[24] M. Khodaei, B. Sadeghi Bigham, and K. Faez, "Adaptive data hiding, using pixel-value-differencing and LSB substitution," Cybernetics and Systems, vol. 47, pp. 617-628, 2016.
[25] N. A. A. Mustafa, "Text hiding in text using invisible character," International Journal of Electrical and Computer Engineering, vol. 10, p. 3550, 2020.
[26] N. K. El Abbadi, "Cover Optimization for Image in Image Steganography," International Journal of Computer Science Issues (IJCSI), vol. 10, p. 556, 2013.
[27] M. M. Hashim, M. S. M. Rahim, F. A. Johi, M. S. Taha, and H. S. Hamad, "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats," International Journal of Engineering & Technology, vol. 7, pp. 3505-3514, 2018.
[28] R. Shmueli, T. Shmueli, and O. Hadar, "Energy based image steganography using dynamic programming," in Applications of Digital Image Processing XLII, 2019, p. 111371R.\
[29] Asgarnezhad, R., et al., An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems. Wasit Journal of Computer and Mathematics Science, 2022. **1**(1): p. 27-35.
[30] Farhan, R.I., A.T. Maolood, and N. Hassan, Hybrid Feature Selection Approach to Improve the Deep
[31] Al Mossawy, M.M.T. and L.E. George, *A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(1): p. 1-14.
[32] E. Noroozi, S. B. M. Daud, and A. Sabouhi, "Critical Evaluation on Steganography Metrics," in Advanced Materials Research, 2013, pp. 927-931.

Article submitted 15 November 2022. Published as resubmitted by the authors 24 December 2022.

Share references by using web pages

https://doi.org/10.31185/wjcm.87

Prof.Dr.Maria A.Wimmer (✉)
Faculty of Computer Science, University of Helsinki, Norway.
mar.wimm@hel.edu.nor

Abstract— During the past recent years, there has been tremendous development reaming the concept of digital libraries-a knowledge base that can be stored and retrieved through online networks. Digital libraries are the most complex form of information systems that support digital document preservation, distributed database management, hypertext, filtering, information retrieval, and selective dissemination of information. This has really overcome geographical barriers offering a wide range of academic, research, and cultural resources with multimedia effects that can be accessed around the world over the distributed networks. The paper examines the concept of Digital library, the technology that has enabled its emergence & architecture of the digital library system. It also highlights the digital library projects undertaken in USA, UK, and India. Here the authors explored the unique feature of digital library and possible challenges ahead for library and information professionals in the digital environment.

Keywords— UX, UI, web design, digital references.

1 Introduction

Web design encompasses many different skills and disciplines in the production and maintenance of websites. The different areas of web design include web graphic design; user interface design (UI design); authoring, including standardized code and proprietary software; user experience design (UX design); and search engine optimization. Often many individuals will work in teams covering different aspects of the design process, although some designers will cover them all[1]. The term "web design" is normally used to describe the design process relating to the front-end (client side) design of a website including writing markup. Web design partially overlaps web engineering in the broader scope of web development. Web designers are expected to have an awareness of usability and if their role involves creating markup then they are also expected to be up to date with web accessibility guidelines.

In 1989, whilst working at CERN Tim Berners-Lee proposed to create a global hypertext project, which later became known as the World Wide Web. During 1991 to 1993 the World Wide Web was born. Text-only pages could be viewed using a simple line-mode browser[3]. In 1993 Marc Andreessen and Eric Bina, created the Mosaic browser. At the time there were multiple browsers, however the majority of them were

Unix-based and naturally text heavy. There had been no integrated approach to graphic design elements such as images or sounds. The Mosaic browser broke this module.

The W3C was created in October 1994 to "lead the World Wide Web to its full potential by developing common protocols that promote its evolution and 3 ensure its interoperability.

This discouraged any one company from monopolizing a propriety browser and programming language, which could have altered the effect of the World Wide Web as a whole.

The W3C continues to set standards, which can today be seen with JavaScript and other languages.

In 1994 Andreessen formed Mosaic Communications Corp. that later became known as Netscape Communications, the Netscape 0.9 browser.

Netscape created its own HTML tags without regard to the traditional standards process. For example, Netscape 1.1 included tags for changing background colours and formatting text with tables on web pages. Throughout 1996 to 1999 the browser wars began, as Microsoft and Netscape fought for ultimate browser dominance. During this time there were many new technologies in the field, notably Cascading Style Sheets, JavaScript, and Dynamic HTML. On the whole, the browser competition did lead to many positive creations and helped web design evolve at a rapid pace [4].

In 1996, Microsoft released its first competitive browser, which was complete with its own features and HTML tags. It was also the first browser to support style sheets, which at the time was seen as an obscure authoring technique and is today an important aspect of web design [5].

The HTML markup for tables was originally intended for displaying tabular data. However, designers quickly realized the potential of using HTML tables for creating the complex, multi-column layouts that were otherwise not possible. At this time, as design and good aesthetics seemed to take precedence over good mark-up structure, and little attention was paid to semantics and web accessibility.

HTML sites were limited in their design options, even more so with earlier versions of HTML.

To create complex designs, many web 4 designers had to use complicated table structures or even use blank spaces .GIF images to stop empty table cells from collapsing. CSS was introduced in December 1996 by the W3C to support presentation and layout.

This allowed HTML code to be semantic rather than both semantic and presentational, and improved web accessibility, see table less web design. In 1996, Flash (originally known as Future Splash) was developed. At the time, the Flash content development tool was relatively simple compared to now, using basic layout and drawing tools,

A limited precursor to Action Script, and a timeline, but it enabled web designers to go beyond the point of HTML, animated GIFs and JavaScript. However, because Flash required a plug-in, many web developers avoided using it for fear of limiting their market share due to lack of compatibility. Instead, designers reverted to gif animations (if they didn't forego using motion graphics altogether) and JavaScript for widgets. But the benefits of Flash made it popular enough among specific target markets to eventually work its way to the vast majority of browsers, and powerful enough to be used to develop entire sites [6].

Further information: Browser wars First Browser War (2001 –1995).

In 1998, Netscape released Netscape Communicator code under an open-source license, enabling thousands of developers to participate in improving the software. However, these developers decided to start a standard for the web from scratch, which guided the development of the open-source browser and soon expanded to a complete application platform. [5]

The Web Standards Project was formed and promoted browser compliance with HTML and CSS standards. Programs like Acid1, Acid2, and Acid3 were created in order to test browsers for compliance with web standards. In 2000, Internet Explorer was released for Mac, which was the first browser that fully 5 supported HTML 4.01 and CSS 1. It was also the first browser to fully support the PNG image format.

By 2001, after a campaign by Microsoft to popularize Internet Explorer, Internet Explorer had reached 96% of web browser usage share, which signified the end of the first browsers wars as Internet Explorer had no real competition [7].

2 Literature

Nowadays everybody is talking about Digital libraries. In this age of Information Technology, it is impossible to read a library journal or attend a library conference or even have a chat with other librarians without hearing the term 'digital library' or 'electronic library'. So, librarians must have an understanding of what a digital library is and how it is designed and implemented. The recent advances in Information technology and exponential growth of data in digital form have created an intensive interest in techniques to assist the users in locating desired data. Digital libraries are structured storage environment of digital data with a consistent format for index and content abstraction.

A digital library is a collection of information that is stored and accessed electronically. The purpose of a digital library is to provide a central location for accessing information on a particular topic [8]. Here two things are important. First, it is a collection of information. We can't confine a digital library to a physical structure or building as in the case of a traditional library. Second point is information is stored and accessed electronically. We can define a digital library, more comprehensively, as an electronic library in which a large number of geographically distributed users can access the contents of large and diverse repositories of electronic objects through computer networks. Electronic objects include multimedia object, networked text, images, sound, videos, maps etc. [8]

The term digital library was evolved in early 1970s. The first application of digital library concepts was associated with character-coded storage and full text indexing of legal and scientific documents. The Legal Information through Electronic (LITE) system was the first digital library implemented by the US Air Force in 1967 [9]. 1970s witnessed the release of a number of software packages for computer-based storage, indexing and retrieval of documents in character-coded form. E.g., STAIRS - IBM's storage and information retrieval system, BASIS - Battelle Automated Search Information System etc. During 1980s sophisticated information storage and retrieval

systems came into light. Online hosts like DIALOG and STN started providing full text online journals although these were simple ASCII or text files without graphics and pictures.

In the late 1980s and early 1990s several full text databases started appearing. E.g., IEEE/IEE Electronic Library (IEL), UMI's International Business Database, US Patents etc. 1990s witnessed a revolution in digital library system with the introduction of WWW, which offered a crucial advantage with the availability of ready-to-use and user-friendly graphical web browser for all prevalent platforms. Standard browsers like Netscape Navigator or Internet Explorer are being upgraded regularly for added functionality such as e-mail, support for JAVA, Active X controls etc. These browsers are freely available and easy to use. The Internet and associated technologies made it possible for digital libraries to include multimedia objects like text, image, audio, video etc. The recent developments in digital library can be attributed to Internet and web technology. Which can act as a media of information presentation and delivery.

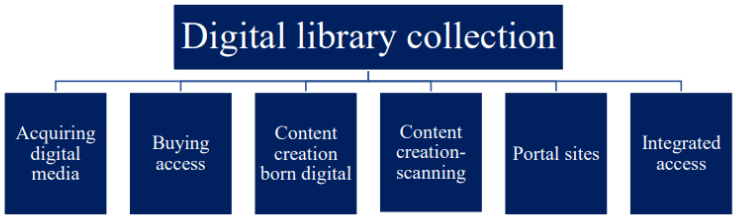
3 Digital Collection Building

According to Rusbridge [6] the resources for a digital library can be divided into four categories.

1. **Legacy resources**: this includes manuscripts, slides, and maps, audio and video records. These are largely non-digital resources. These are major resources of existing libraries. These resources will remain. Outside the scope of digital resources for many years.
2. **Transition resources**: these resources are primarily designed for another medium (print). These resources are converted into digital form for increased access and to reduce reliance on physical libraries.
3. **New digital resources**: these are explicitly created as digital. New digital resources are designed with a particular use in mind. These resources make use of Internet and web technologies.
4. **Future digital resources**: there is an increasingly wide range of digital resources from formally published electronic journals and electronic books through databases.

Digital collection can be built by adopting the following methods. Schematic representation of these methods is given below [7].

Digital library collection:



1. Acquiring Digital Media:

Today a number of commercial agencies supply digital media that contain a vast ocean of knowledge. We can procure these sources of information according to our requirement. E.g., McGraw-Hill Multimedia Encyclopedia of Science and Technology, Silver Platter System produces more than 250 information products on CD-ROM etc.

2. Buying Access:

Here we can subscribe to sources of digital information. A good number of technical journals are published either in electronic form only or they have their own electronic counterpart.

3. Content creation:

We can generate contents by our own. In academic institutions, many faculty members or Research Scholars publish articles

Regularly. We can request those authors to provide us with a soft copy of their articles and this information can be added to our collection. This is called born digital.

4. Content Creation by Scanning:

This is yet another method for building the collection. The existing sources of information may be in print media. These sources can be converted into digital media by scanning the materials. This is the most popular method of converting the existing sources of information. Scanned documents are stored like pictures or graphics and this should be converted as text documents. Many software's are available for this purpose.

5. Portal Site:

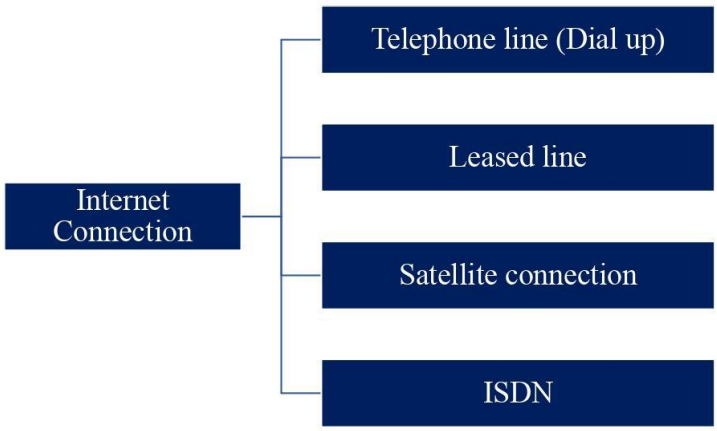
Portal means a gateway or entrance. We can include addresses of websites, which are of interest to our readers in our library so that users may come across these sites. If the user is interested to visit a site, he can directly click the address and he will be connected to that site. In this way our library can act as a portal site.

6. Integrated Access:

We can also develop digital collection by combining one or more methods discussed above.

4 Hardware and Software

Next important issue that needs to be addressed is hardware and software. We must provide enough storage location for digital information. Moreover, the server must have access to the Internet. System should provide enough hard drive space and should be capable of handling the expected access load. System must have a better connection to the Internet, which may be of the following types. Depending upon the type of connection, bandwidth and speed of connectivity varies [11].



5 Conclusions

Another important thing is the ever-changing technology. We must stay keeping up to date with the latest technologies and standards. In the current context is Suggest that instead of going to computing the existing libraries We can create a digital library along with the traditional library, because we You have to spend a huge amount to automate the existing libraries and even After spending that amount, what we get is just a bibliographical detail of the documents are available in a machine-readable format. While in the case of a digital library we can provide relevant information to the right users at the right time. In this way we can provide better and high-quality services to our visitors.

6 Reference

[1] Lester, Georgina. "Different jobs and responsibilities of various people involved in creating a website". Arts Wales UK. Retrieved 2012-03-17.
[2] Zwicky, E.D, Cooper, S and Chapman, D.B. (2000). Building Internet Firewalls. United States: O'Reily & Associates. p. 804. ISBN 1-56592- 871-7.
[3] Jump up toa b c d Niederst, Jennifer (2006). Web Design In a Nutshell. United States of America: O'Reilly Media. pp. 12–14. ISBN 0-596- 00987-

[4] Jump up toa b Chapman, Cameron, The Evolution of Web Design, Six Revisions, archived from the original on 30 October 2013
[5] "AMO.NET America's Multimedia Online (Internet Explorer 6 PREVIEW)". amo.net. Retrieved 2020-05-27.
[6] Richvalsky and Watkins. Designing and Implementing a digital library. ACM Crossroads Student Magazine. January 1998. Htm.
[7] Arora, Jagadish. Building digital libraries: an overview. DESIDOC Bulletin of Information Technology. Vol.21, No.6, November 2001.
[8] Al-ogaili, H. and A.M. Shadhar, *the Finger Vein Recognition Using Deep Learning Technique.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 1-11.
[9] 2. Salim ALRikabi, H.T., et al., *Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN.* International Journal of Interactive Mobile Technologies, 2022. **16**(8).
[10] Al Mossawy, M.M.T. and L.E. George, *A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System.* Wasit Journal of Computer and Mathematics Science, 2022. **1**(1): p. 1-14.
[11] Alaidi, A.H.M., et al., *Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques.* International Journal of Interactive Mobile Technologies, 2022. **16**(10).
[12] Ahmed, H., *A Review of Hash Function Types and their Applications.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(3): p. 120-139.
[13] 6. Jaafar Q. Kadhim, I.A.A., Haider TH. Salim ALRikabi, *Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT.* International Journal of Emerging Technologies in Learning (iJET), 2023. **18**(02).
[14] Nsaif, B.G., A.H. Sallomi, and M.H. Wali, *MOBILE LOCATION PREDICTION IN CELLULAR NETWORKS by SIGNAL RECEIVED STRENGTH.* Design Engineering, 2021: p. 8804-8812.
[15] Khalifa, M.A., et al., *A Novel Arabic Words Recognition System Using Hyperplane Classifier.* Wasit Journal of Computer and Mathematics Sciences, 2022. **1**(2): p. 12-20.
[16] 9. Meteab, W.K., et al. Controlling and Monitoring a Robot-Car Based on Smart Phone Applications. in IOP Conference Series: Materials Science and Engineering. 2021. IOP Publishing.
[17] Nabaa Ali Jasim, H.T.S.A., *Design and Implementation of Smart City Applications Based on the Internet of Things.* International Journal of Interactive Mobile Technologies (iJIM), 2021. **15**(13): p. 4-15.
[18] Rusbridge, Chris. Towards the hybrid library. D-Lib Magazine. July/August 1998. http://www.dlib.org/dlib/july98/rusbridge.hunl 11. AZEEZ, TA Abdul. How to design a digital library. SRELS journal of information management, 2003, 40.3: 267-273.

Article submitted 20 November 2022. Published as resubmitted by the authors 31 December 2022.

Natural Language Processing For Automatic text summarization [Datasets] - Survey

https://doi.org/10.31185/wjcm.72

Alaa Ahmed AL-Banna(✉)
Department of Computer Science, College of Science ,Al-Nahrain University, Baghdad, Iraq.
a.muc92@yahoo.com

Abeer K AL-Mashhadany
Department of Computer Science, College of Science, Al-Nahrain University, Baghdad, Iraq.

Abstract— Natural language processing has developed significantly recently, which has progressed the text summarization task. It is no longer limited to reducing the text size or obtaining helpful information from a long document only. It has begun to be used in getting answers from summarization, measuring the quality of sentiment analysis systems, research and mining techniques, document categorization, and natural language Inference, which increased the importance of scientific research to get a good summary. This paper reviews the most used datasets in text summarization in different languages and types, with the most effective methods for each dataset. The results are shown using text summarization matrices. The review indicates that the pre-training models achieved the highest results in the summary measures in most of the researchers' works for the datasets. Dataset English made up about 75% of the databases available to researchers due to the extensive use of the English language. Other languages such as Arabic, Hindi, and others suffered from low resources of dataset sources, which limited progress in the academic field.

Keywords— Natural Language Processing, Automatic Text Summarization, Abstractive Text Summarization, Extractive Text Summarization, Text Summarization Datasets

1 Introduction

Automatic summarization is a challenge in Natural Language Processing (NLP) that involves developing algorithms that can reduce an input text, such as a scientific journal article, to a compacted version containing just the relevant information. The process of summarizing is complex because it involves not only the selection, assessment, collection, and rearrangement of information but also compression, generalization, and paraphrasing [1]. There are several types of summarizations based on the desired type of input and summary. The two major types of summarizations are Extractive and Abstractive summarizations [2]. In extractive summarization, text segments such as sentences or phrases of the most important are extracted from the original text without being modified words and concatenated to generate the summary [3].

Extractive summarization aims to identify the importance of each text sentence and develop a shorter version of the original text that represents it accurately. On the other hand, text summarization based on abstraction uses linguistic methods for understanding and a deeper analysis of the text [4]. An abstract text summary type consists of new sentences generated by paraphrasing or reformulating the extracted content [5]. Abstractive summaries are usually resembling human-written ones because they tend to represent the content and the meaning of the original text more naturally. Although this type of summarization performs more efficiently, its implementation requires great knowledge of deep learning techniques [6]. Also, the type of input documents used for summarizing may vary. The target of summarizing may be to obtain a summary from several documents or one document to obtain a summary text [7]. Single-document summarizers deal with a single source text and generate summaries from it Independently of other documents [8]. On the other hand, multi-document summarizing is viewed as an extension of a single-document summary. It compiles many documents on the same subject into a single summary. The multi-document summarization task is more complex than summarizing a single document, even if it is lengthy. The difficulty comes from handle within a large set of documents with thematic diversity [9].

1.1 Automatic Text Summarization Evaluation

The quality of the summarized text is evaluated by human assessment and using Natural Language Text Summarization metrics. ROUGE, or" Recall-Oriented Understudy for Gisting Evaluation," is the most popular matrices containing software packages for evaluating automatic summarization and translation in natural language processing. By comparing an automatically produced summary with a reference or a group of contacts (human-produced) [10]. The overlap of unigrams (per word) between the system and reference summaries is referred to as ROUGE-1. In contrast, ROUGE-2 refers to the bigram overlap between the system and reference summaries. And ROUGE-L: Statistics based on the "Longest Common Subsequence (LCS) " The longest common sub-sequence naturally considers sentence-level structural similarities and automatically determines the longest co-occurring in sequence n-grams [11]. In addition to these matrices, human evaluation is adopted based on the correct linguistic rules for the summary, the coherence of the text, etc. [12].

2 Overview of the Datasets

The dataset is the first step to getting a well-trained model to perform a specific task in artificial intelligence [13]. When summarizing texts, it is necessary to look at the available datasets, languages, types of functions, and the latest methods that led to obtaining a well-trained model. Below we review the most famous datasets that have been worked with a summary table of information:-

1) Multi-Document Summarization on "Wikipedia Current Events Portal (WCEP)"

The WCEP dataset for multi-document summarization comprises human-written summaries of news events from the ("WCEP"), each linked with a cluster of news articles. These stories are based on sources mentioned by WCEP editors and automatically collected from Common Crawl News and supplemented with items acquired automatically from t (WCEP) [14]. The best result in the dataset shown in [15] is by using the PRIMERA model by result Rouge-1=46.1 Rouge-2=25.2 Rouge-L=37.9. Multi-Document Summarization captures useful information and filters out superfluous information to summarize a series of documents. Extractive and abstractive multi-document summarization are popular. Extractive summarizing systems extract significant samples, phrases, or sections from texts, whereas abstractive summarization systems paraphrase the information [9].

2) DUC 2004 (Document Understanding Conferences)

The DUC2004 dataset is a multi-document summarization dataset used for testing. It comprises 500 news stories, each with four human-written summaries. It comprises 50 clusters of "Text REtrieval Conference (TREC) " documents drawn from the following collections: "AP newswire, 1998-2000; New York Times newswire, 1998-2000; and Xinhua News Agency (English version) "through 1996-2000. Each cluster had an average of ten papers [16]. in [17] Summarization values got their highest levels: ROUGE-1 = 28.18 ROUGE-2 = 8.49 ROUGE-L = 23.81.

3) CNN/Daily Mail

The "CNN/Daily Mail" dataset is used for summarizing text. Questions (with one of the entities obscured) and associated portions from CNN and Daily Mail news articles were manually constructed to train the algorithm to answer a fill-in-the-blank inquiry. Authors have made available scripts to crawl, extract, and produce passage and question pairs from various resources. The hands specify 11,487 test pairs, 13368 validation pairs, and 286,817 training pairs. Documents in training average 766 words and 29.74 sentences in length, whereas their summaries only use 53 comments and 3.72 sentences [18].in the latest studies in 2022 [19] using “Pegasus 2B + SLiC”, Y. Zhao and others get the best result to text summarization task in this data set, Rouge-1= 47.97, Rouge-2= 24.18, Rouge-L= 44.88.

4) PubMed ("Public/Publisher MEDLINE")

There are a total of 19717 studies on diabetes in the PubMed dataset, which may be broken down into three categories. There are a total of 44338 references in the citation web. A word vector from a vocabulary with 500 different terms is used to define each article in the dataset according to its TF/IDF importance [20]. By using transformers architectures [21] to get the best value to abstractive text summarization in ROUGE-1 =50.95, ROUGE-2= 21.93, and ROUGE-L= 45.61.

5) arXiv ("Arxiv HEP-TH (high energy physics theory) citation graph")

There are 27,770 publications included in the dataset that makes up the "Arxiv HEP-TH" citation graph, and the total number of edges is 352,807. A directed edge connects two nodes in the network if and only if paper I refers to paper J. There is no indication in the graph of any papers outside the dataset being referenced or cited by any documents inside it. Specifically, the data includes articles published between January 1993 and April 2003. (124 months) [22]. the transformer was applied to summarize the text in [21] and reached a ratio of ROUGE-1 =50.95, ROUGE-2 =21.93 ROUGE-L =45.61.

6) XSum (Extreme Summarization)

Extreme Summarizing (XSum) is a dataset for testing abstract single-document summarization methods. The objective is to write a brand-fresh, catchy one-sentence summary that explains the article's subject. A one-sentence summary is provided for each of the 226,711 news stories in the collection. Many different topics are covered in this compilation of BBC stories that span from 2010 to 2017. (e.g., "News, Politics, Sports, Weather, Business, Technology, Science, Health, Family, Education, Entertainment, and Arts"). 204,045 (90%), 11,332 (5%) and 11,334 (5%) documents make up the official training, validation, and test sets, respectively [23]. In [19], researchers work on this dataset and introduce sequence likelihood calibration (SLiC). This makes Decoding unnecessary, and the quality of decoding candidates rises dramatically independent of the decoding method. Exceed SOTA results on various generation tasks, including abstractive summarization, question creation, abstractive question answering, and data-to-text generation, even with small models. Pegasus 2B +SLiC achieved result up to ROUGE-1 =49.77, ROUGE-2 =27.09, and ROUGE-L =42.08.

7) MentSum ("Mental Health Summarization Dataset")

Mental health is still major one in the field of public health. Many people today are turning to internet forums and social media to discuss their struggles with mental health, vent their emotions, and connect with like-minded and trained professionals. The length of the articles may vary, but it is helpful to offer a brief yet relevant description so that the counselors can go through it quickly. MentSum includes over 24k hand-picked user posts from Reddit and their short user-written summary (called TL; DR) in English from 43 mental health subreddits to facilitate research into the summarization of online posts related to mental health. This domain-specific dataset could be of interest not only for generating short summaries on Reddit but also for generating summaries of posts on dedicated mental health forums such as Reachout. in 2022[24]. This paper [25]works on this dataset and evaluates extractive and abstractive state-of-the-art summarization baselines [24]. Using the BART model, better values in this research are "Rouge-1 =29.13, Rouge-2 =7.98, and Rouge-L =20.27".

8) OrangeSum

OrangeSum is an extreme summarizing dataset that focuses on a single document to summarize it. It includes two tasks, title and abstract. Title and abstract assignments have an average ground truth summary length of 11.42 and 32.12 words, whereas 315- and 350-word documents have similar average sizes. Creating a French language version of the XSum dataset was the impetus behind OrangeSum. For models to do well

in OrangeSum, they need to be more abstract than they need to be on the historical CNN, Daily Mail, and NY Times datasets. Extracting article titles and abstracts from the orange Actu website led to the development of OrangeSum. Pages scraped span over a decade, from February 2011 to September 2020, and may be roughly categorized under five broad headings: France, the globe, politics, automobiles, and society. Health, environment, people, culture, media, high technology, unusual ("insolite" in French), and miscellaneous are the eight divisions of the society event [26] .in the 2021 paper [27] provides "BARThez", the first large-scale pre-trained seq2seq model for French, in this paper. "BARThez" is particularly well-suited for generative jobs because of its BART foundation.BARThez is very competitive with cutting-edge BERT-based French language versions such as CamemBERT and FlauBERT.and also proceed to train a multilingual BART on BARThez' corpus and show that the resultant model, mBARThez, greatly improves BARThez' generative performance.

9) BookSum (Books Summarization)

BookSum is a data set library for summarizing books and other lengthy texts. Novels, dramas, and tales are some of the literary works included in this dataset, which also has highly abstractive, human-written summaries at the paragraph, chapter, and book levels. Longer texts, non-trivial causal, temporal relationships, and complex discourse structures are only some of the obstacles that summarizing algorithms must overcome in this dataset. So far, BookSum has summarized 142,753 paragraphs, 12,293 chapters, and 436 volumes [28]. Using BART-LS in [29], the measurements ROUGE-1=38.5, ROUGE-2=10.3, and ROUGE-L=36.4.

10) arXiv Summarization Dataset

For more than 30 years, ArXiv has served the public and scientific communities by offering open access to scholarly publications in fields ranging from physics to computer science and everything in between, including "math, statistics, electrical engineering, quantitative biology, and economics". This vast repository of data provides substantial but, at times, bewildering depth. This dataset is a free, open pipeline on Kaggle to the machine-readable arXiv dataset: a library of 1.7 million articles containing important information such as article titles, authors, categories, abstracts, full-text PDFs, and more, to help make the arXiv more accessible. To enable new use cases that can lead to the exploration of more profitable machine learning techniques that combine multi-modal features for applications such as trend analysis, paper recommender engines, category prediction, co-citation networks, knowledge graph construction, and semantic search interfaces. ArXiv is a community-supported, jointly financed resource created by Paul Ginsparg in 1991 and maintained and controlled by Cornell University [30]. Savelieva and others In [31], using Facet-Aware Modeling Improving Unsupervised Extractive Summarization, the best result is ROGUE-1=40.92 ROUGE-2=13.75 ROUGE-L =35.56.

11) WikiHow Dataset

"WikiHow" is a dataset of over 230,000 article-summary pairs mined from a wiki-based knowledge repository and created by various human writers. The topics covered

and the writing styles represented in these pieces have high diversity [32]. Using state-of-the-art NLP in [33] makes abstractive summaries of "recorded instructional films ranging from gardening and cooking to software configuration and sports". The model is pre-trained on a few large cross-domain datasets in written and spoken English using transfer learning. ROUGE measurement is used to evaluate, and this paper has achieved the best results and used BertSum by relying on this dataset, as it was ROUGE-1 =35.91, ROUGE-2 =13.9, ROUGE-L =34.82.

12) Urdu News Dataset

Over a million news articles from the fields of business, economics, science and technology, entertainment, and sports are included in this collection. This dataset is helpful for numerous Urdu NLP applications since its four unique categories were carefully selected to eliminate ambiguity. For many NLP, Machine/Deep Learning tasks, including "text processing, classification, summarization, named entity recognition, topic modeling, and text generation", the dataset A Large-Scale News Dataset for Urdu Text Processing is the only dataset in the Urdu language that is currently available—created this dataset.in 2021 and so far, no studies have been done on this dataset in text summarization [34].

13) Bengali News Articles ("IndicNLP")

Since the previous several decades, "natural language processing (NLP)" has been used extensively in studying Western languages, especially the English language. Language processing research on the eastern counterpart, particularly the languages of the Indian subcontinent, needs to be increased. Western languages have access to a wealth of dictionaries, WordNet, and related resources. This data collection, which has been cleaned and comes with a train and test set to compare your classification and summarization models against, contains 14k news items. A collection of Bengali news items make up this dataset. It may be applied to problems involving classification and language modeling [35]. Although there has been a substantial amount of critical study on abstractive summary in English, just a few works have been done on Bengali abstractive news summarization. Paper [36] described a seq2seq-based Long Short-Term Memory (LSTM) network architecture focused on the encoder-decoder. The suggested system uses the attention-based model to construct a long sequence of words. The summary was evaluated subjectively and statistically, and its results were compared to other published results. Mechanism of attention demonstrated a considerable improvement in state-of-the-art human assessment ratings.

14) Hindi Text Short and Large Summarization Corpus

The "Hindi Text Short and Large Summarization Corpus" is a collection of 180k articles with headlines and summaries taken from Hindi news websites. This is a first-of-its-kind Hindi Dataset that may be used to benchmark algorithms for Hindi text summarization. This does not include articles from this dataset, which is being released concurrently with this Dataset. The dataset preserves the articles' original punctuation, numerals, and other formatting [37]. In 2022 [38] executed the Hindi text summarization, which had received relatively little attention. A machine learning model has been developed and evaluated using around 100,000 data samples, resulting in highly

accurate summaries that benefit society. The model has an F-Score of 58% and a Rouge Score of 67.5%. Pandas, NumPy, sklearn, and other libraries are utilized.LSTM, word embedding and seq2seq are used to train the data model.

15) Arabic News articles from Aljazeera.net

Natural Language Processing (often known as NLP) is a highly researched area of machine learning. Recent years have seen significant development, paving the way for this field's expansion into widespread use across various contexts. Today, natural language processing (NLP) is used in several contexts, including but not limited to: social media platforms, search engines, translation apps, Chabot helpers, and many more. Progress and outcomes, however, vary from language to language. Most ML systems only care about English and ignore other languages, particularly Arabic. A primary cause of this is the scarcity of relevant datasets. This data collection comprises around 5870 Arabic-language news stories extracted from the aljazeera.net website [39]. An abstractive Arabic text summarization model based on RNN is proposed and used in this dataset in this study [40]. A multilayer encoder and a single-layer decoder are included. Encoder layers use bidirectional long short-term memory, whereas decoder levels use unidirectional long short-term memory. The evaluation shows that the model produced is the best, achieving ROUGE1=38.4.

16) COVID-19 Open Research Dataset Challenge (CORD-19)

In response to COVID-19, the White House and prominent academic organizations created the COVID-19 Open Research Dataset (CORD-19). CORD-19 has almost 1,000,000 academic publications on COVID-19, SARS-CoV-2, and similar coronaviruses, including over 400,000 in full text. This free dataset is supplied to the worldwide research community to utilize natural language processing, and other AI approaches to develop new insights in the battle against this deadly illness. The tremendous increase in coronavirus literature makes it challenging for medical researchers to stay up [41]. In 2022 paper [42] proposes a hybrid, unsupervised, abstractive approach that walks through a document, generating salient textual fragments representing its key points. We then select the most important sentences of the paper by choosing the most similar sentences to the generated texts, calculated using BERTScore.and this method achieved ROUGE-1 =41.02, ROUGE-2=13.79, ROUGE-L =37.25, in the text summarization measures', which are considered the best among the works submitted on this dataset.

17) Scientific Document Summarization (SciTLDR)

A new multi-target dataset of 5.4K TLDRs over 3.2K papers. SciTLDR contains both author-written and expert-derived TLDRs in computer science. The latter are collected using a novel annotation protocol that produces high-quality summaries while minimizing the annotation burden [43]. In this dataset train =1992, valid =618, test=619.The first paper published in this data set is [44] introducing TLDR generation for scientific papers and releasing SCITLDR, a multi-target dataset of TLDR-paper pairs. The result is RPOGE-1=43.8, ROUGE-2=20.9 ROUGE-L=35.5 Using pretrained models. This data set is considered one of the difficult types due to the small

number of samples and the difficulty of training them, which is why researchers often resort to pre-training and fine-tuning methods.

18) ScisummNet Corpus

This massive corpus may be used to train citation-based summarization algorithms for scientific papers, opening new avenues of inquiry into supervised approaches. This dataset includes 1,000 samples. Has been organized since 2014 in computational linguistics and NLP papers[45]. Group of researchers in [46] using BertSum, Continual BERT, Adapter-based BERT, and SummaRuNNer in PubMed and ScisummNet datasets. Bertrum outperforms other pre-trained models used on the ScisummNet dataset, archives result to ROUGE-1= 33.0, ROUGE-2 = 13.4, ROUGE-L= 31.6, but PubMed is better In terms of assessment scores because of phrases use of complex and specialized medical terminologies rather than ScisummNet's general scientific phrases.

19) SUMARABIC

SumArabic is a dataset for abstractive text summarization in Arabic. The information comes from two Arabic news websites: emaratalyoum.com and emaratalyoum.com. - www.almamlakatv.com.The data is divided into four sets: training, testing, validation, and out-of-domain. Each split has the following examples: 75,817 training, 4,121 validations, and 4,174 tests. 652 out-of-domain, Total: 84,764 [47].This dataset is one of the latest additions to 2022 in the Arabic language, which does not contain academic studies on it yet.

20) TalkSumm

TalkSumm is a dataset that contains 1705 automatically-generated summaries papers in science from ACL, NAACL, EMNLP, SIGDIAL (2015-2018), and ICML (2017-2018). The dataset contains titles, URLs, and corresponding summaries. [48]This study presents a unique way for automatically producing summaries for scientific publications based on recordings of lectures at scientific conferences, suggesting that such presentations provide a cohesive and short summary of the paper's content and can serve as the foundation for effective summaries. It compiled a collection of paper summaries from 1716 publications and their accompanying videos. A model trained on this dataset outperforms models trained on a manually constructed dataset of summaries. Furthermore, human specialists confirmed the quality of our this summary [49].

Table 1. Summarizes the basic information of the dataset used to text summarization from Language of dataset ،content ،Input document Single or Multiple and Referring to the best research and methods that achieved the highest percentages in summary matrices

Dataset Name	**Dataset Language**	**Dataset Field**	**Input Type Single/ Multiple**	**Output types Abstractive /Extractive**	**Author Ref. /Methods**	**Result**
1. Multi-Document Summarization on WCEP [14]	English	news articles	Multi documents	Extractive	W. Xiao et al.[14] \ Primer	ROUGE-1=46.1 ROUGE-2=25.2 ROUGE-L=37.9
2. DUC 2004 [16].	English	news articles	Multi documents	Extreme/ Abstractive	S. Shen et al.[17] \ wise sentence	ROUGE1= 28.18 ROUGE-2=8.49 ROUGEL= 23.81
3. CNN/Daily Mail [18]	English	news articles	Single document	Abstractive	Y. Zhao et al.[19] \Pegasus 2B +SLiC	ROUGE-1=47.97 ROUGE-2=24.18 ROUGE-L 44.88
4. PubMed[20]	English	scientific	Single document	Abstractive	B. Pang et al. [21] \Transformer	ROUGE-1=50.95 ROUGE-2=21.93 ROUGE-L=45.61
5.arXiv ("Arxiv HEP-TH (high energy physics theory) citation	English	scientific	Single document	Abstractive	B. Pang et al. [21] \Transformer	ROUGE-1=50.95 ROUGE-2=21.93 ROUGE-L=45.61

graph) " [22]						
6. XSum [23]	English	News ("Politics, Sports, Weather, Business, Technology, Science, Health, Family, Education, and Arts")	Single document	Extreme/ Abstractive	Y. Z o et al.[19] \Pegasus 2B +SLiC	ROUGE-1=49.77 ROUGE-2=27.09 ROUGE-L=42.08
7.MentSum ("Mental Health Summarization Dataset") [24]	English	Mental health	Single document	Extreme/ Abstractive	S. Sotudeh et al.[25] \ BART	ROUGE-1=29.13 ROUGE-2=7.98 ROUGE-L=20.27
8. OrangeSum [26]	French	society	Single document	Abstractive	M. K. Eddine et al. [27]\BARThez'	ROUGE-1=15.49 ROUGE-2=5.82 ROUGE-L=13.05
9.BookSum [28]	English	literary works	Single document	Abstractive	W. Xiong et al. [29] \ BART-LS	ROUGE-1=38.5 ROUGE-2=10.3 ROUGE-L=36.4
10.arXiv Summarization Dataset [30]	English	scientific	Single documents	Extractive	Liang et al. [31] \Facet-Aware Modeling	ROGUE-1=40.92 ROUGE-2=13.75 ROUGE-L=35.56

11.Wiki-How [32]	English	article	Single documents	Abstractive	Savelieva et al. [33] \ BertSum	ROUGE-1 =35.91 ROUGE-2 =13.9 ROUGE-L =34.82
12. Urdu News Dataset [34]	Urdu	news articles	single documents	-	-	-
13. Bengali News Dataset [35]	Bengali	news articles	Single documents	Abstractive	Bhattacharjee et al.[36] \ LSTM	Humans Evaluation
14. Hindi Text Short and Large Summarization Corpus [37]	Hindi	Hindi news	Single documents	Abstractive	Shah et al.[38] \ LSTM+ word embedding	F-Score =58% Rouge =67.5 %
15. Arabic News articles from Aljazeera.net [39]	Arabic	News articles	Single documents	Abstractive	Suleiman et al .[40]\ RNNs	ROUGE-1=38.4
16. COVID-19 Open Research Dataset Challenge (CORD-19) [41]	English	Scientific	Single documents	Abstractive	Bishop et al. [42] \ GenCompareSum	ROUGE-1= 41.02 ROUGE-2 = 13.7 ROUGE-L= 37.25
17.Scientific Document Summarization ("SciTLDR") [43]	English	Scientific	Single documents	Extreme/ Abstractive	Cachola et al.[44] \ CATTS	-
18.ScisummNet Corpus [45]	English	Scientific	Single documents	Abstractive	Park et al. [46]\ BertSum	ROUGE-1= 33.0 ROUGE-2 = 13.4 ROUGE-L= 31.6

19. SumArabic [47]	Arabic	News	Single documents	Abstractive	-	-
20. TalkSumm [48]	English	Scientific	Single documents	Abstractive	Lev et al.[49] \	-

3 Conclusion

This review concludes that the dataset's field in summarizing texts is focused on news and scientific aspects, especially the abstract type. The available datasets lack diversity in topics, primarily literary, artistic, and some fields of science. The dataset available in a large size can be used to train the model, fine-tune a small emerging data set, and get good results. After the significant development in text summarization techniques, getting a good summary has become the beginning of other tasks related to NLP.

4 References

[1] Suleiman, Dima, and Arafat Awajan. "Deep learning based abstractive text summarization: approaches, datasets, evaluation measures, and challenges." Mathematical problems in engineering 2020 (2020).
[2] Munot, Nikita, and Sharvari S. Govilkar. "Comparative study of text summarization methods." International Journal of Computer Applications 102, no. 12, 2014.
[3] V. Gupta and G. S. Lehal, "A survey of text summarization extractive techniques," Journal of emerging technologies in web intelligence, vol. 2, no. 3, pp. 258-268, 2010.
[4] Sinha, Aakash, Abhishek Yadav, and Akshay Gahlot. "Extractive text summarization using neural networks." arXiv preprint arXiv: 1802.10137, 2018.
[5] W.-T. Hsu, C.-K. Lin, M.-Y. Lee, K. Min, J. Tang, and M. Sun, "A unified model for extractive and abstractive summarization using inconsistency loss," arXiv preprint arXiv:1805.06266, 2018.
[6] Nallapati, Ramesh, Bowen Zhou, Caglar Gulcehre, and Bing Xiang. "Abstractive text summarization using sequence-to-sequence rnns and beyond." arXiv preprint arXiv:1602.06023, 2016.
[7] [C.-Y. Lin and E. Hovy, "From single to multi-document summarization," in Proceedings of the 40th annual meeting of the association for computational linguistics, 2002, pp. 457-464.
[8] Christian, Hans, Mikhael Pramodana Agus, and Derwin Suhartono. "Single document automatic text summarization using term frequency-inverse document frequency (TF-IDF)." ComTech: Computer, Mathematics and Engineering Applications 7, no. 4 (2016): 285-294.
[9] Mutlu, Begum, Ebru A. Sezer, and M. Ali Akcayol. "Multi-document extractive text summarization: A comparative assessment on features." Knowledge-Based Systems 183 (2019): 104848.

[10] Lin, Chin-Yew. "Rouge: A package for automatic evaluation of summaries." In Text summarization branches out, pp. 74-81. 2004.
[11] Ozsoy, Makbule Gulcin, Ferda Nur Alpaslan, and Ilyas Cicekli. "Text summarization using latent semantic analysis." Journal of Information Science 37, no. 4 (2011): 405-417.
[12] Gong, Yihong, and Xin Liu. "Generic text summarization using relevance measure and latent semantic analysis." In *Proceedings of the 24th annual international ACM SIGIR conference on Research and development in information retrieval*, pp. 19-25. 2001.
[13] *Wissner-Gross, A. ." Edge.com. Retrieved 8 January 2016.*
[14] Demian Gholipour Ghalandari; Chris Hokamp; Nghia The Pham; John Glover; Georgiana Ifrim, WCEP Dataset [Dataset]. https://paperswithcode.com/dataset/wcep
[15] W. Xiao, I. Beltagy, G. Carenini, and A. Cohan, "Primer: Pyramid-based masked sentence pre-training for multi-document summarization," *arXiv preprint ar X iv: 2110.08499*, 2021.
[16] DUC 2004 Dataset [Dataset]. https://paperswithcode.com/dataset/duc-2004
[17] S. Shen, Y. Zhao, Z. Liu, and M. Sun, "Neural headline generation with sentence-wise optimization," *arXiv preprint arXiv:1604.01904*, 2016.
[18] Ramesh Nallapati; Bo-Wen Zhou; Cicero Nogueira dos santos; Caglar Gulcehre; Bing Xiang, CNN/Daily Mail Dataset [Dataset]. https://paperswithcode.com/dataset/cnn-daily-mail-1.
[19] Y. Zhao, M. Khalman, R. Joshi, S. Narayan, M. Saleh, and P. J. Liu, "Calibrating Sequence likelihood Improves Conditional Language Generation," *arXiv preprint ar X iv: 2210.00045*, 2022.
[20] datadiscovery.nlm.nih.gov (2021). PubMed [Dataset]. https://healthdata.gov/dataset/PubMed/h5mw-dwr6 .
[21] B. Pang, E. Nijkamp, W. Kryściński, S. Savarese, Y. Zhou, and C. Xiong, "Long Document Summarization with Top-down and Bottom-up Inference," *arXiv preprint arXiv:2203.07586*, 2022.
[22] ArXiv Dataset [Dataset]. https://paperswithcode.com/dataset/arxiv.
[23] Shashi Narayan; Shay B. Cohen; Mirella Lapata, XSum Dataset [Dataset]. https://paperswithcode.com/dataset/xsum
[24] Sajad Sotudeh; Nazli Goharian; Zachary Young (2022). Mental Health Summarization (MentSum) [Dataset]. https://ir.cs.georgetown.edu/resources/mentsum.html.
[25] S. Sotudeh, N. Goharian, and Z. Young, "MentSum: A Resource for Exploring Summarization of Mental Health Online Posts," *arXiv preprint arXiv:2206.00856*, 2022.
[26] Moussa Kamal Eddine; Antoine J. -P. Tixier; Michalis Vazirgiannis, OrangeSum Dataset [Dataset]. https://paperswithcode.com/dataset/orangesum.
[27] M. K. Eddine, A. J.-P. Tixier, and M. Vazirgiannis, "Barthez: a skilled pretrained french sequence-to-sequence model," *arXiv preprint arXiv:2010.12321*, 2020.
[28] Wojciech Kryściński; Nazneen Rajani; Divyansh Agarwal; Caiming Xiong; Dragomir Radev, BookSum Dataset [Dataset]. https://paperswithcode.com/dataset/booksum .
[29] W. Xiong, A. Gupta, S. Toshniwal, Y. Mehdad, and W.-t. Yih, "Adapting Pretrained Text-to-Text Models for Long Text Sequences," *arXiv preprint arXiv: 2209.10052*, 2022.
[30] Arman Cohan; Franck Dernoncourt; Doo Soon Kim; Trung Bui; Seokhwan Kim; Walter Chang; Nazli Goharian (2021). arXiv Summarization Dataset Dataset [Dataset]. https://paperswithcode.com/dataset/arxiv-summarization-dataset.
[31] Liang, Xinnian, Shuangzhi Wu, Mu Li, and Zhoujun Li. "Improving unsupervised extractive summarization with facet-aware modeling." The Association for Computational Linguistics Findings*: ACL-IJCNLP 2021*, pp. 1685-1697. 2021.
[32] Mahnaz Koupaee; William Yang Wang (2021). WikiHow Dataset [Dataset]. https://paperswithcode.com/dataset/wikihow

[33] Savelieva, Alexandra, Bryan Au-Yeung, and Vasanth Ramani. "Abstractive summarization of spoken and written instructions with BERT." arXiv preprint arXiv:2008.09676 (2020).
[34] Saurabh Shahane (2021). Urdu News Dataset [Dataset]. https://www.kaggle.com/saurabhshahane/urdu-news-dataset
[35] PrithwirajSust (2020). Bengali News Summarization Dataset [Dataset]. https://www.kaggle.com/prithwirajsust/bengali-news-summarization-dataset
[36] Bhattacharjee, Prithwiraj, Avi Mallick, and Saiful Islam. "Bengali abstractive news summarization (BANS): a neural attention approach." In *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*, pp. 41-51. Springer, Singapore, 2021.
[37] Gaurav (2020). Hindi Text Short Summarization Corpus [Dataset]. https://www.kaggle.com/disisbig/hindi-text-short-summarization-corpus
[38] Shah, Aashil, Devam Zanzmera, and Kevan Mehta. "Deep Learning based Automatic Hindi Text Summarization." In *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1455-1461. IEEE, 2022.
[39] Abdelkader Rhouati (2020). Arabic News articles from Aljazeera.net [Dataset]. https://www.kaggle.com/arhouati/arabic-news-articles-from-aljazeeranet .
[40] Suleiman, Dima, and Arafat Awajan. "Multilayer encoder and single-layer decoder for abstractive Arabic text summarization." Knowledge-Based Systems 237 (2022): 107791.
[41] Allen Institute for AI (2020). cord-19 [Dataset]. https://allenai.org/data/cord-19 .
[42] Bishop, Jennifer, Qianqian Xie, and Sophia Ananiadou. "GenCompareSum: a hybrid unsupervised summarization method using salience." In *Proceedings of the 21st Workshop on Biomedical Language Processing*, pp. 220-240. 2022.
[43] Aaditya Raj (2022). Scientific Document Summarization (SciTLDR-A) [Dataset]. https://www.kaggle.com/datasets/adityawithdoublea/scitldra .
[44] Cachola, Isabel, Kyle Lo, Arman Cohan, and Daniel S. Weld. "TLDR: Extreme summarization of scientific documents." *arXiv preprint arXiv:2004.15011*, 2020.
[45] Michihiro Yasunaga; Jungo Kasai; Rui Zhang; Alexander R. Fabbri; Irene Li; Dan Friedman; Dragomir R. Radev (2021). ScisummNet Dataset [Dataset]. https://paperswithcode.com/dataset/scisummnet .
[46] Park, Jong Won. "Continual bert: Continual learning for adaptive extractive summarization of covid-19 literature." *arXiv preprint arXiv:2007.03405*, 2020.
[47] Mohammad Bani Almarjeh (2022). SumArabic [Dataset]. http://doi.org/10.17632/7kr75c9h24.1 .
[48] Guy Lev; Michal Shmueli-Scheuer; Jonathan Herzig; Achiya Jerbi; David Konopnicki, TalkSumm Dataset [Dataset]. https://paperswithcode.com/dataset/talksumm .
[49] Lev, Guy, Michal Shmueli-Scheuer, Jonathan Herzig, Achiya Jerbi, and David Konopnicki. "Talksumm: A dataset and scalable annotation method for scientific paper summarization based on conference talks." *arXiv preprint arXiv:1906.01351* , 2019.

Article submitted 23 October 2022. Published as resubmitted by the authors 31 December 2022.

Steganography Based on Chaotic System for Random LSB Positions

https://doi.org/10.31185/wjcm.95

Rusul Mansoor Al-Amri (✉)
Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq
College of Nursing, University of Al-Ameed Karbala, PO No: 198 Iraq
sosoalhaji28@gmail.com

Dalal N. Hamood
Computer Department/College of Science University AL-Nahrain, Baghdad, 10001, Iraq
dalal.naeem@ced.nahrainuniv.edu.iq

Alaa Kadhim Farhan
Department of Computer Sciences, University of Technology, Baghdad 10011, Iraq
dalal.naeem@ced.nahrainuniv.edu.iq

Abstract—The objective of hiding text in an image is hiding text without raising suspicions that the image contains a hidden message or text, which leads to protecting and maintaining text confidentiality. The previous hiding methods have problems in capacity, randomization, and imperceptibility. This paper will be solved some of these problems; we suggested a new method for hiding text in an image. Firstly, encrypting the text by the AES-192 bit algorithm for obtaining a secret message. When the initial key of the AES-192 (bit) algorithm is generated by a chaotic system for randomness purposes, secondly, hiding the secret message is into a gray image for obtaining a stego-image. The hiding step is based on a proposed map that chooses from the last round of key expansion in the AES-192 algorithm. This map represented random positions of LSB in each byte of the gray image. The experimental result of this method proved a successful method based on metric criteria. Also, this method is the very speed for hiding ciphertext in the gray image as well as extracting ciphertext from the gray image. Also, it is very safe because it is difficult for attackers to distinguish between the original image and the stego image therefore the correlation between the original image and the stego- image is very close to 1.

Keywords— Chaotic System, Gray Image, Stego-image, LSB Technique.

1 Introduction

Covered Text" is a word synonymous with Steganography. The hiding texts, data and information is very important[1],[2], as it aims to hide data without raising suspicions that it contains a hidden message or file, which leads to protecting it and maintaining its confidentiality[3]. The science of invisibility is completely different from the science of cryptography. To simplify the meaning, data encryption is

represented as a safe that contains data, texts, and information. The safe can only be opened with a specific key, while steganography only refers to camouflaging [4], [5]-[6]. In reality, steganography is an integral part of cryptography after the process of encrypting the text in one of the well-known encryption algorithms and after obtaining the ciphertext, the ciphertext is hidden under the cover and, steganography used to protect data from unauthorized persons [7]. Just as the protection of information requires a great effort, some encryption and concealment algorithms have had great success in concealing information, but some algorithms suffer from delaying the encryption time, delaying the time of concealment, and the quality of concealment. In this research, we have strived to achieve a balance between the speed of the encryption process and proposing a steganography map that achieves very high quality. The chaotic system was used to generate the encryption key. Chaos is one of the conducts that connect nonlinear systems and that develops specific values of an information system [8]. The discovery of this random system was considered a revolution that led to many interrelated issues, stability theory, new engineering features, and offers to distinguish signatures. The chaotic function has been used mainly to develop mathematical models for non-linear systems and has been attracted by many mathematicians because of the high sensitivity of the initial value and its applications to daily life problems [9]. The chaotic functions have good features "sensitivity to initial conditions", Fractal dimensions, the Lyapunov exponent, "strangeness", and ECT [10], [11], therefore, it used in this research to generate the encryption key (Symmetric key) of the AES-192 bit algorithm to increase the confidentiality of the transmitted information and secure the transmission process. Also, the chaotic system is characterized by there are many types of chaotic functions, each of which has an advantage over the others of these types: Lorenz Equation., Rössler Equation, and Logistic Equation (this function has been used in our work) [12]. In this research, the chaotic system was used to generate the encryption key, and this is one of the most prominent strengths in our work, as it helped to increase the strength of the encryption and the speed of generating the encryption key, also use the last round of key expansion such as random positions of LSB technique for hiding secret text into gray image, therefore, the chaotic system helps the process of encryption and concealment gained durability and Speed and success this the proposed method. Section 2 describes some of the related work; Section 3 describes the proposed method; section 4 describes the experiments and results. Conclusions are explained in Section 5

2 Literature Review

Hussein L. Hussein [13] in this Search Steganography has done several masking methods according to the proposed maps to hide the message inside a gray image, so that the text is masked by drawing a map from ASCII that used (AMT) to create an encrypted table by mapping the text message and matching some bits with the cover image. The result is referred Low computational efficient performance to be used for multiple purposes Applications. Alaa Kadhim F and Rasha Subhi Ali [14] in this research, an advanced map was used to hide data, with which they used biotechnological methods for encryption and to improve the strength of data security while hiding

messages inside an image. In this research, data hiding using LSB and DNA arithmetic were presented and they presented a new secret map to hide the data. (DNA) computing was used to encrypt data, and LSB was used to arrange the encrypted data to the least important elements of the cover, and they used a new secret map to locate locations. And Steganography. The researchers pointed out that the same equation is used for both the sender and the receiver to create a map, and this map depends on a common key.

Alaa Kadhim Farhan , Nadia M.G. Al-Saidi, Abeer Tariq Mold, Fahimeh Nazarimehr and Iqtadar Hussain [15], in this research, a new and unique chaotic system has been proposed, represented by crossing inside and outside the cylinder repeatedly. As an engineering system, the efficiency of the system in encryption images was tested. The performance of the encryption method is analyzed using the histogram, correlation coefficient, Shannon entropy, and encryption quality. The results show that the encryption method using the proposed chaotic system has reliable performance. Relying on this system and the tests conducted on it, the same tests were used in the research and the proposed method for our work.

Jagan Raj Jayapandiyan, Ph.D. Research Scholar, Kavita, Assistant Professor and Sakthivel and Professor [16] this proposed work improving the (LSB) method is based on the spatial domain. The proposed method is based on encrypting the text in two stages. The first stage is creating metadata and storing header information in the first few bytes of the images. The second stage is the process of including secret texts. Inside the cover image using the improved method, and in this proposed method, it results in the acquisition of space or a lesser method for the secret message in the cover image, and this leads to improving the quality of masking and obtaining standards for better results than the results obtained (eLSB). Our research presented in this paper has obtained much better results than the results obtained in this method in terms of evaluation criteria, and the consideration has been taken from several. This method will be encoded (eLSBRAISDSCSO) in our research in order to compare it with its results.

Ranyiah Wazirali, Waleed Alasmary, Mohamed Mahmoud and Ahmad Alhindi [17], In the research, the researchers presented a proposal for a new information steganography that works on the basis of a genetic algorithm. The researchers confirmed that this research works to increase the embedding capacity and reduce distortion. The research showed that scanning is better for pixels for vertical and horizontal directions, circular transformation, secret bit fluctuation, and transmission of confidential information after using the genetic algorithm. The (LSB) to include the data and the evaluation criteria were applied to it. The paper for our work was compared with this work and it was proven that the work presented in our research is better in terms of evaluation metrics. This method will be encoded (AOSHCAIUGA) in our research in order to compare it with its results.

Mansoor Fateh, Mohsen Rezvani, and Yasser Iran [19], In this paper, the LSB approach has been proposed with an updated version, where the proposed matching approach works to LSB that the number of bits in the secret text is greater than 2 The work has been clarified in two steps, the first is to hide the secret text and the second is

to extract the text. It has been shown that the method of the proposed approach needs to be changed less than LSBMR when the number of bits is greater than 2. The capacity in the proposed approach is higher than the F5 method when the number of the bit =3, where it was found that the number of secret text bits is greater than 2, its value = 75% this method is considered a new coding method because it reduces the change in the image. The results showed that this new method provides a 10% larger detection error for SRNet via two Steganography schemes. This method will be symbolized in our research (CFSLSB) in order to be compared with its results.

Ali Salem Ali, Mohammed Sabbih Hamoud Al-Tamimi and Alaa Ahmed Abbood [18], in this research improvement of the (Bit Inverting Map) method of narrowing the gap to obtain effective results to maintain a balance between image accuracy, protection, and security. Comparisons of this method with previous methods have proven that the method is effective and superior to the rest of the methods. This method will be symbolized in our research (SISTMS) in order to be compared with its results.

3 Method

In the proposed method, the chaotic system was used to generate the encryption key, and this is one of the most prominent strengths in our work, as it helped to increase the strength of the encryption and the speed of generating the encryption key, also use the last round of key expansion such as random positions of LSB technique for hiding secret text into the gray image as shown in figure 1. The proposed method consists of two phases: the hiding phase and Extracting Phase. Both phases have two parts: cryptography and steganography. The hiding phase consists of the encryption process and the hiding process. Also, extracting phase consists of the decryption process and extracting process.

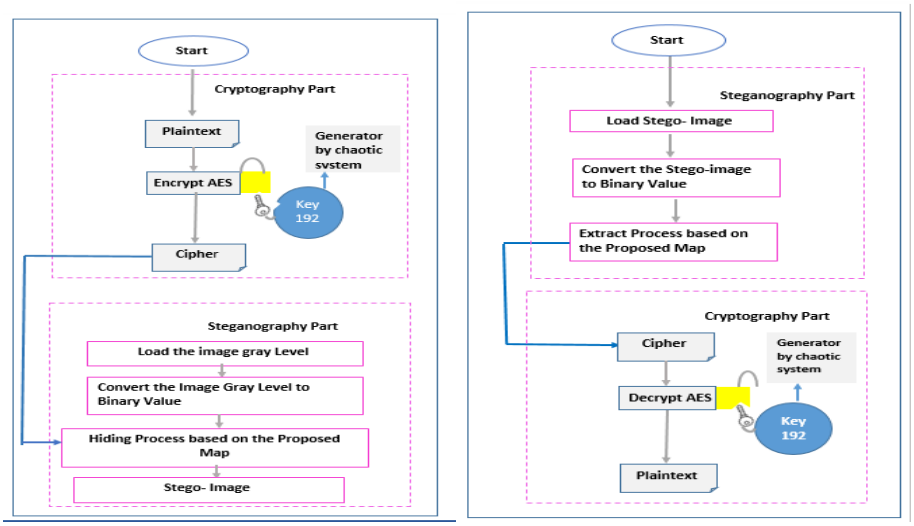


Fig. 1. Main flowchart of the proposed method: (a) hiding phase and (b) extracting phase

In cryptography part, the AES-192 (bit) algorithm used for encrypting a text. The text consists of different lengths of characters. This algorithm has several advantages in terms of:

- Security: AES has the ability to resist attacks better than other encryption algorithms.
- Cost: This algorithm includes unlimited global domain and royalty-free.
- Implementation: The AES algorithm is flexible and well suited when implemented in hardware and software.

The AES-192 (bit) used because it is more complex than the AES-128 (bit) and less expensive than the AES-256 (bit). The initial key generated by chaotic system where a 24-digit was generated randomly each time to generate the key. The chaotic system was chosen in the generation of the key in order to achieve high protection strength and an increase in the chaos of key generation and the difficulty of predicting it. Where modern methods were used in chaotic sampling of data TOA (Time - of - arrival) in chaotic samples instead of random samples, and thus we will produce a sequence of chaotic values called (Chaotic sequences). And as we know that the chaotic system is a non-linear system its structure is unstable and the output behaves as a random behaviour in some steps and depends on the (initial condition) and (control parameters).in order to determine the (Localization GD) and therefore equation (1) is the equation of the simple chaos logistics function chosen to generate the key of the algorithm AES192 bits. [20, 21]:

$$(X_{N+1}) = \lambda X_N (1 + X_N) \quad (1)$$

Where, N = 0, 1……..... L= Length of Sequence λ = control Parameter

Table 1 shows chaotic system generated a different sequence with a different initial value. This key is distinguished by the speed of generation and the strength of the key, as it is difficult to predict the value of the key by an attacker.

Table 1. The chaotic system generated a different sequence with a different initial value

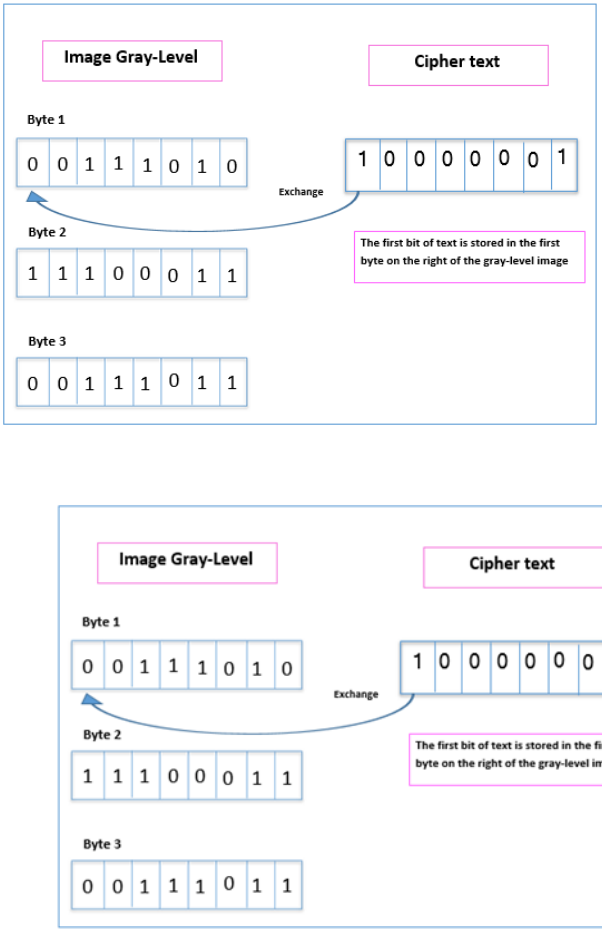
No	Initial value	Initial key (sequence)
1	0.33	131301301230123130013132
2	0.93	312222301223013023000123
3	0.20	123122301302300000122230
4	0.59	230130123230000013000130

In the steganography part, the secret message hides in gray image based on a map that represented a random positions of the LSB as shown in table 2. The proposed map represented last round of key expansion in the AES-192 algorithm. In the map, when the value equal to 1, meaning hide one bit from secret message into the byte of gray image, when the value equal to 2, meaning hide two bits from secret message into the byte of gray image, when the value equal to 3, meaning hide three bits in the byte, and when the value equal to zero, meaning no hide in the current byte of the gray image. This map repeated for the length of secret message.

Table 2. The proposed hiding map (last Round of Key Expansion)

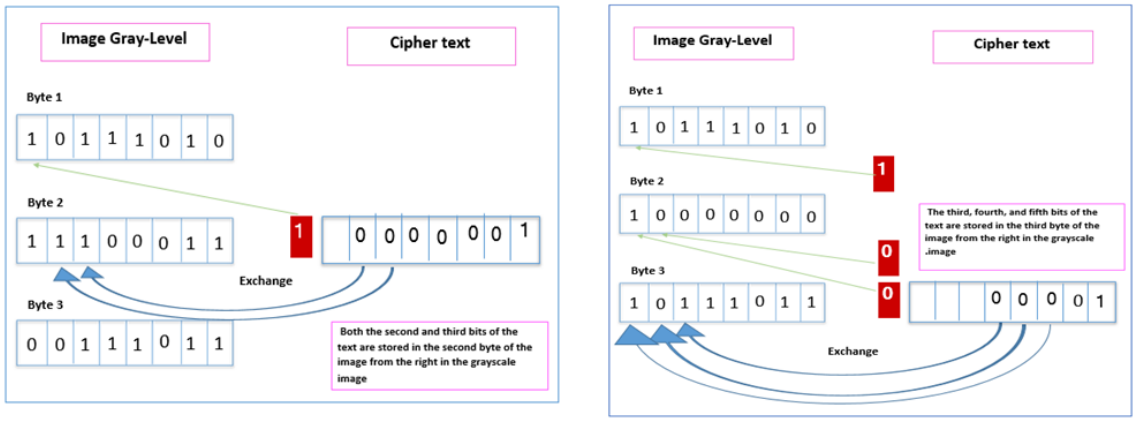
No.	Value in Hex	Decimal number	Map (Reminder of 3)
1	58	88	1
2	9d	157	1
3	36	54	0
4	Eb	235	1
5	fd	253	1
6	ee	238	1
7	38	56	2
8	7d	125	2
9	0f	15	0
10	Cc	204	0
11	9b	155	2
12	ed	237	0
13	4c	76	1
14	40	64	1
15	46	70	1
16	bd	189	0

The hiding process explains by the following example, suppose the ciphertext =" 10000111", gray sub-image (Byte1=00111010, Byte2=11100011, Byte3=00111011) and map=123. The first step, hide the first bit of cipher text "1"



(a)

in the LSB of the first byte of gray sub-image as shown in figure 2(a). In the second step, hide the second and third bits of ciphertext "00" in the LSB of the second byte of gray sub-image as shown in figure 2(b). The third step, hide the fourth,fifth,and sixth bits of cipher text "001" in the LSB of the third byte of gray sub-image as shown in figure 2(c).



(b) (c)

Fig. 2. (a) (b) (c) Hide the secret message into gray image based on random positions of the LSB

4 Results and Discussion

In testing the proposed system for variant data and testing many coefficients for both the cryptography part and steganography parts. Take as an example 10 plaintext with different lengths and 10 gray images (or colored image transform for gray image) for the text steganography.

4.1 Cryptography Part

This is the first part of the proposed system, applying the AES 192-bit algorithm. The initial key generated by the chaotic system, table 3 illustrated the different lengths of the plaintext that take different times for the encryption process, including the key generation time that generation chaotic system for achieving randomness. The encryption time is measured by picosecond because of the faster encryption process.

Table 3. Encryption time for different lengths of plaintext and Hiding Time for different lengths of Ciphertext

No	Plaintext (Char)	CipherText	Length Text char) (	Length Text Bl) ock (	Encryption Time Picosecon) (d

1	Securities	7BC5FC6DF981BDC1E687B98791DE84D9	10	1B	00:00:00.0064022
2	College Science	481CE5A868F5CB5ED9F87717C7A6C5E0	15	1B	00:00:00.0103620
3	Al-Nahrain University	8030D2C95DA1430D66F1385557C2E2E3F02E29F7000AB2FB75D0A7BEE8BE340D	20	2B	00:00:00.0120211
4	InThisResearchWeUsedidea	8076498979C11B952B839A5DEA0D94619173B9401AED39295CBF95572814BA87	25	2B	00:00:00.0124387
5	(AES) Algorithm With Key .192	EED071F281E768317BD54481D10369D9DE3868457A88825422C0E3044985830C	30	2B	00:00:00.0124844
6	The Texts Consisting Of Difference	D30281A802181D32B92B861E78C8E07C7544E7EF03A6E347CA45EB39CD6E4B9425D3DCEE784DF67BDEA4E171A871FE3F	35	3B	00:00:00.0124889
7	Cost: This Algorithm Includes Unlimited	9E0F3765EB13C54DBC8C5FA2FD85D0AD71BF9799BD905AA27AE7B12070442A836E8F9548FC2BA2A92093D6C30B7382CB	40	3B	00:00:00.0125163
8	Implementation: The AES Algorithm Is Flexible	B28CC01C55D49FBDDE13FFFF234AC59DB2B7	45	3B	00:00:00.0126289

		A3B7656182B6C CB57BACB6F6F A7AF2EBFA 3401D8CF9E8F8 24E905D395BF			
9	The 192 Cipher Keys Was Used Be-cause It Is More	90A38700717B8 59CFD01E929C E08D04B45 BDBDCDDDCE CF93CBA2D8CE B5E1F4FC88 2D4C132E0D65 B52E9BD9084D 039AA80819 E07D285241915 A9BEDA11F925 859	50	4B	00:00:00.0 134009
1 0	And After Selecting The Image We Convert The Value Of Each Pixel In The Image To The Binary System.	7BA3A6573629A46F BDF58EA123829222 8E F6E9AD3CCC1622E 641970214EF4557DA DA D8ABFE3DFF914806 CB8D4C0326ABDD A3A A636E8A49F76DBD B24C8B530F1EF5E2 57F9 EC7E07A14381289C F8E0E10DA3BAC4B 019F 5E1F013DA331277D D27B42B58FF6F	100	7B	00:00:00.0 855387

From the above result in table 3, the range of the plaintext from 10 (char) to 100 (char) in the other words, the range of the plaintext from (1) Block to (7) Block when increases the plaintext length due to increase the encryption time. The positive Relationship between the encryption time and plaintext length, as shown in figure 3.

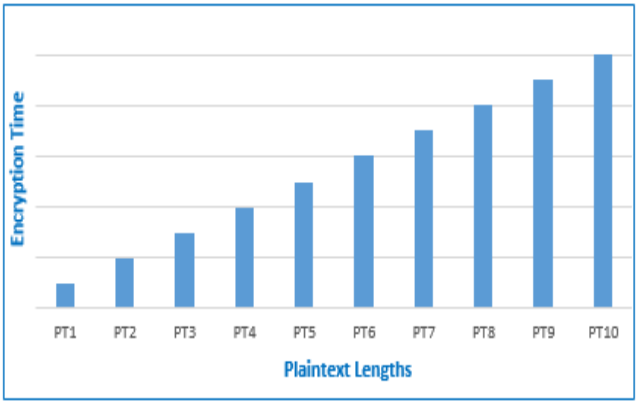


Fig. 3. The positive Relationship between Encryption Time and Plaintext lengths.

The proposed method that used chaotic system to generate initial key of the AES-192-bit standard algorithm, when examined the security of the cipher text against attacking by using the NIST. The proposed method proved is the strongest security and its success in all testing. Table 4 explains the cipher text encrypted by using key generation of chaotic system. From the result explain in table 4 the proposed modified key generation is stronger because its very secure ciphertext against the most attacks in all different cases.

Table 4. NIST Test for The Ciphertext that Encrypted based on Chaotic System

No	The Proposed AES-192 bit Proportion														
	Attacks / Ciphertext	Frequency	Block-Frequency	cumulative-sums	cumulative-sums	runs	longest-run	rank	Fft	nonperiodic-templates	overlapping-templates	Universal	Apen	Serial	lempel-ziv	linear-complexity
1	7BC5FC6DF981BDC1E687B98791DE84D9	0.1500	1.0000	0.4500	0.2500	0.3500	1. 0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.7300	1.0000	1.0000
2	481CE5A868F5CB5ED9F87717C7A6C5E0	1.0000	1. 0000	0.7990	08990	0.7990	1.0000	0.0000	1.0000	1.0000	1.0000	1. 0000	1.0000	0.6500	1.0000	1.0000
3	8030D2C95DA1430D66F1385557C2E2E3F02E29F7000AB2FB75D0A7BEE8BE340D	0.9300	0.8800	0.6900	0.7900	0.9810	1. 0000	0.0000	1.0000	1.0000	1.0000	1. 0000	1.0000	0.7800	1.0000	1.0000
4	8076498979C11B952B839A5DEA0D9461917 3B9401AED39295CBF95572814BA87	0.7700	1. 0000	0.9600	0.9770	0.9980	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9800	1.0000	1.0000
5	EED071F281E768317BD54481D10369D9 DE3868457A88825422C0E3044985830C	0.8600	1.0000	0.7800	0.9860	0.7600	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.8400	1.0000	1.0000
6	D30281A802181D32B92B861E78C8E07C7 544E7EF03A6E347CA45EB39CD6E4B9425D 3DCEE784DF67BDEA4E171A871FE3F	0.6200	1.0000	0.9430	0.8300	0.8300	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9800	1.0000	1.0000
7	9E0F3765EB13C54DBC8C5FA2FD85D0AD71BF 9799BD905AA27AE7B12070442A836E8F9548 FC2BA2A92093D6C30B7382CB	0.9500	1.0000	0.9250	0.9250	0.8990	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.8990	1.0000	1. 0000
8	B28CC01C55D49FBDDE13FFFF234AC59DB2B7 A3B7656182B6CCB57BACB6F6FA7AF2EBFA 3401D8CF9E8F824E905D395BF	0.8410	1.0000	0.9200	0.8200	0.9430	1.0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9870	1.0000	1.0000
9	90A38700717B859CFD01E929CE08D04B45 BDBDCDDDCECF93CBA2D8CEB5E1F4FC88 2D4C132E0D65B52E9BD9084D039AA80819 E07D285241915A9BEDA11F925859	1.0000	0.8330	0.8220	0.8220	0.9220	1. 0000	0.0000	1.0000	1.0000	1.0000	1.0000	1.0000	0.9110	1.0000	1.0000

10	7BA3A6573629A46FBDF58EA1238292228EF6E9AD3CCC1622E641970214EF4557DADAD8ABFE3DFF914806CB8D4C0326ABDDA3AA636E8A49F76DBDB24C8B530F1EF5E257F9EC7E07A14381289CF8E0E10DA3BAC4B019F5E1F013DA331277DD27B42B58FF6F	0.9865	1.0000	0.6520	0.7830	0.7880	1.0000	0.0000	1.0000	1. 0000	1.0000	1.0000	1.0000	0.8520	1.0000	1.0000

4.2 The Steganography part

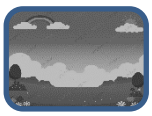
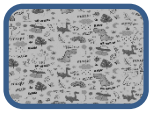
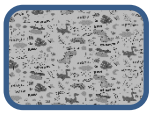
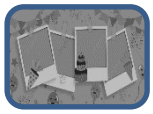
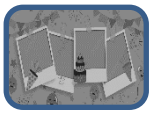
This is the second part of the proposed system, apply Hiding process in the LSB but with random positions Of bits (based proposed map explain in table 1) in each byte of the gray image. Table 5 on the illustrated the gray image properties that used for hiding process.

From the result in table 5, the gray images have a different size and different image resolution. The proposed work checks the image size with the ciphertext length for making decisions that image has enough capacity for hiding

Table 5. Gray images properties

Original Image Properties				
.No	Image Name	Size Image	Image Resolution	Image Format
1	Image 1	KB 114.2	781 * 573	(Jpg.)
2	Image 2	Kb 16.4	241 * 318	(Jpg.)
3	Image 3	Mb 3.1	1024 *1280	(Jpg.)
4	Image 4	Mb 1.7	1600 * 900	(Jpg.)
5	Image 5	Kb 315.8	225 * 225	(Jpg.)
6	Image 6	Kb 607.5	1208 *1200	(Jpg.)
7	Image 7	Mb 1.1	1201 *1200	(Jpg.)
8	Image 8	Kb 391.9	567 *1200	(Jpg.)
9	Image 9	Kb 349.3	483 *487	(Jpg.)
10	Image 10	Kb 708.1	1208 *1200	(Jpg.)

Table 6. the hiding time for different lengths of ciphertext

No	CipherText	Original image	Sego-Image	Time Hide Cipher Text of Pico-second
1	*7BC5FC6DF981BDC1E687B98791DE84D9*			00:00:00.0006772
2	481CE5A868F5CB5ED9F87717C7A6C5E0			00:00:00.0006922
3	8030D2C95DA1430D66F1385557C2E2E3F0 2E29F7000AB2FB75D0A7BEE8BE340D			00:00:00.0011228
4	8076498979C11B952B839A5DEA0D9461917 3B9401AED39295CBF95572814BA87			00:00:00.0012078
5	EED071F281E768317BD54481D10369D9 I. DE3868457A88825422C0E3044985830C			00:00:00.0012495
6	D30281A802181D32B92B861E78C8E07C7 544E7EF03A6E347CA45EB39CD6E4B9425D 3DCEE784DF67BDEA4E171A871FE3F			00:00:00.0017155
7	*A.* 9E0F3765EB13C54DBC8C5FA2FD85D0AD71BF *B.* 9799BD905AA27AE7B12070442A836E8F9548 FC2BA2A92093D6C30B7382CB			00:00:00.0017796
8	B28CC01C55D49FBDDE13FFFF234AC59DB2B7 A3B7656182B6CCB57BACB6F6FA7AF2EBFA 3401D8CF9E8F824E905D395BF			00:00:00.0018156
9	90A38700717B859CFD01E929CE08D04B45 BDBDCDDDCECF93CBA2D8CEB5E1F4FC88 2D4C132E0D65B52E9BD9084D039AA80819 E07D285241915A9BEDA11F925859			00:00:00.0020989

10	7BA3A6573629A46FBDF58EA1238292228E F6E9AD3CCC1622E641970214EF4557DADA D8ABFE3DFF914806CB8D4C0326ABDDA3A A636E8A49F76DBDB24C8B530F1EF5E257F9 EC7E07A14381289CF8E0E10DA3BAC4B019F 5E1F013DA331277DD27B42B58FF6F			00:00:00.0046315

From the above result, the original images similar to the stego-images that any person could not show the effectiveness of the hiding process of your eye. When increases the cipher text length due to increase the hiding time. The Positive Relationship between hiding time and cipher text lengths, as shown in figure 4

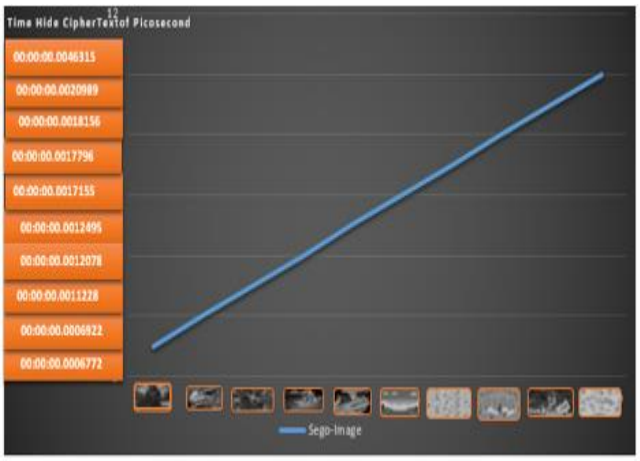


Fig. 4. The positive relationship between hiding time and cipher text lengths.

Tested 10 gray images with different properties for hiding ciphertext with different lengths. The measurements that used in this research, mean square error (MSE), Signal-To-Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Embedded Capacity measured (EC), Entropy, and Histogram. Table 7 illustrated the result of the previous metrics.

In the a blew table 7, the MSE that all values ranged between the highest value of 0.195816697 for gray image that has resolution (318X241)and the lowest value being very close to Zero 0.000977083 for gray image that has

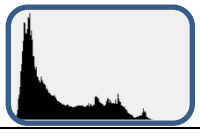
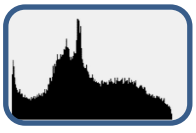
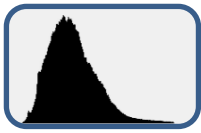
resolution (900 X 1600). Also, the gray image that has the lowest value of MSE that has the highest value of PSNR 75.72135129 and the highest value of the SNR 68.61384535 And the gray image that has the highest value of MSE that has the lowest value of PNSR 52.70217015 and the lowest value of SNR 47.15894861 These results

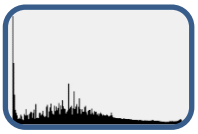
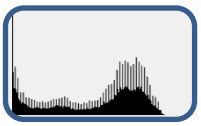
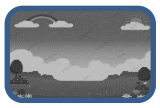
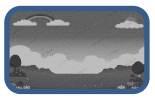
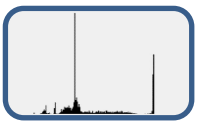
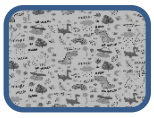
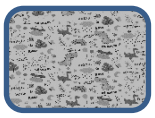
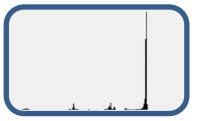
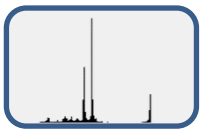
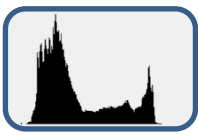
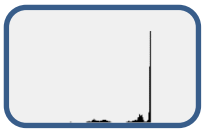
indicate that the proposed method is a good quality and high secret according to the specific values of MSE, PSNR, and SNR [23].

Also, EC measured is to embed and calculate the highest number of safe bits that can be hidden in the image that it is measured in units bits per pixel (bpp) [21,24]. The largest value of EC in table 6 is (0.006680759) and smallest value of EC is (0.00015009). This result gives a good trace achieved through the proposed method, (EC) depends on the properties of the image as well as the length of the ciphertetxt.

Entropy is a measure of the degree of randomness between the original image and the stego image [25-29], the entropy values ranged between (2.820111545) and (5.160472612). From entropy values notice that the entropy ratio is an acceptable and a good ratio compared to other steganography methods, where the lower the value is more optimize. The histogram shape was drawn to the stego image that hidden a ciphertext of different lengths, in table 7, the histogram shape has a good result that depends on the properties of the image and the length of the ciphertext. In additional, the investigation Variance and correlation that calculated between original image and Steganography image, as shown in figure 5.

Table 7. The result of the MSE, SNR, PSNR, EC, Entropy, and Histogram

No	Original Image	*a)* *Stego-image*	MSE	SNR	PSNR	EC	Entropy	Histogram
1			0.016719067	56.27142619	63.38854686	0.000286025	4.756356902	
2			0.195816697	47.15894861	52.70217015	0.006680759	5.160472612	
3			0.008908081	58.09952948	66.07723042	0.000195313	4.706273263	

4			0.000977083	75.72135129	68.61384535	0.000177778	4.982106828	
5			0.26224197531	46.05826704	51.34221401	0.00505679	4.857598492	
6			0.006272765	64.09699232	67.64607724	0.000264901	3.865668401	
7			0.033364557	59.49768484	60.38781368	0.000266445	2.820111545	
8			0.031293357	57.75807129	60.66614582	0.000564374	3.282382696	
9			0.230595908	45.88919929	51.90072013	0.002176676	4.80577407	
10			0.040427704	58.77464446	59.55387655	0.000618102	3.093078133	

Entropy is a measure of the degree of randomness between the original image and the stego image [25,26], the entropy values ranged between (2.820111545) and (5.160472612). From entropy values notice that the entropy ratio is an acceptable and a good ratio compared to other steganography methods, where the lower the value is more optimize. The histogram shape was drawn to the stego image that hidden a ciphertext of different lengths, in table 7, the histogram shape has a good result that depends on the properties of the image and the length of the ciphertext. In additional, the investigation Variance and correlation that calculated between original image and Steganography image, as shown in figure 5.

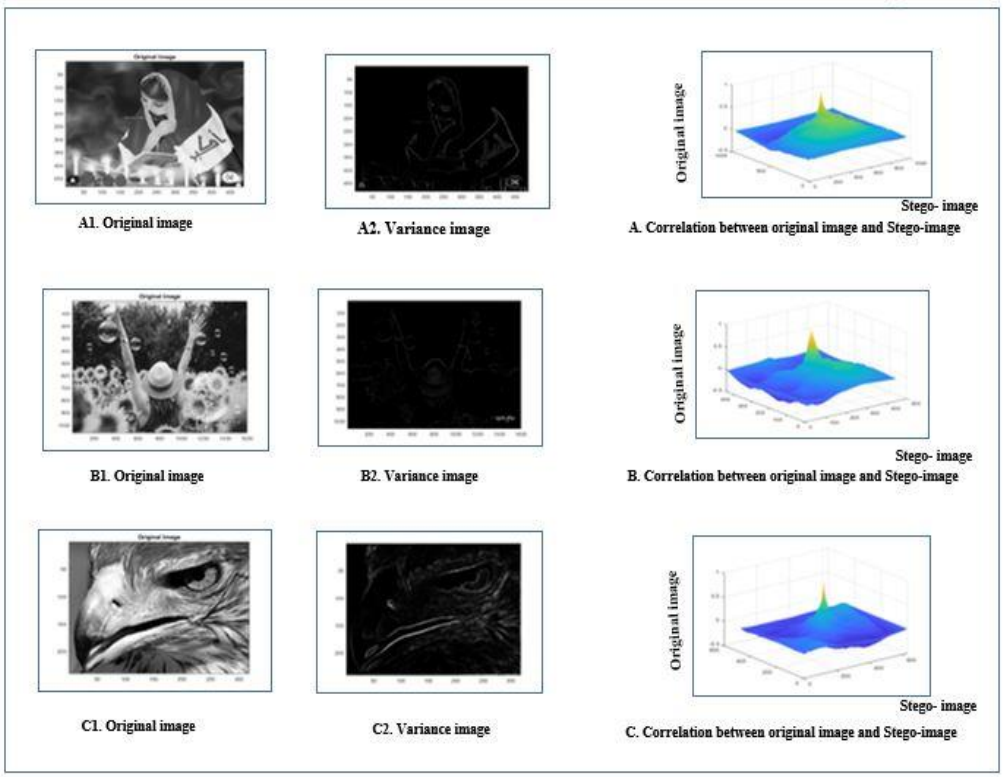


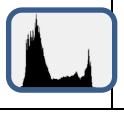
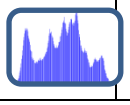
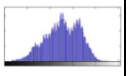
Fig. 5. The investigation Variance and The Correlation.

From the above result in figure 5, it shows the variance of the images. The variance refers to how the pixel values are spread in the images, where the variance calculated for the original image and the stego-image was the result of the image (A) = 1.4981 and (B) =5.1627 and (C) = 5.9343. Figure 5 illustrated the last measurement that is the Correlation between original image and Steganography image. It shows the Correlation between the original image and the steganography image according to the graph shown the Correlation of A = (0.982) and B= (0.999) and = (0.951). The results show that the relationship between the original image and the image is very close to 1 meaning that it is difficult to distinguish between the two images and this is evidence it is difficult for attackers to distinguish and the proposed method has proven to be a successful method.

Compare the results obtained through our proposed work to hide the ciphertext in a gray-level image based on the proposed map. It is worth mentioning that each of the methods in the comparison table 8 has used different properties of the images, as well as texts of different lengths. Then Compare the results for the best value in each method.

In the blew table (8), the evaluation results between the different remaining steganography methods and the proposed method showed.According to the results, the results of the proposed method are very good results compared to the rest methods.

Table 8. The comparison Evaluation Criteria between proposed method and other methods

Evaluation Criteria	proposed method	eLSBRAISDSCSO	SISTMS	CFSLSB	AOSHCAIUGA
MSE	0.0009	0.00122		0.0147	-------
PSNR	75.7213	74.2795	72.82	66.4486	66.46
SNR	68.613	-------	-------	-------	-------
Entropy	2.8201	-------		-------	-------
EC	0.00015 bit	-------	131,02Byte 6	3276 Byte 8	8,192 byte
Variance	5.1627	-------	-------	-------	-------
Correlation	0.999	-------	-------	-------	-------
Histogram			-------	-------	

4.3 Algorithm of the proposed Method

```
Algorithm name: Steganography Based on Chaotic
 System for Random LSB Positions
Input: Plaintext, Initial value, Image as Img
Output: Stego-Image
Processes:
   Begin
Step 1: Initial_key=chaotic System (initial_value)
              // Generate Initial Key by using cha-
otic system
Step 2: Key_rounds=Expansion key(Initial_key)
             // Generate key rounds by using expan-
sion key of the AES algorithm
Step 3: ciphertext=Encryption process (plaintext,
key_rounds)
Step 4:Img_binary=convert_array_of_binary(Img)
```

```
Step 5:CT=Convert_CipherText_to_Binary(ciphertext)
Step 6: set hidden_map=first_round (key_rounds)
```

```
Step 7:    Hidden_R=Reminder (hidden_map,3)
Step 8:   Set i , j
Step 9: Set L=Length (Ciphertext)
Step 10: While i<L
Step 11:    If (Hidden_R==1)
           Hide One bit of CT (i) Into Img(X, Y).R
Step 12:      Else if (Hidden_R==2)
Hide Tow bits of CT (i) Into Img(X, Y).G
 Step 13:    Else if ( Hidden_R==3)
Hide Three bits of CT (i) Into Img(X, Y).B
Step 14:    InCrement  X
Step 15:   if   X =  Img .Width  &   i  <=  L    Then
Step 16:     ReSet    X
Step 17:     InCrement   Y
                  End if
Step 18:   i = i + 6
               Wend   //end While
End
```

5 conclusion

Because increase the attackers and intruders that theft the information, the text steganography need for achieving the confidentiality. In this paper, suggested a new method for hiding a text in an image. Firstly, encrypting the text by the AES-192 bit algorithm for obtaining a secret message. When the initial key of the AES-192 (bit) algorithm is generated by chaotic system for randomness purpose, secondly, hiding the secret message into a gray image for obtaining a stego-image. The hiding step based on a proposed map that choice from last round of key expansion in AES-192 algorithm. This map represented a random positions of LSB in each byte of gray image. This map cannot guested testing of the proposed method obtained a faster method for hiding ciphertext in the gray image as well as extracting ciphertext from gray image. Also, it is difficult to distinguish between the original image and stego-image because the correlation between the original image and the image is very close to 1 meaning that it is difficult for attackers to distinguish among two images and the proposed method has proven to be a successful method based on Mean Square Error (MSE), Signal to Noise Rate (SNR), Peak Signal Noise Rate (PSNR), Embedding Capacity (EC), Entropy, and Histogram.

6 ACKNOWLEDGEMENTS

The authors would like to thank Al-Nahrain University, University of Technology and Iraqi Ministry of Education for their support to conduct the work published in this paper.

7 REFERENCES

[1] Amrita Bhatnagar, Shweta Chaku and Monica Sainger, “Hiding Compressed and Encrypted Data byusing a Technique of Steganography,” International Journal of Engineering Research & Technology (IJERT). Volume 09, Issue 04 (April 2020) , DOI: 10.17577/IJERTV9IS040320.

[2] Jammi Ashok, Y.Raju, S.Munishankaraiah and K.Srinivas, “Steganography: An Overview,”International Journal of Engineering Science and Technology. Vol. 2(10), 2010, 5985-5992.

[3] Milad Taleby Ahvanooey, Qianmu Li, Jun Hou, Ahmed Raza Rajput and Chen Yini, “Modern Text Hiding, Text Steganalysis, and Applications: A Comparative Analysis,” Entropy 2019, 21(4), 355;doi.org/10.3390/e21040355.

[4] Dalal N. Hmood, Khamael A. Khudhia , Mohammed S. Altaei, “A New Steganographic Method for Embedded Image In Audio File,” International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (2) : 2012 .

[5] K. Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim,Hassanain Mahdi Alzuabidi , “Combination of Steganography and Cryptography: A short Survey,” 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019), IOP Conf. Series: Materials Science and Engineering 518 (2019) 052003 IOP Publishing ,doi:10.1088/1757-899X/518/5/052003.

[6] Rawaa Hamza Ali, Jamal Mohamed Kadhim,” Text-based Steganography using Huffman Compression and AES Encryption Algorithm,” Iraqi Journal of Science, 2021, Vol. 62, No. 11, pp: 4110-4120, DOI:10.24996/ijs.2021.62.11.31.

[7] Zainab N. Sultani and Ban N. Dhannoon, “Image and audio steganography based on indirect LSB,” Kuwait J.Sci., Vol.48, No. (4), October.2021, pp (1-12).

[8] Abhinav Gupta, Divya Tiwari, Vineet Kumar, K. P. S. Rana and Seyedali Mirjalili ,"A Chaos–Infused Moth–Flame Optimizer,"Arabian Journal for Science and Engineering, 23 April 2022.

[9] Ricard V. Soléa and JordiBascompteb, “Measuring chaos from spatial information,” Journal of Theoretical Biology Volume 175, Issue 2, 21 July 1995, Pages 139-147.

[10] Ziaur Rahman, Xun Yi, Ibrahim Khalil, and Mousumi Sumi, “Chaos and Logistic Map based Key Generation Technique for AES-driven IoT Security”. Electronics 2022, 1, 0.doi.org/10.3390/electronics1010000

[11] Ray Huffaker, Marco Bittelli, and Rodolfo Rosa, “Nonlinear Time Series Analysis with R, ” Oxford Scholarship Online: February 2018, DOI:10.1093/oso/9780198782933.001.0001.

[12] Lawande Q.V., Ivan B.R and Phodapkar S.D, “Chaos Based Cryptography, ” A new approach To Secure Communication, No. 258 , July 2005 .

[13] Hussein L. Hussein, Ahmed A. Abbass, Sinan A. Naji, and Salam Al-augby a, Jasim H. Lafa “Hiding text in gray image using mapping technique, “Article in Journal of Physics Conference Series • May 2018, DOI: 10.1088/1742-6596/1003/1/012032.

[14] Alaa Kadhim F And Rasha Subhi Ali"Hidden Encrypted Text Based On Secrete Map Equation And Bioinformatics Techniques," Journal of Theoretical and Applied Information Technology, 15th January 2019. Vol.96. No 1.

[15] Alaa Kadhim Farhan, Nadia M.G. Al-Saidi, Abeer Tariq Maolood, Fahimeh Nazarimehr and Iqtadar Hussain "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," Entropy 2019, 21(10), 958,doi.org/10.3390/e21100958.

[16] Jagan Raj Jayapandiyan, C. Kavitha and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in spatial domain of Steganography using character sequence optimization," IEEE Access, August 5, 2020, doi: 10.1109/ACCESS.2020.3009234.

[17] Ranyiah Wazirali, Waleed Alasmary, Mohamed Mahmoud And Ahmad, Alhindi, "An Optimized Steganography Hiding Capacity And Imperceptibly Using Genetic Algorithms," IEEE Access, 2019, DOI 10.1109/ACCESS.2019.2941440.

[18] Ali Salem Ali, Mohammed Sabbih Hamoud Al-Tamimi and Alaa Ahmed Abbood, "Secure Image Steganography through Multilevel Security,"International Journal of Innovation, Creativity and Change. Volume 11, Issue 1, 2020.

[19] Mansoor Fateh, Mohsen Rezvani, and Yasser Iran,"A New Method of Coding for Steganography Based on LSB Matching Revisited,"Hindawi Security and Communication Networks, 08 Feb 2021, Volume 2021, Article ID 6610678, doi.org/10.1155/2021/6610678.

[20] Sachin Dhawan and Rashmi Gupta," Analysis of various data security techniques of steganography: A survey," Information Security Journal: A Global Perspective, 12 Aug 2020, Volume 30, 2021 - Issue 2, doi.org/10.1080/19393555.2020.1801911.

[21] Mohammed Mahdi Hashim and Mohd Shafry Mohd Rahim,"Image Steganography Based On Odd/Even Pixels Distribution Scheme and Two Parameters Random Function". Journal of Theoretical and Applied Information Technology, 30th November 2017. Vol.95. No 22.

[22] Azhaar Akram Abdallah and Alaa Kadhim Farhan, "A New Image Encryption Algorithm Based on Multi ChaoticSystem , " Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337DOI: 10.24996/ijs.2022.63.1.31

[23] Manohar N and Peetla Vijay Kumar ,"Data Encryption & Decryption Using Steganography , " Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2020) ,IEEE Xplore , Part Number:CFP20K74-ART; ISBN: 978-1-7281-4876-2

[24] Ammar Mohammed Ali And Alaa Kadhim Farhan "Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document, " in IEEE Access, vol. 8, pp. 27448-27458, 2020, doi: 10.1109/ACCESS.2020.2971779.

[25] Nuha A. S. Alwan and Zahir M. Hussain," Compressive Sensing with Chaotic Sequences: An Application to Localization in Wireless Sensor Networks," Wireless Personal Communications, IEEEAccess, 06 February 2019, doi:10.1109/ACCESS.2019.2941440.

[26] R. Asgarnezhad, S. S. A. Majeed, Z. A. Abbas, and S. S. Salman, "An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 1, pp. 27-35, 2022.

[27] R. I. Farhan, A. T. Maolood, and N. Hassan, "Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS," *Wasit Journal of Computer and Mathematics Science*, pp. 66-83, 2021.

[28] M. M. T. Al Mossawy and L. E. George, "A digital signature system based on hand geometry-Survey: Basic Components of Hand-based Biometric System," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 1, pp. 1-14, 2022.

[29] Kaiser A. Reshak, Ban N. Dhannoon and Zainab N. Sultani,"Explicit feedback based movie recommendation system: A survey ," AIP Conference Proceedings 2290, 040009 (2020) , doi.org/10.1063/5.0027433.

Article submitted 16 December 2022. Published as resubmitted by the authors 28 December 2022.

Artificial Intelligence and Its Role in The Development of Personalized Medicine and Drug Control

https://doi.org/10.31185/wjcm.85

Prof.Dr. Johan Waden(✉)
Department of Computer science, University of Helsinki ,Norway.
jwaden_cs@hel.edu.nor

Abstract— DNA sequencing, imaging procedures, and wireless healthcare monitoring devices are all examples of high-throughput, data-intensive precision medicine assays and technologies that have necessitated new methods for analysing, integrating, and interpreting the enormous volumes of data they produce. While several statistical approaches have been developed to deal with the "big data" generated by such tests, previous experience with artificial intelligence (AI) techniques suggests that they may be especially well-suited. Furthermore, data-intensive biomedical technologies applied to study have shown that people differ greatly at the genetic, biochemical, physiological, exposure, and behavioural levels, particularly with regards to disease processes and treatment receptivity. This indicates the need to 'personalise' medications so that they better suit the complex and often individual needs of each patient. AI can play a significant role in the clinical research and development of new personalised health products, from selecting relevant contribute to sustainable to testing their utility, because of the importance of data-intensive assays in revealing appropriate intervention objectives and approaches for personalising medicines. The work here presents a variety of ways in which AI can contribute to the progress of personalised medicine, and we argue that the success of this endeavour is critically dependent on the improvement of appropriate assays and methods for storing, aggregating, accessing, and ultimately combining the data they generate. In addition, the manuscript also discusses the potential future research directions and highlights the shortcomings of various AI methods.

Keywords— Artificial Intelligence, AI in Personalized Medicine, Drug Control, Drug Discovery using AI.

1 Introduction

There are a number of underlying concepts that govern or perhaps dominate today's biomedical research. Many of the issues plaguing precision medicine today may be resolved if AI approaches were trained and validated using huge data sets before being applied to personal data [1]. The given instances emphasise yet another possible use of augmented intelligence: the role of electronics in the hands of individuals to aid in "just in time" risk communication or as an agent of behaviour modification. Despite the fact that most studies to yet have been small and the data restricted, the capacity to identify

at-risk individuals will translate into individualised treatment when identification is paired with ways to alert and intervene. Mobile applications, wearables, virtual assistants, and other technologies are all being explored by researchers as potential means of providing individuals with tailored experiences while interacting with autonomous machines [2].

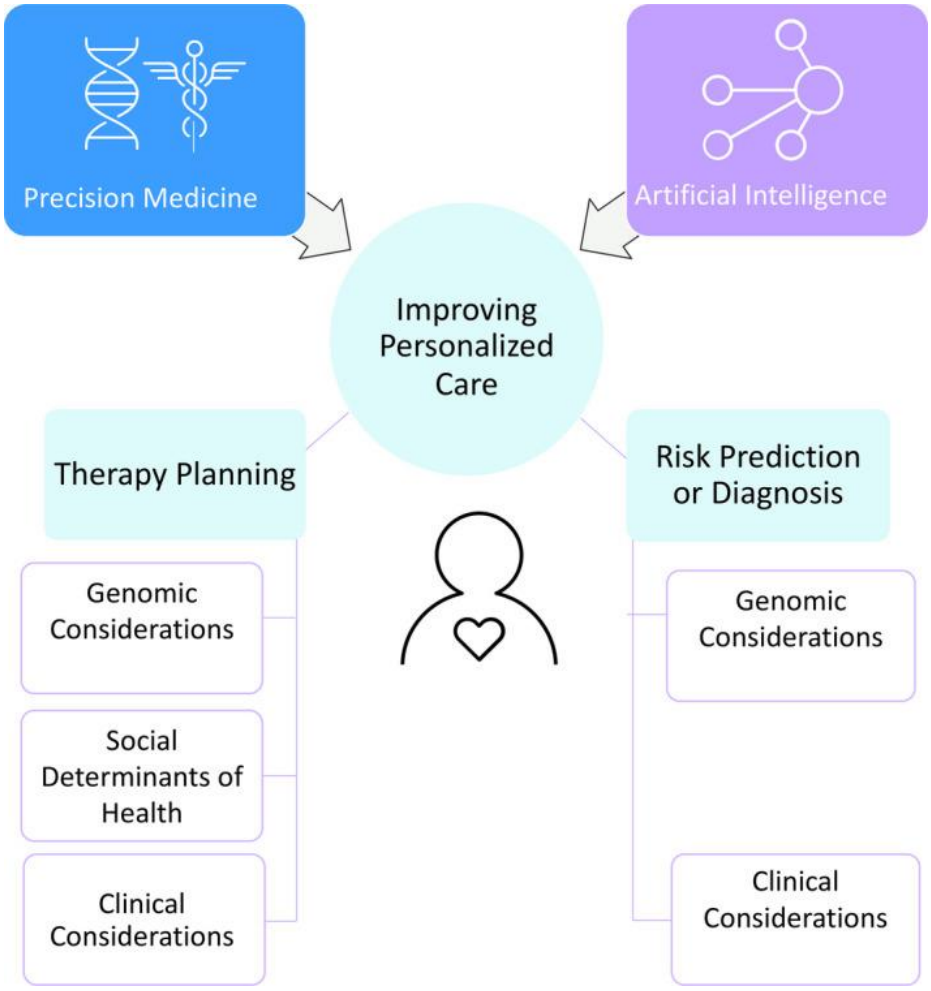


Fig. 1. Personalized Medicine and Heath Care

The intersection of AI and precision medicine is illuminating a future in which people's and doctors' access to highly individualised medical diagnostic and treatment information will enhance their ability to provide better care to their patients. The

combined effect of these two trends on healthcare is congruent with the long-term objective of reducing the overall illness burden and the expense of treating avoidable conditions [3].

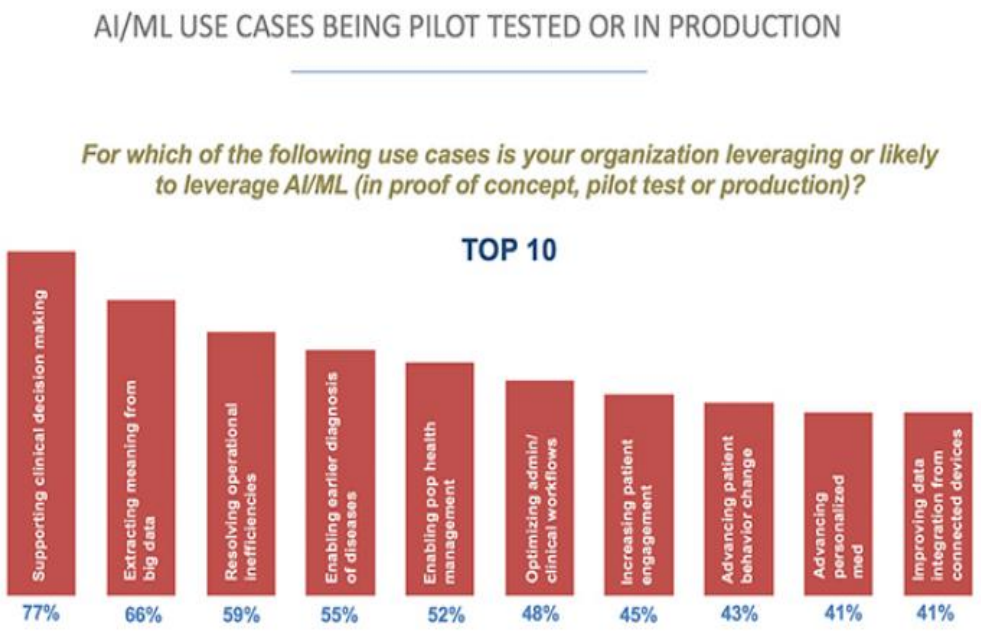


Fig. 2. Key Use Cases of Artificial Intelligence in Heath Care

The concept of "personalised medicine," which holds that each person's health care needs must be addressed in light of their own genetic, biochemical, physiological, exposure, and behavioural characteristics [4], Making use of new data-heavy assays like DNA sequencing, proteomics, radiology procedures, and wireless health monitors;. 'Big data' research paradigms, in which large amounts of data, such as those generated from arising data-intensive biological and medical assays, are compiled from alternative viewpoints, harmonised, and available for analysis, allowing for the identification of patterns that would otherwise go unnoticed if the data points were analysed separately; and 4. Artificial intelligence (AI; which we define here to encompass algorithms-based machine learning, learning techniques, neural network constructions, and a broad variety of related techniques) to discover meaningful patterns in large data sets [5].

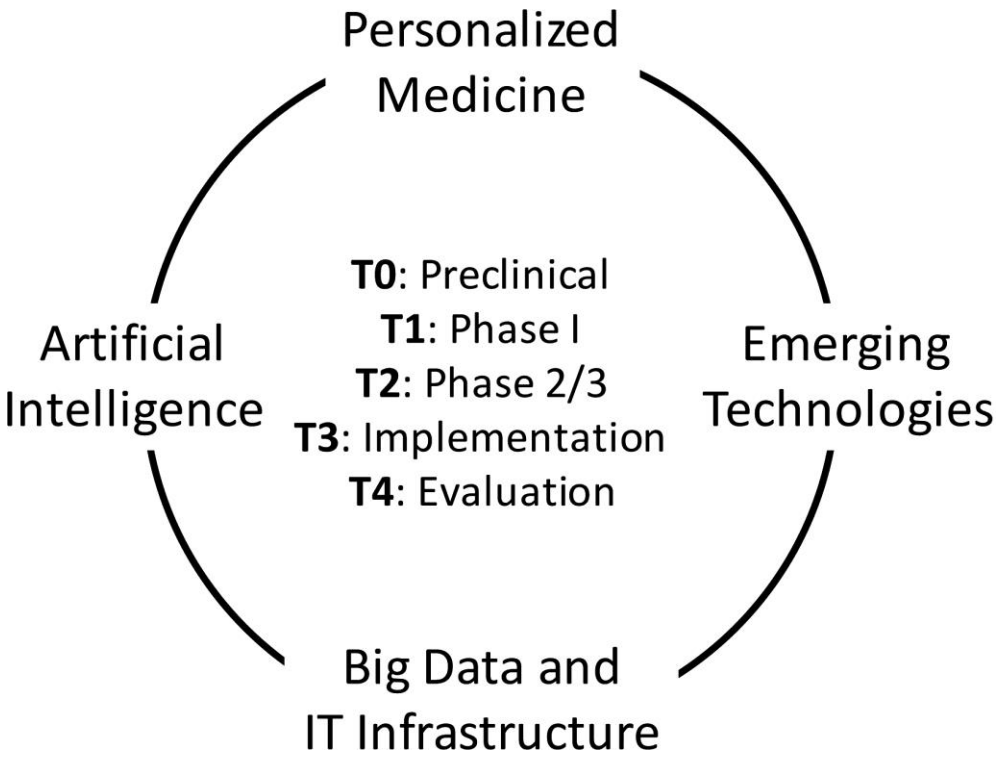


Fig. 3. Assorted Phases in Personalized Medicines

As these four developing topics span disciplines as diverse as cell biology, genetics, pathology, computers, computer science, statistic, clinical science, and medicine, it is not a simple task to bring together the research efforts related with them. Since it is uncertain how relevant clinical and pathological insights may be obtained from big data-generating devices which might complement or build upon the insights from expert in diverse fields [6], AI will play a unique role in this accession process if the objective is to develop personalised medicine. Because of this, AI has the potential to greatly improve many aspects of the research and development process for new drugs, general therapies, and other goods, including diagnostics, prognostics, decision assistance systems, etc. In this segment, we detail and comment on current research that make use of AI at each of these stages [7].

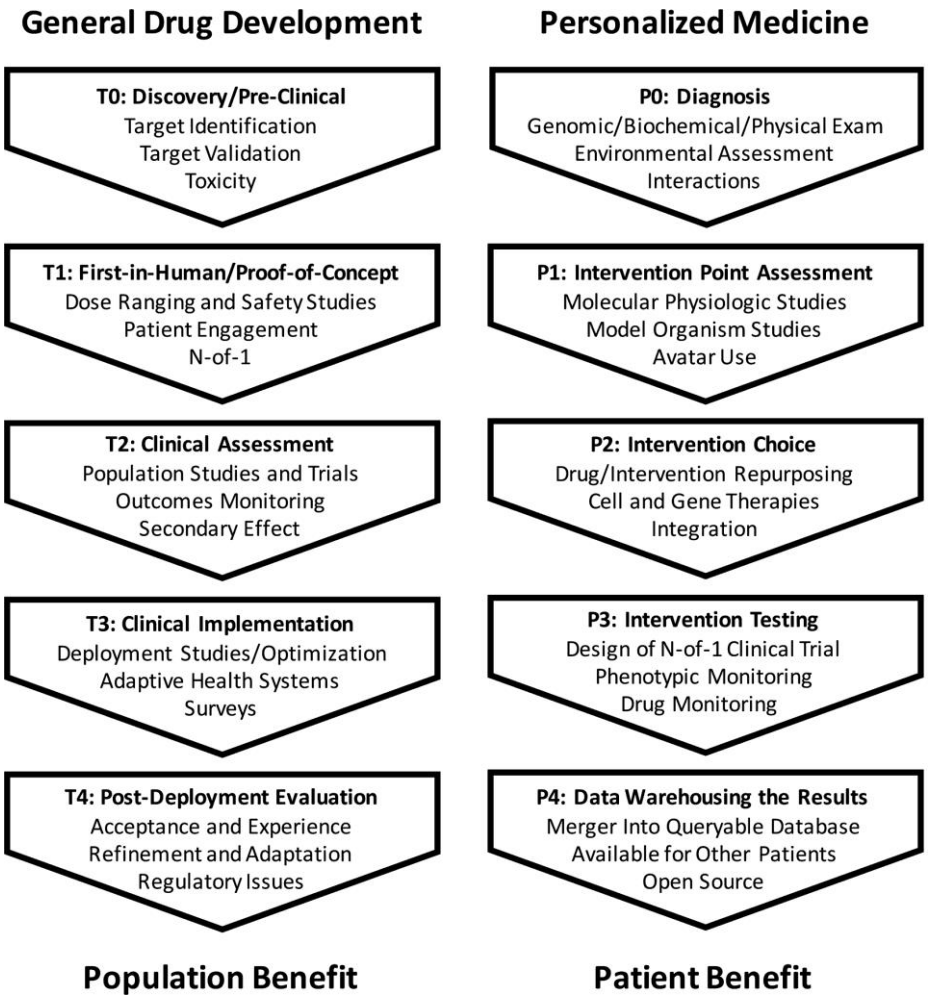


Fig. 4. Benefits and Key Advantages towards Implementation Patterns

A mechanism similar to that used in medication and device discovery underlies the actual delivery of customised medicine. Thus, P0 activity entails making a diagnosis or estimating an individual's risk of disease; P1 activity entails identifying the primary pathophysiologic processes, if not recognised, that are affecting (or likely to cause) the a disease that might be susceptible to modulation by an effective interventions; P2 activity considers the identification of a specific interventions given what was identified in P0 and P1; and P3 activity entails testing the action on the relevant individual [8].

There are a few important details to remember while working with such procedures. First, it has been noted that the communication of data from one component to another, or the transitions between components, is of crucial importance, even though the science attributed with each constituent involves unique knowledge and expertise and

provide a breeding soil for partnering with AI tools and scientists individually of the other components

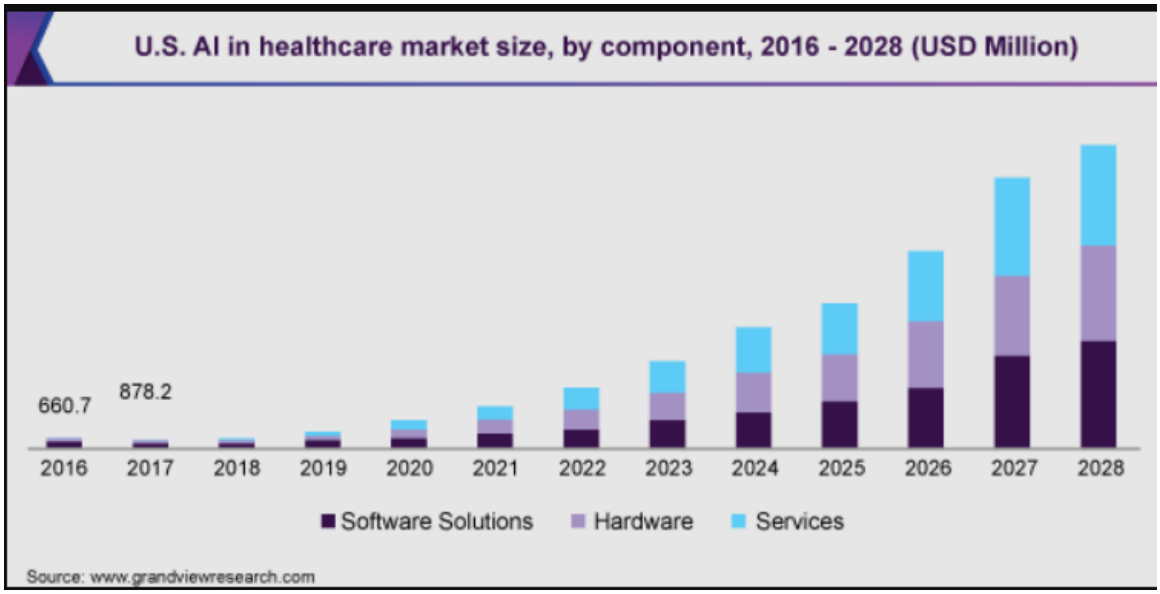


Fig. 5. Predictive Data Analytics

2 Aspects towards Limitations

While AI has great potential, there are several obstacles that prevent it from being used to create truly individualised pharmaceuticals. Just a few of the most important ones are touched on quickly here. The first criticism levelled by big data analysis is that they often fail to reveal crucial individual-level linkages despite the fact that they pool data from several people in order to spot patterns that represent relationships between points at the population level. In the absence of 'ergodicity,' models may be useless in selecting appropriate therapies for specific patients. For instance, as more economic indicators are accumulated on each individual, any projections of the target individual's heath trajectory might also rely more on the legacy datasets on that entity and less on the population level data in order to accurately predict the target individual's health trajectory. Training AI systems to recognise this is a vital step toward improving individualised healthcare [9].

Second, there's a pressing need to evaluate the efficacy of AI-driven medical technologies. The motivation for this comes from the fact that various AI and big relevant data health care systems, like IBM's Watson therapy decision support system, have shown uneven outcomes. Traditional randomised clinical studies for evaluating the efficacy of such systems have been explored in the literature, and several AI-based decision analysis tools have been demonstrated to be effective in such trials. Vetting AI-based decision support systems like IBM's Watson may be necessary because of the

possibility for incorrect suggestions or forecasts if the underlying system's decision making capabilities was trained on an incomplete or biassed data set. Case in point: Google's flu prediction engine, which has a fairly poor reputation. If the system for matching pharmaceuticals to patient profiles is demonstrated not to operate better than standard of care or an alternate technique of matching drugs to patient features, then a few further issues may be raised in the context of the trials, in which the underlying scheme is being evaluated. It's possible that the medications, or a significant proportion of them, are useless, which would have a negative influence on how well the matching method works as a whole. Also, it's possible that the medications themselves are effective, but that the inappropriate matcher or scheme is preventing them from being administered to the right patients. These concerns arose in light of the study, a so-called "bucket trail" that showed the medication matching strategy to be no more effective than conventional methods of treating patients [8, 9].

Third, it's possible that learning systems, where the recommendation rules or algorithms are continually updated, are a better means to evaluate at least decision support tools than randomised clinical trials [10].

Unfortunately, this might take a long time to grow into a machine with accurate and reliable decision making, and it would also require a lack of objectivity in the initial data sets used to seeding the learning system in order to assure generalizable findings [10]. Finally, deep learning and tensorflow algorithms are used in many AI-based decision assistance products.

Using a sufficiently large training set, these algorithms may make very accurate predictions; nevertheless, the relationships between the data used to train the algorithm and the predictions it generates are not always clear. Because of this 'Black Box' issue, many AI-based systems may not be trusted to provide accurate predictions in situations when human lives are at risk. Furthermore, not all AI methods are built to establish causal links between inputs and outcomes, but rather to make just associative or predictive claims. However, recognising causal linkages is vital if the objective is to, for example, find a pharmacological target that, when adjusted, leads to a desired result.

3 Research Perspectives in Assorted Dimensions of Precision Medicine

The convergence of AI with precision medicine has the potential to completely alter the healthcare system. Methods used in precision medicine are able to classify individuals into phenotypes based on their unusual reactions to therapy or specific medical requirements. By using complex computing and inference to uncover insights, AI makes it possible for the system to understand and learn, and it augments the intellect of clinicians to make better decisions. The most pressing problems in precision medicine may be overcome through translational studies of this intersection of fields; in particular, the integration of non-genomic and cytogenetic determinants with patient symptoms, health characteristics, and lifestyle data should improve the accuracy of diagnosis and prognosis.

A recent report by the National Academy of Medicine discussed the present and future of AI in healthcare, highlighting "unprecedented opportunities" to supplement the care of specialists and the aid that AI can provide in combating the realities of being human (such as fatigue and inattention) and the hazard of machine error. The research emphasises the need of exercising caution while using these technologies despite the many potential benefits they provide. Transformation and advancement in the development and implementation of AI in healthcare are fuelled by the digitalization of healthrelated data and the fast use of technology. There may be obstacles to the application of AI in healthcare, such as multimodal data integration, security, distributed learning (which requires fundamental advancements in fields like privacy, large-scale machine learning, and decentralized optimization), prediction accuracy, and bias.

A lot has changed in the last decade in terms of AI's development and acceptability across many industries, but the healthcare sector is one that has experienced significant growth and acceptance. Artificial intelligence (AI) opens up several prospects for developing innovative goods, services, and business strategies. But there are also social and ethical concerns with how AI is used, particularly in regards to privacy, safety, and human rights.

Many different types of artificial intelligence (AI) are employed in the medical field, ranging from entirely virtual (such as deep learning-based health information administration systems and active coaching of clinicians in their treatment choices) to cyber-physical). Many image based detection and diagnosis in healthcare are now able to perform as well as, or even better than, physicians because to the ability of AI technology to spot complicated patterns and hidden structures.

Clinical decision-support systems powered by AI might help doctors make more accurate diagnoses, provide more insight to aid in making tough choices, and streamline the process of extracting and documenting patient information from electronic health records. Natural language processing (NLP), pattern recognition, efficient search, prediction, and bias-free reasoning are all areas of computing that are on the cusp of significant advancement, which will ultimately lead to new capabilities in artificial intelligence (AI) that can solve pressing issues today.

Similarly, research into precision medicine is expanding rapidly. The sequencing of the human genome has sparked a revolution in medical practise known as "precision medicine," which may be best characterised as the establishment of "a New Taxonomy of human illness based on molecular biology." The discipline has progressed to appreciate how a person's health, illness, and treatment choices may be accurately characterised by integrating multi-omic data with medical history, social/behavioral variables, and environmental understanding. This study will utilise the terms "precision medicine" to refer to the aforementioned approach to healthcare and research agenda, and "personalised care" to express how this approach affects each patient uniquely.

As opposed to making medical decisions based on data gleaned from the population as a whole, precision medicine allows doctors to instead take into account each patient's specific background and history. With this tool, doctors can more easily provide individualised treatment for each patient [11]. Discoveries in precision medicine open doors to opportunities that were previously closed.

The early diagnosis of disease and the development of individualised therapies are only two examples of how advances in precision medicine are translating into a better health care system. Multiple data collecting and analytics tools fuel precision medicine's capacity to tailor treatment to each individual. More specifically, the unprecedented possibility to derive novel phenotypes from real-world clinical and biomarker data is made possible by the confluence of high-throughput genotyping with the worldwide deployment of EHRs. When integrated with EHR data, these phenotypes may help show the need of further therapies or refine the identification of disease variations.

Genotype-guided therapy is perhaps the most researched effect of precision medicine on modern healthcare. The right dosage of warfarin has been established with the use of genetic data, which clinicians have utilised as a guideline. Genotype-based pharmacological recommendations were released by the Clinical Pharmacogenetics Application Consortium to assist physicians in making informed decisions about patient care in light of genetic test findings. Patients with breast or lung may benefit from individualised treatment strategies based on tumour genomic analysis, which can provide. When applied to healthcare, precision medicine has the ability to improve diagnostic accuracy, identify at-risk patients before they show symptoms, and provide individualised treatment programmes that are both effective and safe. Examples from Biobanks in various countries, such as the UK Biobank, BioBank Japan, and Australian Genomics Heath Alliance, show the power of shifting attitudes toward precision medicine on a global scale, and this trend is not limited to the United States.

While AI and precision medicine show great potential, additional research, testing, and practise adjustments are needed. Adopting standardised data formats (such as Fast Consolidated Level Resources), getting adequate and high quality labelled data for training algorithms, and resolving regulatory, economic, and sociocultural needs are all obstacles that researchers must overcome [12].

Data collection, storage, normalisation, and tracking are all important uses of AI in healthcare. Google's artificial intelligence (AI) research division has unveiled a new initiative called DeepMind Health, which will be used to sift through mountains of medical information in an effort to improve and speed up healthcare delivery. Moorfields Eye Hospital NHS Foundation Trust began working together on a joint endeavour to enhance eye care in 2016. Moorfields provided DeepMind with a collection of one million randomized eye scans and some anonymous statistics about eye health and illness management to explore how technology may aid to evaluate eye scans.

Oncologists now have access to more therapy choices because to IBM Watson's new oncology initiative. Watson for Oncology's superior capacity to interpret the context and significance of structured and non - structured material in case information and reports that may be pivotal in deciding on a treatment course is a major selling point. Treatment options for a patient are then determined by the program's incorporation of clinical knowledge, variable on the basis, and data.

Medical Sieve is IBM's newest software offering. The project's ultimate goal is to create a sophisticated "cognitive assistant" with extensive clinical knowledge and the ability to think critically and reason analytically. Medical Sieve has the right credentials to help with radiology and cardiology-related clinical decisions. The 'cognitive health assistant' can analyse radiological pictures to more quickly and accurately diagnose

issues. Radiologists may soon just need to review the most complex cases requiring human oversight.

The Dutch firm Zorgprisma Publiek utilises IBM Watson in the cloud to sift through digital hospital and insurance company bills. If a doctor, clinic, or hospital often makes the same errors with a given ailment, they may use this information to do better and save people from being hospitalised unnecessarily [13].

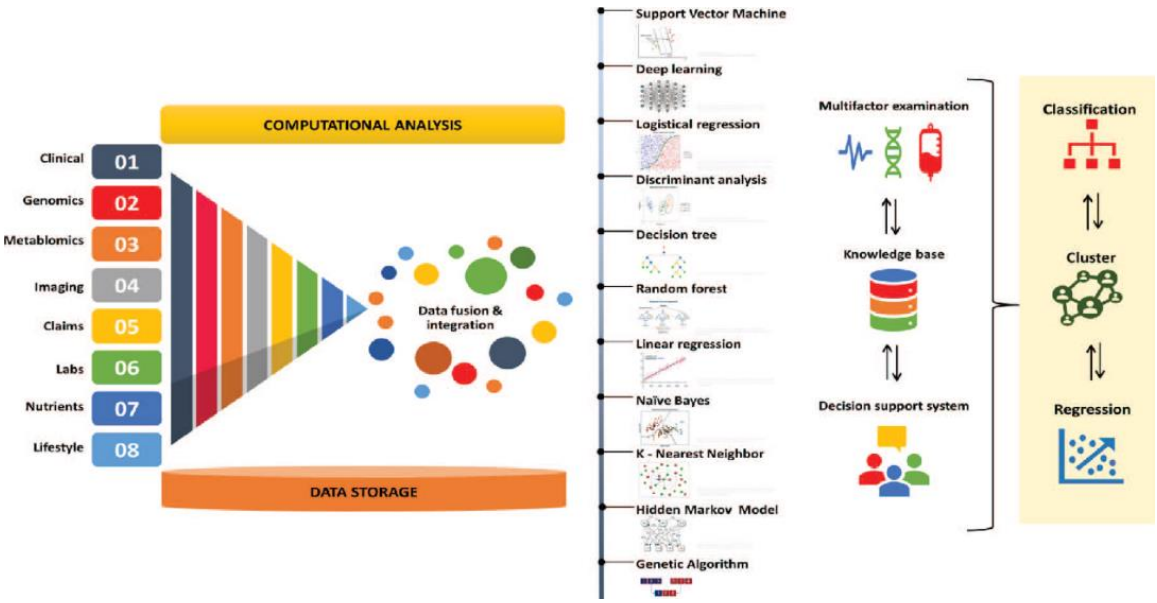


Fig. 6. Artificial Intelligence Based Approach for Predictive Analytics in Personalized Medicine and Drug Discovery

The goal of Deep Genomics is to find mutations and disease links by analysing huge troves of genetic information and medical records. Scientists are developing next-generation computational tools to predict the cellular responses to natural or therapeutic genetic variation.

Clinical studies for new drugs may take years, if not decades, and cost billions of dollars to complete. If this process could be sped up and made more cost-effective, it would have a profound impact on modern health care and the dissemination of medical discoveries. Atomwise employs powerful computers to sift through a library of molecular structures in search of potential treatments. In 2016, Atomwise began an online hunt for potential Ebola treatments already on the market that were already safe to use. The company's AI algorithm was able to anticipate two medications that showed promise in reducing Ebola's infectiousness. This analysis, which would usually take months or even years to conduct, was finished in less than a day [14-27].

While the trends are encouraging, several businesses have yet to provide evidence of the effectiveness of their approach and the toxicity of ANI in studies that have been examined by experts in the field.

4 Conclusion

This manuscript presents how AI has the potential to significantly contribute to the development of customised medicine in the future. AI-based health solutions will not only become more widely used, but they may also take use of new computer technologies like quantum computing to get faster and deal with ever-growing data sets. Larger data sets, which may be used as seeds and key offs for the formulation of more accurate forecasts, are anticipated to result from improved and more advanced monitoring health monitoring equipment. Future AI-based wellness products and applications will likely involve a deeper grasp of biology in addition to leveraging increased speed and computing efficiency. Much work in the fields of artificial intelligence (AI), machine learning (ML), and statistical analysis has centred on discovering such straightforward input/output relationships among data points; doing so under the constraints that are known to govern relevant phenomena presents an exciting new avenue for exploration. In conclusion, much of the application of AI in the development of personalised medicines is geared toward the management of people with outright disease: identifying the neurological dysfunction, determining which therapies might make most sense to just provide given what is recognised about that pathology and the process of action of the meddling, and testing to see if the technique works. As a result, the bulk of AI-based products and technologies used to advance customised medicine centre on the diagnosis, prognosis, and treatment of people. The high expense of present therapies, especially in the case of cancer, makes a pressing need for innovation and efficiencies all the more pressing. However, there has been a lot of progress and interest in using AI for illness prevention. For instance, 'polygenic risk scores' that may be used to identify a person with an elevated hereditary risk for disease and could benefit from closer monitoring have been demonstrated to be valuable in the development of AI and machine learning approaches. [86–88] In addition, illnesses may be stopped in their tracks before complex therapies are required for more severe manifestations of the disease by combining knowledge of genetic susceptibility to disease with ongoing surveillance to detect early indicators of disease. Using artificial intelligence (AI) methods with cutting-edge sensors might significantly improve this kind of monitoring. At the end of the day, the excitement around the use of AI methods is not going to die down. Manufacturing, sales and marketing, banking, the financial sector, and even transportation might all be affected by AI. Artificial intelligence (AI) has the potential to significantly contribute to the necessary advances across all of these sectors. This segment has been able to demonstrate that the healthcare sector has just as much to gain from AI as any other, provided that it is integrated and tested properly.

5 Reference

[1] Segler MHS, Preuss M, and Waller MP, Planning chemical syntheses with deep neural networks and symbolic AI. Nature, 2018. 555(7698): p. 604–610.

[2] Ahneman DT, et al., Predicting reaction performance in C-N cross-coupling using machine learning. Science, 2018. 360(6385): p. 186–190.

[3] Radovic A, et al., Machine learning at the energy and intensity frontiers of particle physics. Nature, 2018. 560(7716): p. 41–48.
[4] Silver D, et al., Mastering the game of Go without human knowledge. Nature, 2017. 550(7676): p. 354–359.
[5] Madhukar NS, et al., A New Big-Data Paradigm For Target Identification And Drug Discovery. BioRxiv (10.1101/134973), 2018.
[6] Chen B and Butte AJ, Leveraging big data to transform target selection and drug discovery. Clin Pharmacol Ther, 2016. 99(3): p. 285–97.
[7] Hu Y and Bajorath J, Entering the 'big data' era in medicinal chemistry: molecular promiscuity analysis revisited. Future Sci OA, 2017. 3(2): p. FSO179.
[8] Hernandez D, How Robots Are Making Better Drugs, Faster, in Wall Street Journal. 2018, Dow Jones & Company New York, New York.
[9] Patient-centered drug manufacture. Nat Biotechnol, 2017. 35(6): p. 485.
[10] Schellekens H, et al., Making individualized drugs a reality. Nat Biotechnol, 2017. 35(6): p. 507–513.
[11] Mukhopadhyay, A., Sumner, J., Ling, L. H., Quek, R. H. C., Tan, A. T. H., Teng, G. G., ... & Motani, M. (2022). Personalised Dosing Using the CURATE. AI Algorithm: Protocol for a Feasibility Study in Patients with Hypertension and Type II Diabetes Mellitus. International Journal of Environmental Research and Public Health, 19(15), 8979.
[12] Blasiak, A., Truong, A. T., Remus, A., Hooi, L., Seah, S. G. K., Wang, P., ... & Ho, D. (2022). The IDentif. AI-x pandemic readiness platform: Rapid prioritization of optimized COVID-19 combination therapy regimens. NPJ digital medicine, 5(1), 1-12.
[13] Vadapalli, S., Abdelhalim, H., Zeeshan, S., & Ahmed, Z. (2022). Artificial intelligence and machine learning approaches using gene expression and variant data for personalized medicine. Briefings in bioinformatics.
[14] Perumal, S., Escalation of Security and Privacy in Internet of Things using Advanced IPv6 Based Security Mechanism. Wasit Journal of Computer and Mathematics Science, 2021: p. 43-51.
[15] J. Q. Kadhim, , Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT. International Journal of Emerging Technologies in Learning (iJET), 2023. 18(02).
[16] D. Al-Malah, H.H.K.J., Enhancement of educational services by using the internet of things applications for talent and intelligent schools. Periodicals of Engineering and Natural Sciences (PEN), 2020. 8(4): p. 2358-2366.
[17] Ibrahim, H., A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. Wasit Journal of Computer and Mathematics Sciences, 2022. 1(3): p. 76-108.
[18] Jasim, N.A., and M.S. Farhan. Internet of Things (IoT) application in the assessment of learning process. in IOP Conference Series: Materials Science and Engineering. 2021. IOP Publishing.
[19] Hassan, H.A., Review Vehicular Ad hoc Networks Security Challenges and Future Technology. Wasit Journal of Computer and Mathematics Science, 2022. 1(3).
[20] Khalifa, M.A., et al., A Novel Arabic Words Recognition System Using Hyperplane Classifier. Wasit Journal of Computer and Mathematics Sciences, 2022. 1(2): p. 12-20.
[21] Alaidi, A.H.M., et al., Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques. International Journal of Interactive Mobile Technologies, 2022. 16(10).
[22] Alam, S., Smart health costing system. Wasit Journal of Computer and Mathematics Sciences, 2022. 1(3): p. 70-75.

[23] Al-Jaff, S., O. Bayat, and A.H. Sallomi. Analysis of Interference and Signal Quality in Cellular Wireless Networks. in IOP Conference Series: Materials Science and Engineering. 2020. IOP Publishing.
[24] Salim, H.T. and Hussein .T. Hazim, Secure Chaos of 5G Wireless Communication System Based on IOT Applications. International Journal of Online & Biomedical Engineering, 2022. 18(12).
[25] Rihab Salah Khairy, A.S.H., The Detection of Counterfeit Banknotes Using Ensemble Learning Techniques of AdaBoost and Voting. International Journal of Intelligent Engineering and Systems, 2021. 14(1): p. 326-339.
[26] H. Alrikabi, H.T.H., Enhanced Data Security of Communication System using Combined Encryption and Steganography. International Journal of Interactive Mobile Technologies, 2021. 15(16): p. 144-157.
[27] Lin, B., & Wu, S. (2022). Digital transformation in personalized medicine with artificial intelligence and the internet of medical things. OMICS: A Journal of Integrative Biology, 26(2), 77-81.

Article submitted 20 November 2022. Published as resubmitted by the authors 20 December 2022.

Networks Data Transfer Classification Based on Neural Networks

https://doi.org/10.31185/wjcm.96

Doaa Mohsin Abd Ali(✉)
Al- Mustansiriyah University.
Doaa_muhsin@uomustansiriyah.edu.iq

Donia Fadil Chalob
Al- Mustansiriyah University.
donia_fadil@uomustansiriyah.edu.iq

Ameer Badr Khudhair
Al-Mansour University College.
Ameer.badr@muc.edu.iq

Abstract— Data transmission classification is an important issue in networks communications, since the data classification process has the ultimate impact in organizing and arranging it according to size and area to prepare it for transmission to minimize the transmission bandwidth and enhancing the bit rate. There are several methods and mechanisms for classifying the transmitted data according to the type of data and to the classification efficiency. One of the most recent classification methods is the classification of artificial neural networks (ANN). It is considered one of the most dynamic and up-to-date research in areas of application. ANN is a branch of artificial intelligence (AI). The neural network is trained by backpropagation algorithm. Various combinations of functions and their effect while utilizing ANN as a file, classifier was studied and the validity of these functions for different types of datasets was analyzed. Back propagation neural university (BPNN) supported with Levenberg Marqurdte (LM) activation function might be utilized with as a successful data classification tool with a suitable set of training and learning functions which operates, when the probability is maximum. Whenever the maximum likelihood method was compared with backpropagation neural network method, the BPNN supported with Levenberg Marqurdte (LM) activation function was further accurate than maximum likelihood method. A high predictive ability against stable and well-functioning BPNN is possible. Multilayer feed-forward neural network algorithm is also used for classification. However BPNN supported with Levenberg Marqurdte (LM) activation function proves to be more effective than other classification algorithms.

Keywords— Data Transmission, Levenberg Marqurdte (LM) Activation Function, Back Propagation Neural University (BPNN), Artificial Neural Networks (ANN).

1 Introduction

The amount of data is advancing at an exponential rate, and in order to extract useful information from it, it is necessary to analyze such enormous amount of data. The field of data mining emerged as a result of this. The extraction of knowledge along such a large sum of databases is referred to as data mining. Information mining is center of KDD operation. KDD is coordinated course of recognized, legitimate, novel, helpful and reasonable example from enormous and complex dataset. [1]. Tasks involving data mining fall towards two categories: expressive and prescient. Time series analysis, classification, and regression are examples of predictive tasks, whereas clustering and association rules are examples of descriptive tasks [2]. Such approaches might be utilized in particular areas. Talk about these techniques and how they might be applied in various fields. Applications for data mining can be found in a wide range of fields, containing banking, insurance, medicine, finance, marketing, healthcare, and sales [4,5]. A method of data mining called classification is used to predict the class of objects. It's a good demonstrating of supervised learning. The categorical label is predicted by classification (discrete, ordered). There are two steps involved in data classification. A classifier is built to describe a predetermined set of data classes during the learning (or training) step of the early step. The first-stage model is used in the second step to classify unknown data, and test data are used to estimate the classifier's accuracy. Decision tree, K nearest neighbor, naive Bayesian classifier, and artificial neural network are just a few of the classification algorithms available [7].8] provides an examination of these classification algorithms in comparison. An artificial neural network is a method of machine learning used to solve classification issues.

It is usually referred to as the neural network model and is a branch of artificial intelligence or Artificial Neural Networks (ANNs). The ANN learns the system to perform the mission, rather than programming an algorithm to perform specific tasks. to achieve such synthetic tasks. The AI system is being created as an operating model which might find patterns buried in data that replicate useful knowledge quickly and accurately. Neural networks are one case of AI schemes, being that AI systems should discover from data on a consistent basis in regions medical diagnosis using dissimilar data, the utmost available techniques are Artificial intelligence technologies. An artificial neural network consists of various artificial neurons linked together according to the design network geometry. The objective of a neural network is to convert inputs to important outputs. Learning placement might be supervised or unsupervised. Neural Networks actually learn in the presence of noise. Data Classification is a two stages process: (1) the preparation (or learning) stage and (2) the test (or assessment) stage where the genuine class of the occasion is contrasted and the anticipated class. On the off chance that the hit rate is OK to the examiner, the classifier is acknowledged as being fit for grouping future cases with obscure class. Characterization of data is a two-step process: (1) the preparation (or learning) stage and (2) the testing (or assessment) stage where the real class of the case is contrasted with the normal class. In the event that the hit rate is OK to the parser, the classifier is acknowledged as having the option to group future occurrences with an obscure class [1,11].

a) Data Classifications

Actually, data classification is a very important subject, since data classification is the process of analyzing structured or unstructured data and organizing it into categories based on file type, contents, and other metadata. Data classification helps organizations answer necessary questions concerning their data which inform how they mitigate risk and manage data governance policies. Data types with similar levels of risk sensitivity are grouped together into data labels. Networks use four data classifications: unclassified, controlled, restricted, censored, and public information. Classification is a data extraction function that maps items in a collection to target classes or classes. The goal of classification is to accurately predict the target group for each case in the data. For example, a rating model can be used to identify loan applicants as low, medium, or high credit risk. Figure 1 displays an example of data classification scheme.

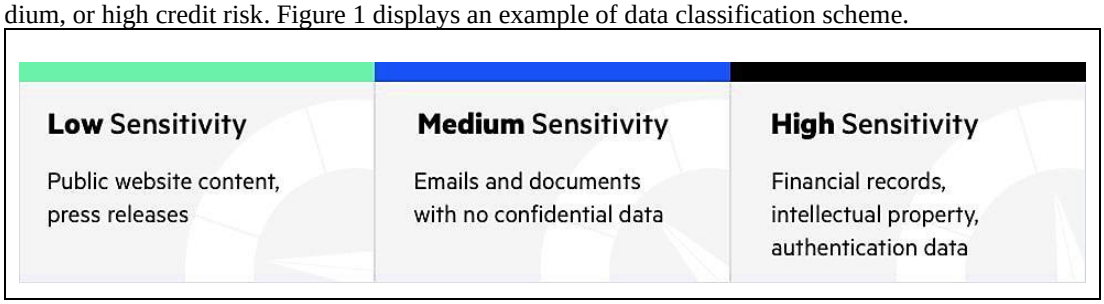


Fig. 1. An example of data classification scheme [4].

b) Classification Algorithms

Classification is commonly obtained by supervised learning but might also be achieved via unsupervised learning, e.g. where the category is not utilized or is unknown as in the ensemble technique. For the examine or test, we apply algorithms from the following methods: (1) Decision tree, (2) Rule extrapolation, (3) Clustering, (5) Artificial neural network (ANN), (6) Bayesian classifier and (6) Support vector machine. Classifiers' performance is usually computed by an accuracy scale. Such metric is evaluated by dividing the number of correctly categorized instances by the total amount of the instances. A properly classed instance is an instance in which the classifier expects the correct class for the test instance [11,12]. Also by referring to [5-10] we might locate the arrangement of the classification algorithms which are sorted according to the action quality as presented in Table 1.

Table 1. Total Accuracy by Technique [12].

Technique	Average accuracy
Decision Trees	83,10%
Artificial Neural Networks	82,85%
Rules	82,76%
Clustering	82,07%
Bayesian Classifiers	81,76%
SVM	74,72%

As might be observed from Table 1, the best accuracy is achieved using the decision tree algorithm, which may be preferable to apply it to data classification. It also competes against the ANN algorithm in second place, which provides very close efficiency, as it is the preferred algorithm depending on the state and conditions of the data and the network.

2 Related Works

In this section, we will introduce a survey of the utmost available articles along with relevant recent scientific studies concerning the subject of data classification using ANNs. The algorithm's learning rate, weight, bias, and initial parameter setting are the foundation of the neural network training method. It begins its leaning with a certain starting value, and the weight is updated with each iteration. The structure of a neural network is intricate and time-consuming to train. Such element made brain network less appropriate for order in information mining. It is possible to suggest a method for learning both the weight and the structure of the network. Weight adjustment in ANN is a combinatorial problem, and we must optimize the weight to achieve the desired output. The following are some approaches to ANN learning in various classification problems:

a) Artificial neural network with back propagation [10] suggests one variant of an ANN with BP for use in the classification of Landsat data. The neural network is trained with the back propagation algorithm. For multispectral image classification, another variant of ANN with BP is proposed in [11].The neural network is used to classify the image after the BP is trained on a traditional area of the image.

b) Improved back propagation algorithm [12] Discuss the gradient delta rule-based neural network training with back propagation algorithm. It is very useful for architectures of parallel hardware. Instead of remaining constant, the momentum factor is determined with each step. Speed and convergence stability are better with improved BP than with conventional BP.

Some meta-heuristic algorithms in soft computing include the cuckoo search, firefly, genetic, and particle swarm optimization algorithms [13].Neural network training can benefit from these meta-heuristic algorithms. The meta-heuristic algorithms can be used in any field and yield approximate results. Where traditional algorithms produce

a local optimum, these algorithms are used. Additionally, traditional algorithms consume more time to produce results and incur higher computational costs. To circumvent its limitations, numerous researchers used ANN in conjunction with these meta-heuristic algorithms in previous research. The following are examples:

- **ANN with Particle Swarm Optimization (PSO)** A developmental framework which is a mix of structural advancement with weight learning, called PSONN, to work on the exhibition of fake brain networks was proposed in [14].In some structural methods, such as hill climbing, where the results are susceptible to becoming trapped at structure local optima, the initial network architecture determines the outcome. The hybrid method known as PSONN is utilized on two issues in the medical field: heart problems and breast cancer.[15] suggested a hybrid approach that combines the advantages of PSO and BP by utilizing the global searching capabilities of PSO and BP's local searching capabilities. Compared to BP, this hybrid method provides better classification accuracy and uses less CPU time. The iris classification issue is the focus of its application.[16] For fruit classification, a method that combined PSO, ABC, and a single hidden layer feed forward neural network was proposed.
- **ANN with Genetic Algorithm (GA)** [17] Present a brand-new hybrid neural network structure for the purpose of categorizing ECG beats. It is used to determine the number of nodes and their weight in the first layer of a neural network.[18] The land cover classification of remotely sensed data is demonstrated using a genetic algorithm and neural network in this paper. Back propagation and real coded GA hybrid are used. The neural network is optimized with genetic operators to prevent premature convergence. On GA, the BP algorithm is used to determine the initial connection weight.
- **DNA microarray classification was proposed by ANN with Artificial Bee Colony (ABC)** [19].ABC is used to reduce dimensionality and select the best set of genes for identifying specific diseases. These reduced genes are then used to teach ANN how to classify the DNA microarray.[20] Classify an MR brain image as normal or abnormal by utilizing a hybrid approach that combines improved ABC and forward neural network (FNN).Improved ABC, which is based on fitness scaling and chaotic theory, is used to optimize FNN parameters.[21] Train the neural network for the classification problem in the medical field using the ABC algorithm. The crossover method is applied on nine different certifiable issue of clinical area.
- **The improved cuckoo search was used to train the neural network in ANN with improved cuckoo search (ICS)** [22].The behavior of the cuckoo species, which lay their eggs in the nests of host species, serves as inspiration for the cuckoo search. In terms of parameters, improved cuckoo search differs from standard cuckoo search. To find an improved solution both globally and locally, the parameters pa and alpha are used. The algorithm's accuracy and convergent rate are improved as a result. The value of these parameters is fixed in the standard cuckoo search.
- **Ant Colony Optimization (ACO) was used for ANN training** [23] to optimize the neural network's weight. It teaches the neural network how to classify patterns.[24] trained the ANN using a hybrid approach consisting of ACO and BP. Local optima are entrapped by back propagation (BP).Therefore, the global optimization

algorithm will be utilized in this hybrid training to provide BP with good initial weight. These two methods are utilized for the classification of medical data : diabetes, heart, and cancer datasets.

ANN with forbidden search [35] Proposed a framework which half breed the four methods to be specific hereditary calculation reproduced tempering, unthinkable pursuit and back proliferation is utilized for brain network preparing. The uphill property of simulated annealing also exists (occasionally accepting bad moves). The parallel search characterizes GA. Flexible memory is a feature of tabu search. All of these aspects are combined in the proposed system. Four classification problems and one prediction problem are solved using the proposed method.

ANN with GSA (gravitational inquiry streamlining) [36] Propose an iris acknowledgment framework. It provides two half breed strategies FNNPSO and FNNGSA for iris characterization. It consists of four stages: using ANN, image acquisition, segmentation, normalization, and feature extraction are followed by classification. In order to train neural networks with optimal biases and weights, both PSO and GSA are utilized.

ANN with biogeography-based optimization [37] Provide a technique for classifying fruits based on their shape, color, and texture. The weight of the neural network is updated using an optimization algorithm based on biogeography.

The proposed neural network model for a fuzzy logic control and decision system is based on an ANN. A neural network's training example might be utilized to construct a fuzzy and decision system, and a connectionist structure might be trained to develop a fuzzy logic rule and discover an input-output relationship.

3 Methodology

In order to implement the idea of the data classification using artificial neural networks (ANNs), the concept of ANN algorithm must be understood for data classification aspects. A weight is assigned to each connection in an ANN, which is a collection of connected input and output networks. One input layer, one or more intermediate layers, and one output layer make up the structure. The neural network learns by varying the weight of each connection. The network's performance is improved incrementally by updating the weight. ANN might be divided into two groups based on their connection: recurrent network and feed-forward network. A feed forward neural network is one in which unit-to-unit connections do not cycle, whereas a recurrent neural network does [9]. The learning rule, the architecture, and the transfer function all have an impact on the behavior of a neural network. The weighted sum of the input triggers the activation of neural network neurons. A single neuron output is produced when the activation signal is transmitted through the transfer function. This transfer function results in a nonlinear network. The interconnection weight is improved during training until the network achieves the desired level of accuracy. It is useful in a variety of applications, including pattern recognition [2], medical [2,3], business applications [4], [4], pharmaceutical science [5], bankruptcy application [6], and speech recognition [7,8]. It has several advantages, such as parallelism, less affected by noise, and good

learning ability [9]. Compatibility, tolerance for noisy data, parallelism, and the ability to learn from examples are among the neural network's most appealing features. The network's speed is increased by parallelism. However, in addition to these benefits, it has numerous drawbacks. First, neural network training is expensive and time-consuming. The accuracy of a classification is significantly impacted by the training of a neural network. There are numerous algorithms for neural network training [10]. It has been argued that neural networks lack interpretability. For instance, it is challenging for humans to decipher the symbolic meanings of the network's "hidden units" and learned weights.

3.1 ANN Structure

The neurons utilized in the ANN algorithm are numeric amounts. It is represented as a model of biological neurons. Formal neurons might be thought of as primitive units in a pseudo-neural network. The shown graph deals with the general numerical model of formal neurons [20] and as shown in Figure 2:

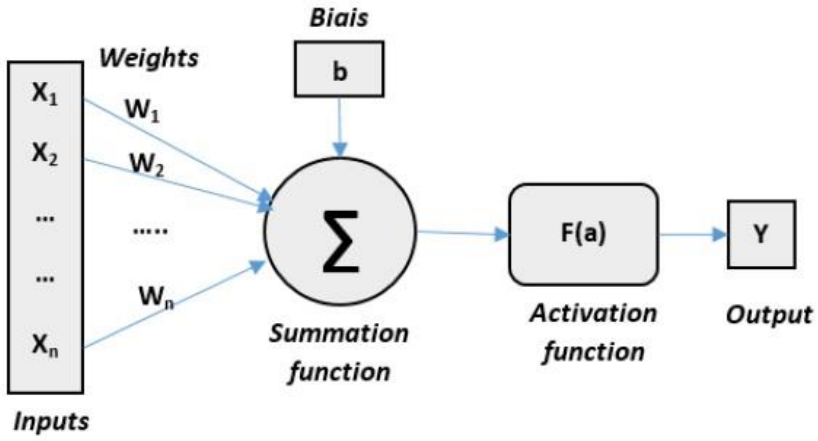


Fig. 2. Numerical structure of the formal neuron.

The formal neuron which is illustrated in the above figure has n inputs indicated as $\{X1,X2,\dots ,Xn\}$. Every line which interfaces such contributions to the addition intersection is allocated a weight signified as $\{W1,W2,\dots ,Wn\}$. The net info yin can be determined as follows:

$$yin = x1.w1 + x2.w2 + x3.w3 + \dots + xn.wn + b \quad (1)$$

The improveimg function $F(a)$ is part of the essential pieces of a neuron. A little initiation capacities might be thought of (limit work, direct capacity, sigmoid capacity …). In this study, we have picked a sigmoid function as presented in Figure 3, for its nonlinearity which composes it conceivable to inexact either capacity. Finally, the resulting $\boldsymbol{y}$ of the neuron is provided in the accompanying recipe:

$$y = F(y_{in}) \sum w_i * x_i + b \quad (2)$$

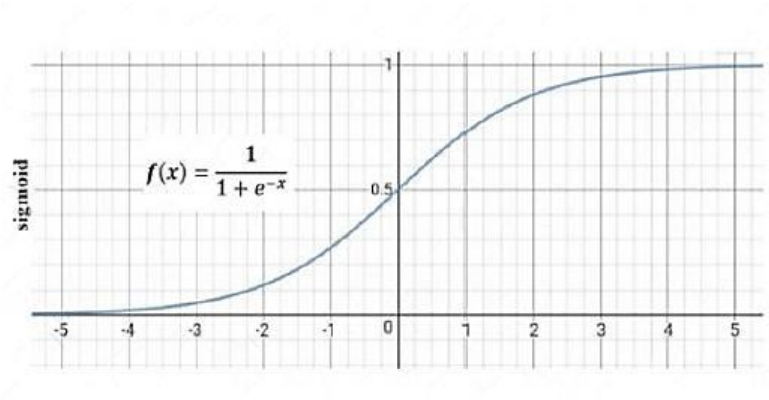


Fig. 3.the sigmoid function illustration.

3.2 Multi-Layer Perceptron

The multi-facet perceptron (MLP) displayed in Figure 4 is a class of feed-forward fake neural network that has somewhere around three layers of hubs. It creates a bunch of yields $\{y_1, y_2, \ldots, y_m\}$ from a bunch of data sources $\{X_1, X_2, \ldots, X_n\}$. With the exception of the info hubs, every hub is a neuron that utilizes a nonlinear initiation work [22-24].

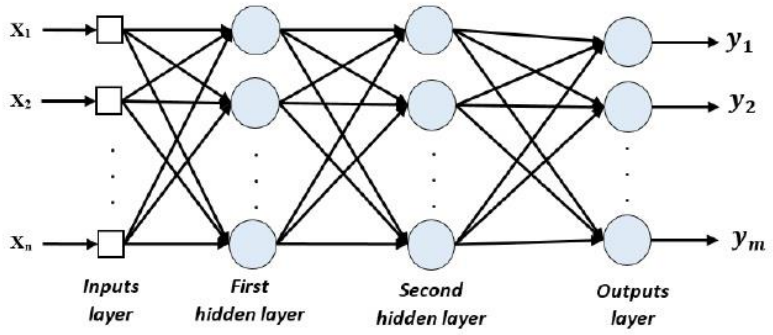


Fig. 4. Block diagram of MLP scheme.

A neural network is prepared with info and target pair designs with the capacity of learning. MLP can isolate information that isn't directly recognizable [21]. It is particularly prepared utilizing a supervised learning technique got back to propagation (BP)

algorithm [22], which targets limiting the worldwide mistake estimated at the yield layer by the connection howl:

$$e(t) = yd\ (t) - ym\ (t) \tag{3}$$

Where $yd(t)$ signifies the ideal output, and ym (t) the deliberate yield of the neuron.

The BP algorithm utilizes an iterative supervised learning system, where the MLP is prepared with a bunch of predefined sources of info and yields. The worldwide mistake Eg (t) is determined by equation (4), this blunder can be limited by the gradient descent technique [23].

$$E_g(t)=\frac{1}{2}\sum_{i=1}^{n}\left(y_{d,i}(t) - y_{m,i}(t)\right)^2 \tag{4}$$

There are a few preparing algorithms that might become utilized to train a MLP network. In this study, we will present a subjective examination between two preparing algorithms: semi newton and form slope. Wherein the pre-owned preparing capacities are separately train-lm: (Levenberg Marquardt (LM)) and train-scg (Scaled Conjugate Gradient (SCG)).

3.3 The Proposed Data Classification with ANN Algorithm

The operation of the proposed structure will be implemented using data set from www//http//kaggle.com web site, representing medical data having information of mixed medicine cancer cases for a medicine health center. These mixed data are various type of cancer cases with different levels of importance according to the patient case. Such data sets will be entered to the designed ANN algorithm in order to classify them according to their importance. The block diagram of the suggested model is shown in Figure 5.

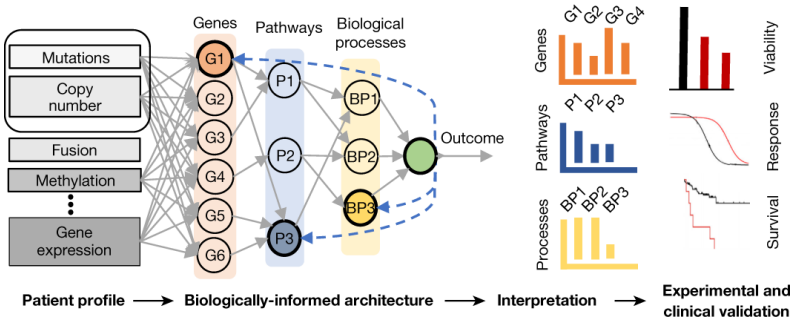


Fig. 5. The block diagram of the suggested model.

Also, the flowchart of the proposed data classification along ANN algorithm has been illustrated in Figure 6.

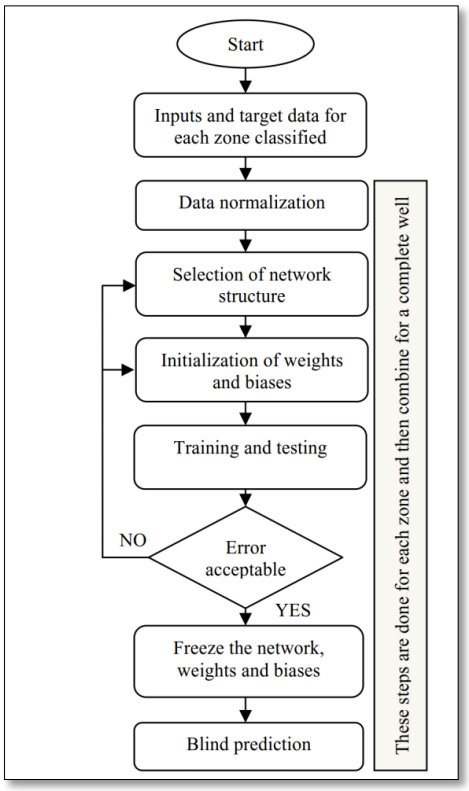


Fig. 6.the flowchart of the proposed data classification along ANN algorithm.

The data set will be entered to the first ANN layer to be prepared for analysis. The data are normalized, then the network structure will be selected according to the design (backpropagation neural network method, the BPNN supported with Levenberg Marqurdte (LM) activation function). Next, the ANN weights and their basis will be normalized. The entered data will be trained and tested according to the designed ANN settings. After that, the resulting response will compared with the required targits, if the error still high, the process will be repeated untill reaching to the acceptable error. Hence the weights and basis will be recorded and the program will be terminated.

4 Simulation Results

The proposed structure has been implemented and examined successfully utilizing MatLab2020 simulation program, m. files. This software, will employ the ANN algorithm upon entered-packets data samples. The suggested scheme design requirements are tabulated in table 2.

ANN algorithm Details	Cancer Data Size	Input Layer	Hidden Layer	Output Layer
	9× 699	9	50	2

The designed ANN algorithm with backpropagation neural network method, the BPNN supported with Levenberg Marqurdte (LM) activation function is presented in Figure 7.

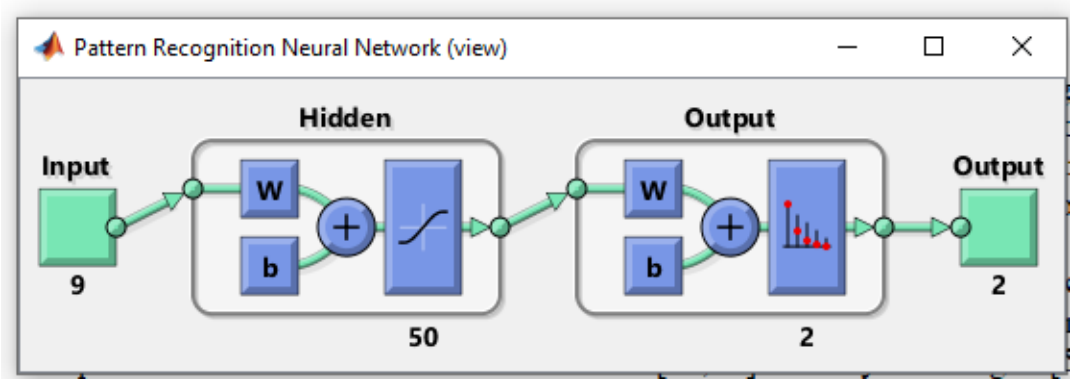


Fig. 7. Structure of the ANN architecture [12].

The program has been implemented according to the entered cancer cases data sets, and the resulting performances of the ANN algorithm training are illustrated in the in-comming figures.

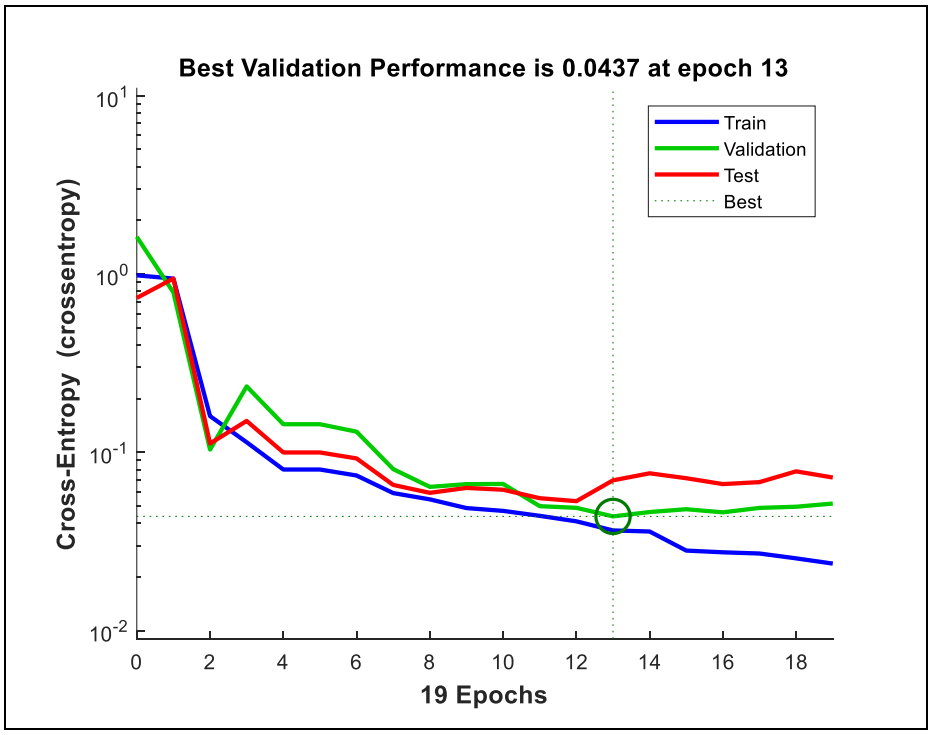


Fig. 8. Eroor performance of the ANN architecture algorithm examination.

From the above figure, it is obvious that, the best validation performance of the mean square erroe (MSE) has been achieved with 0.0437 at epoche of 13. Next, the confusion matrix has been obtained and displayed in Figure 9.

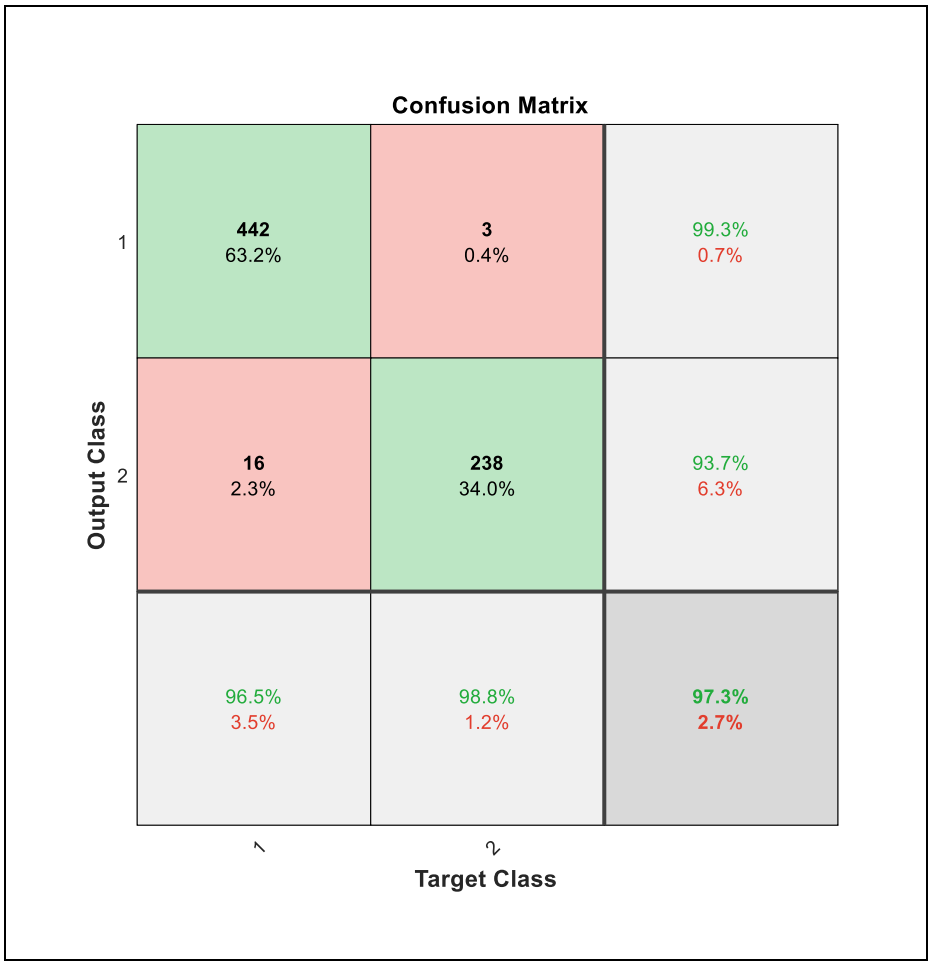


Fig. 9. The confusion matrix.

By referring to Figure 9, the confusion matrix of our implemented data classification against ANN algorithm has shown a very high matching among the resulting class with the targit class with 97.3% matching and onlt 2.7% missmatch. Also, the gradient and the validation fall results have been illustrated in Figure 10.

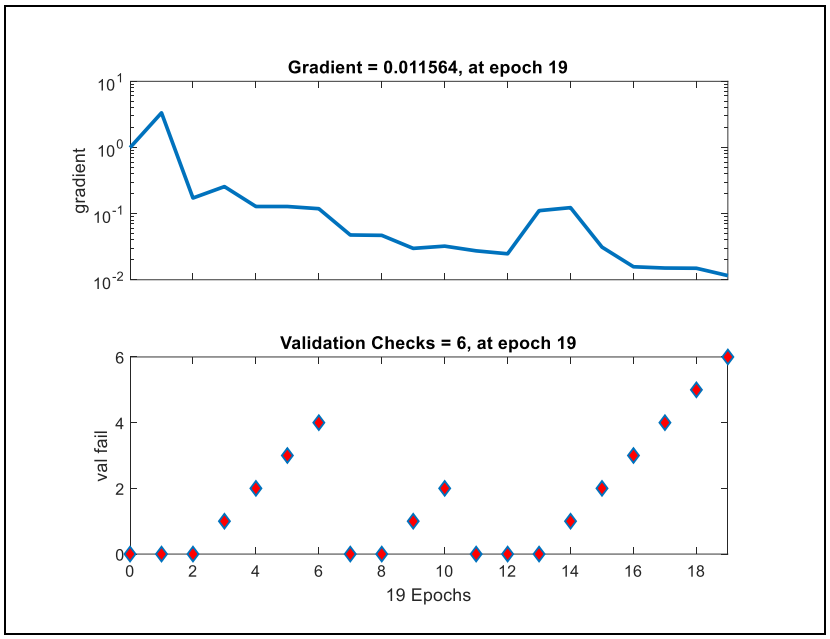


Fig. 10. The gradient and the validation fall results.

A very good gradient value of 0.011564 with validation check of 6 at epoche 19 those ensuring the excellent performance of the examination program. Furthermore, the error histogram of the algorithm has been displayed in Figure 11.

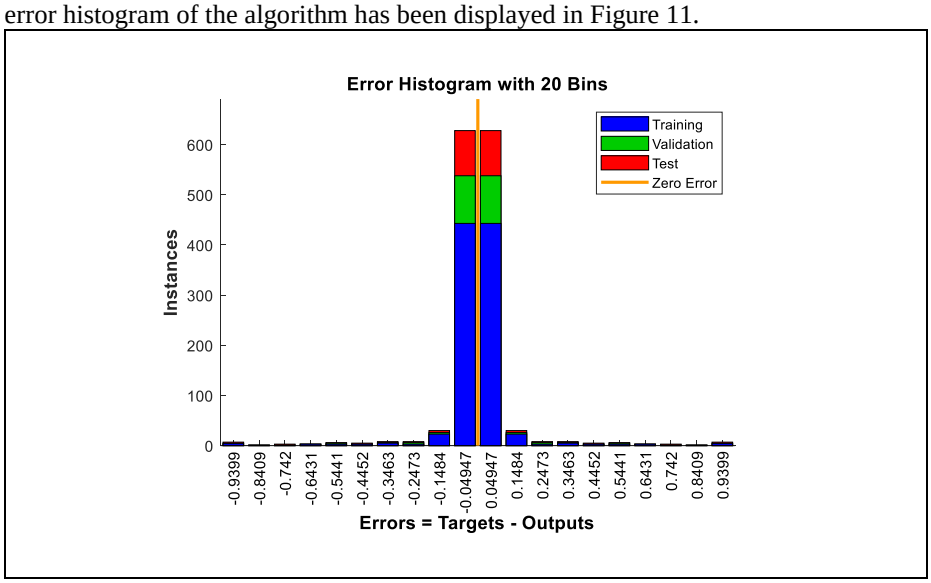


Fig. 11. Error histogram of the ANN algorithm.

Moreover, the error performance of the examination program showing an excellent performance for the trained, validated, and tested instances, with 0.04957 error amount. Finally, the receiver operating characteristic curves have been shown in Figure 12.

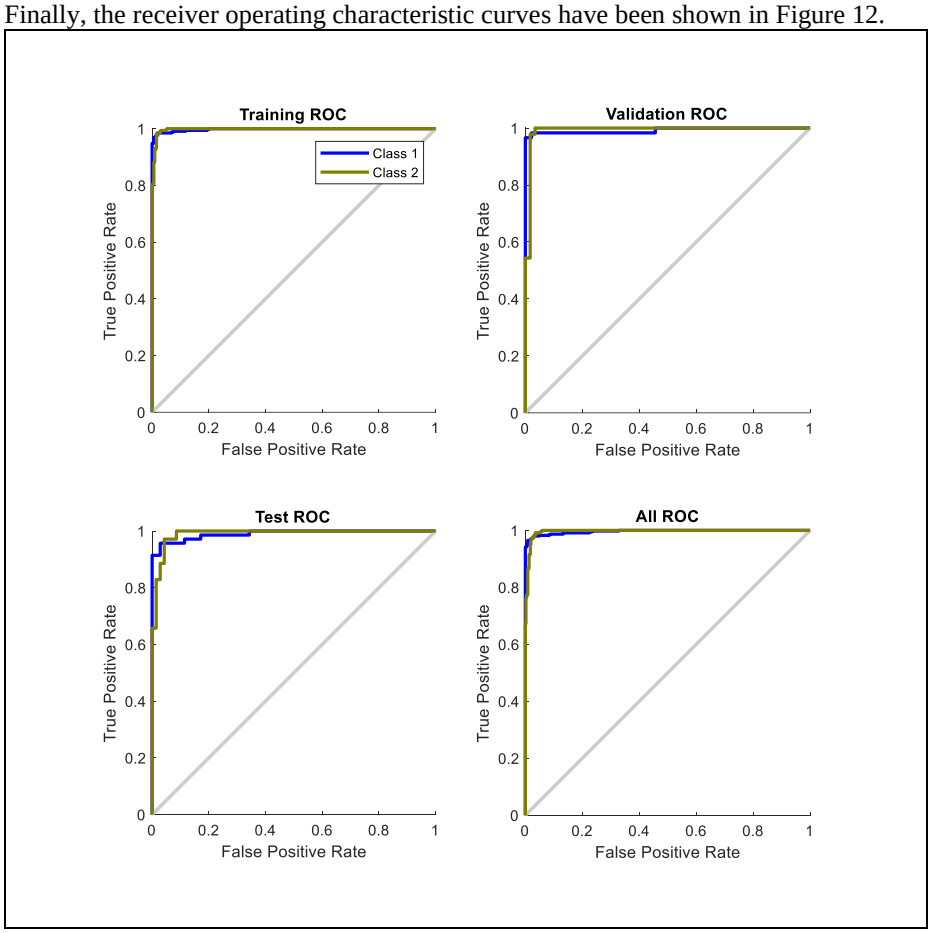


Fig. 12. The receiver operating characteristic curves.

At last, the ROC curves of the implemented ANN algorithm presenting a perfect matching among true with false posetive rates for the trained, validated, tested, and all cases. This indicates that the examined cancer data have been perfectly matched with the required classes. Now, the plot of the entered cancer data set have been illustrated in Figure 13. The figure shows the connections among the training set with the target data values for each input data value which have been indicated with blue colour. Also, the plot of the obtained classified cancer data set have been presented in Figure 14. Similarly, the figure shows the connections among the validation set with the validation data values for each input data value which have been indicated with red colour.

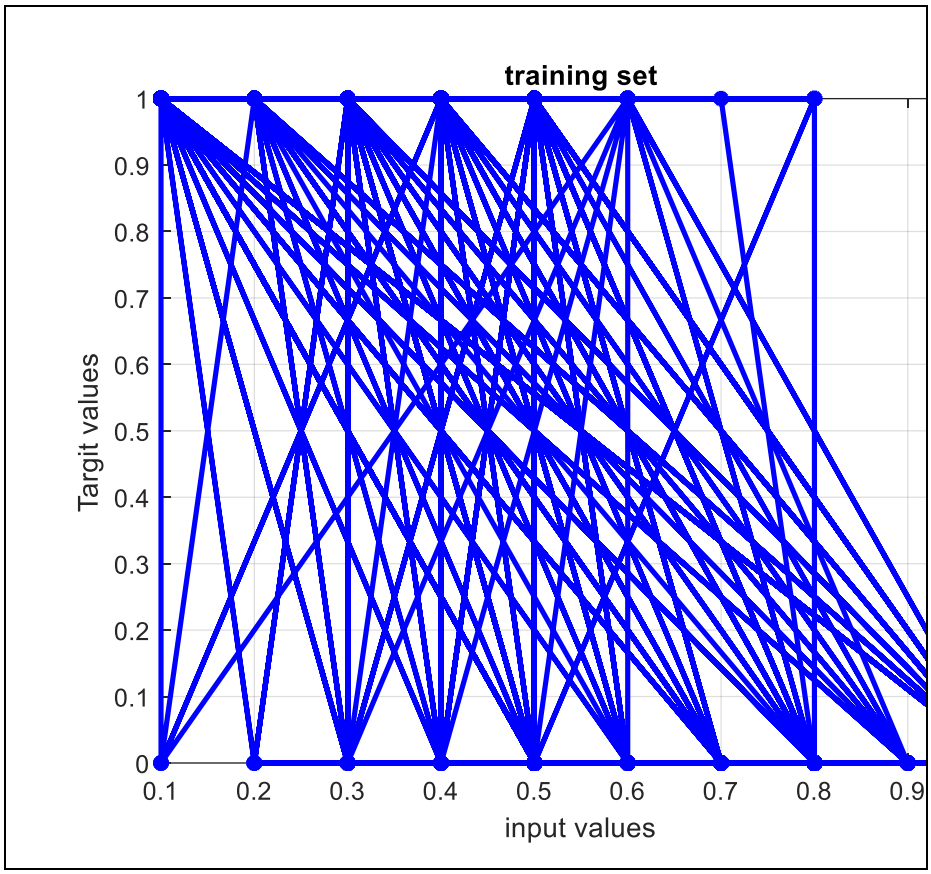


Fig. 13. The plot of the entered cancer data set.

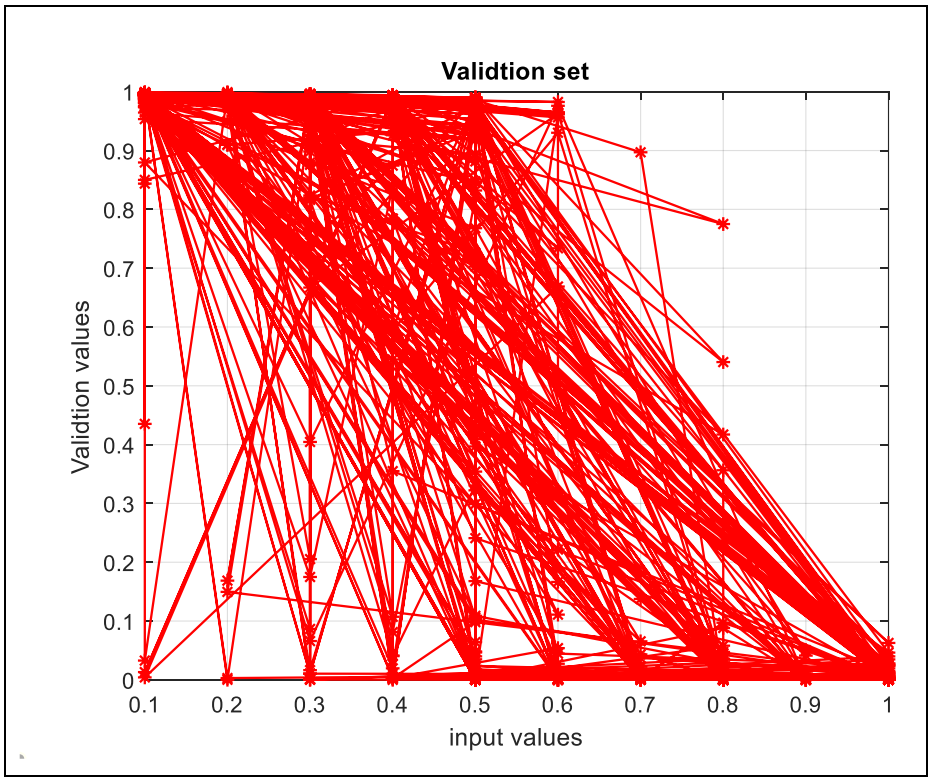


Fig. 14. The plot of the obtained classified cancer data set.

5 Conclusions

Artificial neural network (ANN) classification is one of the most recent classification techniques. It is regarded as one of the most dynamic and current areas of application-related research. A subfield of artificial intelligence (AI) is ANN. The backpropagation algorithm is used to train the neural network. Back propagation neural university (BPNN) with Levenberg Marqurdte (LM) activation function might be applied as a successful data classification tool with the right set of training and learning functions that work at maximum likelihood. In this study, the validity of such functions for cancer based datasets was examined, as was the effect of various combinations of functions when using ANN as a file classifier. The BPNN supported by Levenberg Marqurdte (LM) activation function was more accurate than the maximum likelihood method when compared to the backpropagation neural network approach. It is possible to have a high predictive ability against BPNN that is stable and operates well. For cancer data classification, the multilayer feed-forward neural network algorithm is also utilized. The Levenberg Marqurdte (LM) activation function-supported BPNN, on the other hand, outperforms other classification algorithms. The obtained results were very good with the best validation performance of the mean square erroe (MSE) of 0.0437 at

epoche of 13. Also, the confusion matrix of our implemented data classification against ANN algorithm has shown a very high matching among the resulting class against the targit class with 97.3% matching and onlt 2.7% missmatch. Furthermore, the ROC curves of the implemented ANN algorithm presenting a perfect matching among true with false posetive rates for the trained, validated, tested, and all cases. This indicates that the examined cancer data have been perfectly matched with the required classes.

6 References

[1] S. Knerr, L. Personnaz, and G. Dreyfus, “Handwritten digit recognition by neural networks with single-layer training,” IEEE Trans. Neural Netw., vol. 3, no. 6, pp. 962–968, 1992.

[2] D. M. Joshi, N. K. Rana, and V. M. Misra, “Classification of brain cancer using artificial neural network,” in Electronic Computer Technology (ICECT), 2010 International Conference on, 2010, pp. 112–116.

[3] F. Y. partovi and murujan anandrajan, “classifying inventory using artificial neural network approach,” Comput. Ind. Eng., vol. 41, no. 4, pp. 389–404, 2002.

[4] D. C. Park, M. A. El-Sharkawi, R. J. Marks, L. E. Atlas, and M. J. Damborg, “Electric load forecasting using an artificial neural network,” IEEE Trans. Power Syst., vol. 6, no. 2, pp. 442–449, 1991. 1818 Rajni Bala, Dr. Dharmender Kumar

[5] S. Agatonovic-Kustrin and R. Beresford, “Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research,” J. Pharm. Biomed. Anal., vol. 22, no. 5, pp. 717–727, 2000.

[6] G. Zhang, M. Y. Hu, B. E. Patuwo, and D. C. Indro, “Artificial neural networks in bankruptcy prediction: General framework and cross-validation analysis,” Eur. J. Oper. Res., vol. 116, no. 1, pp. 16–32, 1999.

[7] herve bourlard and nelson morgan, “Continuous Speech Recognition by Connectionist Statistical Methods,” IEEE Trans. Neural Netw., vol. 4, no. 6, pp. 893–909, 1993.

[8] R. P. Lippmann, “Review of neural networks for speech recognition,” Neural Comput., vol. 1, no. 1, pp. 1–38, 1989.

[9] patric van der smagt, “Minimisation methods for training feedforward neural networks,” Neural Netw., vol. 7, no. 1, pp. 1–11, 1994.

[10] H. Bischof, W. Schneider, and A. J. Pinz, “Multispectral classification of Landsat-images using neural networks,” IEEE Trans. Geosci. Remote Sens., vol. 30, no. 3, pp. 482–490, 1992.

[11] P. D. Heermann and N. Khazenie, “Classification of multispectral remote sensing data using a back-propagation neural network,” IEEE Trans. Geosci. Remote Sens., vol. 30, no. 1, pp. 81–88, 1992.

[12] J. leonard and M. . kramer, “improvement of backpropagation algorithm for training neural network,” Comput. Chem. Eng., vol. 14, no. 3, pp. 337–341, 1990.

[13] S. Binitha, S. S. Sathya, and others, “A survey of bio inspired optimization algorithms,” Int. J. Soft Comput. Eng., vol. 2, no. 2, pp. 137–151, 2012.

[14] C. Zhang, H. Shao, and Y. Li, “Particle swarm optimisation for evolving artificial neural network,” in Systems, Man, and Cybernetics, 2000 IEEE International Conference on, 2000, vol. 4, pp. 2487–2490.

[15] Jing Ru Zhang, jun Zhang, Tat Ming Luk, and Michael R. Lyu, “hybrid particle swarm optimization–back-propagation algorithm for feedforward neural network training,” Appl. Math. Comput., vol. 185, no. 2, pp. 1026–1037, 2007.

[16] S. Lu, Z. Lu, P. Phillips, S. Wang, J. Wu, and Y. Zhang, “Fruit classification by HPA-SLFN,” in Wireless Communications & Signal Processing (WCSP), 2016 8th International Conference on, 2016, pp. 1–5.
[17] Z. Dokur and T. Ölmez, “ECG beat classification by a novel hybrid neural network,” Comput. Methods Programs Biomed., vol. 66, no. 2, pp. 167–181, 2001. Classification Using ANN: A Review 1819
[18] Z. Liu, A. Liu, C. Wang, and Z. Niu, “Evolving neural network using real coded genetic algorithm (GA) for multispectral image classification,” Future Gener. Comput. Syst., vol. 20, no. 7, pp. 1119–1129, Oct. 2004.
[19] B. A. Garro, K. Rodríguez, and R. A. Vázquez, “Classification of DNA microarrays using artificial neural networks and ABC algorithm,” Appl. Soft Comput., vol. 38, pp. 548–560, Jan. 2016.
[20] Y. Zhang, L. Wu, and S. Wang, “Magnetic resonance brain image classification by an improved artificial bee colony algorithm,” Prog. Electromagn. Res., vol. 116, pp. 65–79, 2011.
[21] D. Karaboga and C. Ozturk, “Neural networks training by artificial bee colony algorithm on pattern classification,” Neural Netw. World, vol. 19, no. 3, p. 279, 2009.
[22] E. Valian, S. Mohanna, and S. Tavakoli, “Improved Cuckoo Search Algorithm for Feed forward Neural Network Training,” Int. J. Artif. Intell. Appl., vol. 2, no. 3, pp. 36–43, Jul. 2011.
[23] C. Blum and K. Socha, “Training feed-forward neural networks with ant colony optimization: An application to pattern classification,” in Hybrid Intelligent Systems, 2005. HIS’05. Fifth International Conference on, 2005, p. 6–pp.
[24] M. Mavrovouniotis and S. Yang, “Evolving neural networks using ant colony optimization with pheromone trail limits,” in Computational Intelligence (UKCI), 2013 13th UK Workshop on, 2013, pp. 16–23.
[25] C. Zanchettin and T. B. Ludermir, “A methodology to train and improve artificial neural networks’ weights and connections,” in Neural Networks, 2006. IJCNN’06. International Joint Conference on, 2006, pp. 5267–5274.
[26] M. R. M. Rizk, H. H. A. Farag, and L. A. A. Said, “Neural Network Classification for Iris Recognition Using Both Particle Swarm Optimization and Gravitational Search Algorithm,” in 2016 World Symposium on Computer Applications & Research, 2016, pp. 12–17.
[27] R. Asgarnezhad, S. S. A. Majeed, Z. A. Abbas, and S. S. Salman, "An Effective Algorithm to Improve Recommender Systems using Evolutionary Computation Algorithms and Neural Network: Using Evolutionary Computation Algorithms and Neural Networks, an Effective Algorithm to Improve Recommender Systems," *Wasit Journal of Computer and Mathematics Science,* vol. 1, no. 1, pp. 27-35, 2022.
[28] R. I. Farhan, A. T. Maolood, and N. Hassan, "Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS," *Wasit Journal of Computer and Mathematics Science,* pp. 66-83, 2021.
[29] H. T. Salim, I. A. Aljazaery, J. S. Qateef, A. H. M. Alaidi, and R. a. M. Al_airaji, "Face Patterns Analysis and Recognition System Based on Quantum Neural Network QNN," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 8, 2022.
[30] Y. Zhang, P. Phillips, S. Wang, G. Ji, J. Yang, and J. Wu, “Fruit classification by biogeography-based optimization and feedforward neural network,” Expert Syst., vol. 33, no. 3, pp. 239–253, Jun. 2016.

Article submitted 28 November 2022. Published as resubmitted by the authors 21 December 2022.

Review paper of overlapping stenosis in artery

https://doi.org/10.31185/wjcm.93

Hawraa Dheyaa Asfoor (✉)
Department of Mathematics, college of Education of Pure Science, Wasit University, Iraq.
hawraadheyaa93@gmail.com

Abstract— Blood diseases are considered one of the most common diseases in the world for humans, which occurs as a result of abnormal growth on the artery wall, which leads to strokes and heart attacks, given that the artery is a tube. There are many types of narrowing of the arteries that can be described mathematically. In this research, we will explain again considering the overlapping stenosis of the artery and describing it mathematically.

Keywords— Artery, Stenosis, overlapping, growth.

1 Introduction

Stenosis is an arterial disease that results in narrowing of blood vessel due to collection of plaque on the wall of arteries. It reduces the flow of blood and the situation gets worse when this stenosis also produces a thrombus within the vessel, (i.e., a blood clot is formed inside the artery). In this scenario, the flow through such diseased arteries is improved by using a catheter. The blood flow problem for an artery having stenosed walls was explained by Ponalagusamy [1].

- **(1996)** Chakravarty and Mandal [2] stated that the presence of an overlapping stenosis in the artery is more critical than of a mild one. For this reason, researches have shown an increased interest to evaluate the effects of this kind of stenosis with different conditions and methods.
- **(2010)** Srivastava et al [3], studied the presence of red cells in an overlapping narrowed catheter artery by calculating the characteristics of blood flow. It was observed that the resistance increases with the increase in the size of the narrowing.
- **(2012)** Mekheimer and Kot [4], discussed blood flow between two eccentric tubes where the inner tube represents catheter while the outer tube was a tapered artery with stenosis. Blood flow was analyzed mathematically by using the perturbation method considering it as a Newtonian fluid for stenosis overlapping is artery.
- **(2016)** Jian et al[5], used the Mathematics program to calculate the results of the blood characteristics of a catheter artery with overlapping stenosis based on Newtoni-an blood with symmetric mild stenosis.
- **(2021)** . Bakheet, A., Alnussairy, E. A.[6] , studied the magnetic-mechanical effects of unstable blood flow on Casson's fluid through an artery mean of overlapping stenosis. The mathematical model of the problem was solved by using the pressure

correction method with Mac's algorithm to understand the phenomenon of blood flow in the diseased artery.

2 Mathematical Model

The schematic diagram for the overlapping stenosis under consideration is shown in Fig. 1. Following Chakravarty and Mandal [7], the geometry of the elastic (moving wall) arterial wall of the time variant overlapping stenosis for different taper angles is written mathematically as:

$$R(z,t) = \begin{cases} (mz + R_0) - \dfrac{\delta cos\phi}{l_0}(z-d)\left\{11 - \dfrac{94}{3l_0}(z-d) + \dfrac{32}{l_0^2}(z-d)^2 - \dfrac{32}{3l_0^3}(z-d)^3\right\} \\ \qquad \Omega(t), d \le z \le d + \dfrac{3l_0}{2} \\ = (mz + R_0)\Omega(t) \qquad otherwise \end{cases} \quad (1)$$

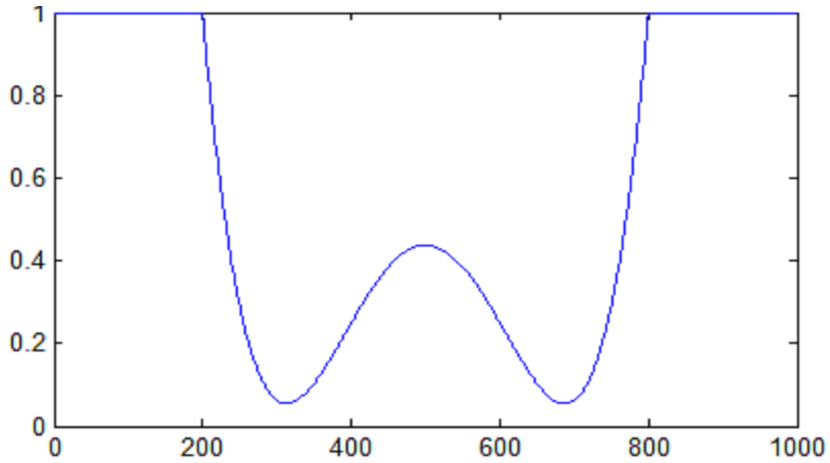


Fig. 1. Geometry of overlapping

Where $R(z,t)$ is the radius of the tapered arterial segment in the constricted region. R_0 Is the constant radius of the normal artery without stenosis, ϕ is the Angle of tapering, $3l_0/2$ is the engh of overlapping stenosis, d is the location of the stenosis $\delta cos\phi$ is the critical value of the overlapping stenosis $m = tan\phi$ is the slope of the tapered vessel, b is the constant ωis the represents the angular frequency of forced oscillation, t is the time.

3 Results and Discussion

The equation for overlapping stenosis was developed by MATLAB by taking different values tapered angle $\phi = -0.5,0,0.5$ and different values of stenosis height $\delta^* = 0.1,0.2,0.3$,radius of the normal artery without stenosis , $R_0 = 1$ and time $t = 0.5$, and location of the stenosis $d = 1.4$.

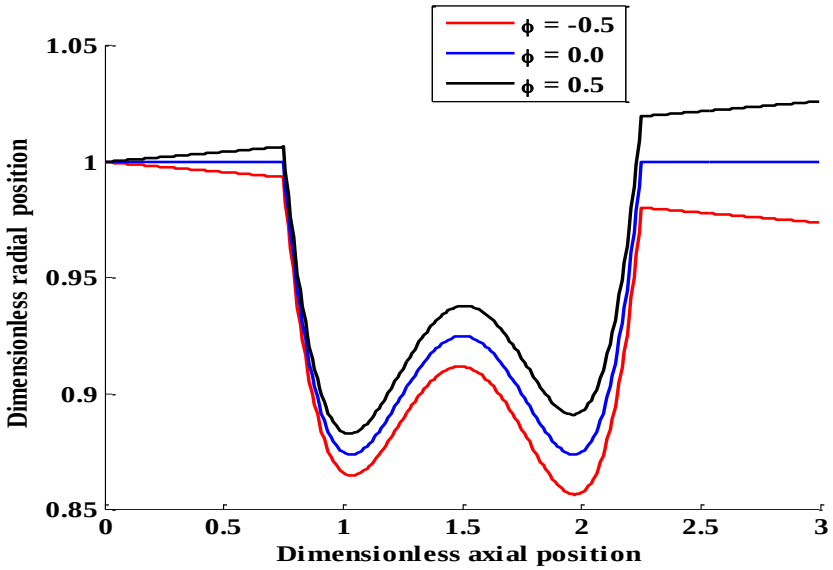


Fig. 2. Geometry of overlapping stenosed tapered artery for different angle of ϕ

We can show geometry of overlapping stenosed tapered artery for different tapered angle $\phi = -0.5,0,0.5$ the parameter $L = 3, R = 1, l_0 = 1, d = 1.4, \delta^* = 0.4, t = 0.5$.

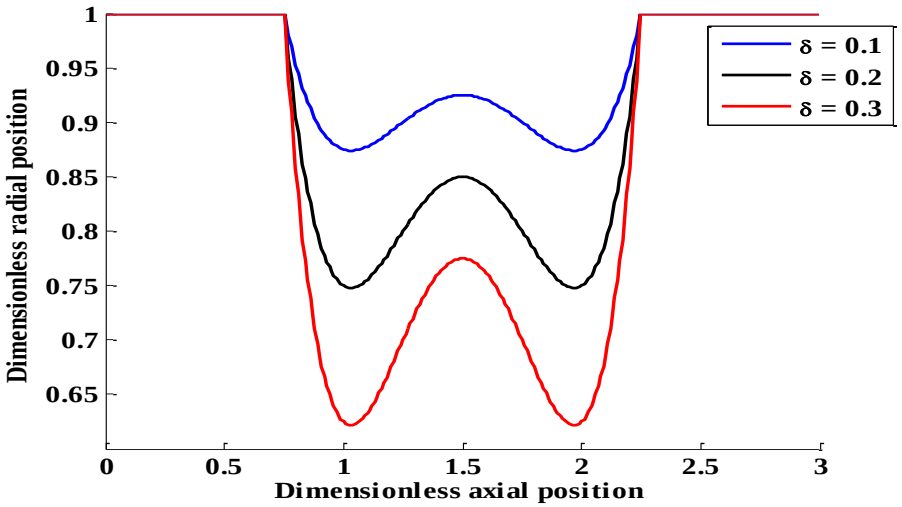


Fig. 3. Geometry of overlapping stenosed artery for different δ^* .

We can show geometry of overlapping stenosed tapered artery for different stenosis height δ^* the parameter $L = 3, R = 1, l_0 = 1, d = 1.4, t = 0.5, \phi = 0$ and $\delta^* =$ 0.1,0.2,0.3.

4 Conclusion

mathematical model to illustrate the stenosis of overlapping arteries.The results were obtained using the MATLAB code. Figure (2) shows different values of the tapered angle, taking the value of the highest height of the stenosis in the artery. As for Figure (3), different values are given for the height of the stenosis.

5 Reference

[1] Ponalagusamy, R. (1986). Blood flow through stenosed tube (Doctoral dissertation, Ph.D. Thesis). IIT Bombay, India.

[2] Chakravarty, S. and Mandal, P. K. 1996. A nonlinear two-dimensional model of blood flow in an overlapping arterial stenosis subjected to body acceleration, Mathematical and Computer Modelling, 24: 43–58.

[3] Srivastava, V. P., Vishnoi, R., & Sinha, P. (2010). Particulate suspension blood flow through a stenosed catheterized artery. Applications and Applied Mathematics: An International Journal (AAM), 5(2), 1.

[4] Mekheimer, K. S., & El Kot, M. A. (2012). Mathematical modeling of axial flow between two eccentric cylinders: Application on the injection of eccentric catheter through stenotic arteries. International Journal of Non-Linear Mechanics, 47(8), 927-937.

[5] Jian, T. C., & Amin, N. (2016, June). Analysis of blood flow through a catheterized stenosed artery using Mathematica. In AIP Conference Proceedings (Vol. 1750, No. 1, p. 030048). AIP Publishing LLC.

[6] Bakheet, A., Alnussairy, E. A. (2021). Numerical Simulation of Magnetohydro- dynamic Influence on Casson Blood Flow through Overlapping Stenosed Artery, Iraqi Journal of Science, 62(3),1410-1420.

[7] Chakravarty, S., & Mandal, P. K. (2000). Two-dimensional blood flow through tapered arteries under stenotic conditions. International Journal of Non-Linear Mechanics, 35(5), 779-793.

Article submitted 11 December2022. Published as resubmitted by the authors 25 December 2022.

On Degree Topology and Set-T_0 space

https://doi.org/10.31185/wjps.91

Zainab Naji Hameed(✉)
Faculty of Education for Girls, University of Kufa, Iraq
zainabn.alkraawy@student.uokufa.edu.iq

Hiyam Hassan Kadhem
Faculty of Education, University of Kufa, Iraq

Abstract— This work is aimed to introduce a new topology on a graph, namely the degree topology. This topology is defined by the degree of the vertices of the graphs. We find the degree topology for certain types of graphs and determine their types. The degree topology for the complete graph K_n is an indiscrete topology. While The degree topology is generated by a complete bipartite graph $K_{n,m}$ with $n \neq m$ is a quasi-discrete topology. In addition, a new property is initiated namely set-T_0 space and discussed the link between it and T_0 space. We verify that every degree topology is a set-T_0space.

Keywords— Degree- topological Space, Set-T_0 space

1 Introduction

The field of graph theory is broad and diverse. It is not merely a relational structure; among many other mathematical structures, it can also be seen as topological spaces and combinatorial objects. Graphs can be used to abstractly represent a wide range of notions, which makes them particularly beneficial in real-world applications [1].

Several topological spaces had been built from certain types of graphs. Ahlborn in 1964 established a unique topological space on a digraph $\mathbb{G}(\mathbb{V}, \mathbb{E})$ by any set $\mathbb{A}$ in $\mathbb{V}$ is openly provided there does not exist an edge from $\mathbb{V} - \mathbb{A}$ to $\mathbb{A}$[2]. In 2013, Hamza and Faisel constructed a topology on a finite undirected graph on a set of edges and also created a topology on subgraphs. In addition, they investigated the connectedness of these graphs based on the connectedness of their induces topologies of them. They introduced symmetric topological spaces for the isomorphic graphs [3].

Hassan and Abed [4] introduced a family of sub-basis for a topology to define a new independent topology on undirected graphs. In addition, Hassan and Jafar [5] presented a family of sub-basis that motivated a new topology including all vertices non-incident alongside the edge E (non-end vertices of the edge E) on the vertex set V of each simple graph G. Al'Dzhabri et al. initiated DG- topological space by DG −open set which is related alongside the digraph $G = (V, E)$ is designated by T_{DG}[6].

This work is aimed to introduce a new topology on a graph, namely the degree topology. This topology is defined by the degree of the vertices of the graphs. We find the degree topology for certain types of graphs and determine their types. The degree topology for the complete graph $K_n$is an indiscrete topology. While The degree topology is generated by a complete bipartite graph $K_{n,m}$ with $n \neq m$ is a quasi-discrete topology. In addition, a new property is initiated namely set-T_0 space and discussed the link between it and T_0 space.

2 Preliminaries

This section includes one of the central concepts which are needed in the rest sections.

2.1 Definition [7]

A graph $G = (V, E)$, where V is a set whose elements are called vertices, and E is a set of paired vertices, whose elements are called edges**.**

2.2 Definition [8]

Let X be a set and τ be a collection of subsets of X. If τ has the following properties:

- the empty set and X are both in τ
- Any (finite or infinite) union of sets in τ is itself in τ
- Any finite intersection of sets in τ is itself in τ

Then, τ is called a topology on X and the pair (X, τ) is called a topological space.

3 Degree-Topology

Throughout this section, a new topological space called the degree topology is introduced in the following definition:

3.1 Definition

Let $G(V, E)$ be a simple graph and K be the max degree of all vertices in G. Then, the topology that defines on vertex set $V$and generated by a basis B is called degree topology and it is denoted by T_{deg} where $B_{deg} = \{A_i : i = 0, \dots, K\}$, A_i is the set of all vertices that have a degree i, and K is the maximum degree of all vertices in G.

3.2 Example

Let $G(V,E)$ be a graph as in Figure 3.1 where $V=\{v_1,v_2,v_3,v_4,v_5\}$. Then, $A_0=\emptyset, A_1=\{v_5\}, A_2=\{v_1,v_3\}, A_3=\{v_2\}$, and $A_4=\{v_4\}$.So, the basis for T_{deg} is $B_{deg}=\{\emptyset,\{v_5\},\{v_1,v_3\},\{v_2\},\{v_4\}$.

Thus, $T_{deg}=\{\emptyset,V,\ \{v_5\},\{v_1,v_3\},\{v_2\},\{v_4\},\{v_5,v_1,v_3\},\{v_5,v_2\},\{v_5,v_4\},\{v_1,v_3,v_2\},\{v_1,v_3,v_4\},\{v_2,v_4\}\}$.

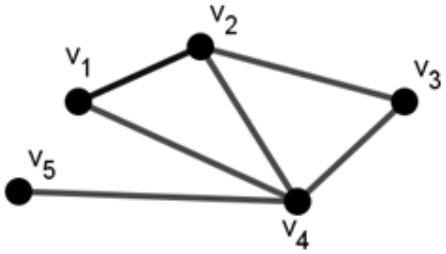


Figure 3.1

3.3 Example

Let $G(V,E)$be a graph as in Figure 3.2, where $V=\{v_1,v_2,v_3,v_4\}$. Then, $A_0=A_1=A_2=\emptyset$, and $A_3=V$.So, the basis for $T_{deg}$is $B_{deg}=\{\emptyset,V\}$. therefore, $T_{deg}=\{\emptyset,V\}$.

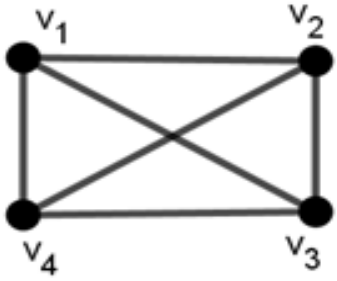


Figure 3.2

3.4 Theorem

The degree topology generated by a complete bipartite graph $K_{n,m}$ with $n=m$ is an indiscrete topology

Proof:

Assume that$K_{n,m}(V,E)$ is a complete bipartite graph with $n=m$=q. Suppose that the vertex set V partitioned into two disjoint subset V_1 and V_2 such that the number of vertices for V_1 and V_2 is $n$and m, respectively.

By definition of a complete bipartite graph, every vertex in $V_1$is adjacent to all vertices in V_2. Then, the degree of any vertex in $V_1$is$m$ and the degree of any vertex in $V_2$is n. Since $n = m = q$, so the degree of all vertices in $K_{n,m}$ is q. Thus, $A_0 = \emptyset$, and$A_q = V$, hence $B_{deg} = \{\emptyset, V\}$. Therefore, $T_{deg} = \{\emptyset, V\}$.■

3.5 Theorem

The degree topology generated by a complete bipartite graph $K_{n,m}$ with $n \neq m$ is a quasi-discrete topology.

Proof

Assume that $K_{n,m}(V, E)$ a complete bipartite graph with $n \neq m$ and the vertex set V. Let V be partitioned into two disjoint sets V_1 and V_2 and the number of vertices for V_1 and V_2 is $n$and m, respectively.

By definition of the complete bipartite graph, every vertex in $V_1$is adjacent to all vertices in V_2. Then the degree of any vertex in V_1 are m and the degree of any vertex in V_2 is n. Since $n \neq m$, we have $A_0 = \emptyset$,$A_m = V_1$ and$A_n = V_2$. So, the basis for T_{deg} is$\{\emptyset, V_1, V_2\}$ and by taking all unions of the degree topology generated by a complete bipartite graph is$\{\emptyset, V, V_1, V_2\}$. ■

3.6 Theorem

The degree topology generated by a complete graph K_n with n vertices is an indiscrete topology.

Proof

Assume that $K_n(V, E)$ is a complete graph with the vertex set $V = \{v_1, v_2, \dots, v_n\}$. By definition of the complete graph, any two vertices in K_n are adjacent, So, v_1 is adjacent with $v_2, v_3, \dots, v_n$ so that the degree of $v_1$is $n - 1$.

Similarly, v_2 is adjacent with $v_1, v_3, \dots, v_n$ so that the degree of v_1 is $n - 1$and so on. Then, the degree of any vertex in $K_n$has the degree $n - 1$, we have $A_0 = \emptyset$, and$A_{n-1} = V$. Thus the basis for T_{deg} is$\{\emptyset, V\}$and by taking all unions of the degree- the topology generated by the complete graph is$\{\emptyset, V\}$. ■

3.7 Theorem

The degree topology generated by the cycle graph C_n with n vertices is an indiscrete topology.

Proof:

Assume that $C_n(V,E)$ is a cycle graph with the vertex set $V=\{v_1,v_2,\dots,v_n\}$. By definition of the cycle graph, it is 2-regular. Then, any vertex in $C_n$has a degree 2, we have $A_0=\emptyset$, and $A_2=V$. Thus the basis for T_{deg} is $\{\emptyset,V\}$and by taking all unions the degree topology generated by the cycle graph is$\{\emptyset,V\}$. ■

3.8 Theorem

The degree topology generated by the path graph P_n with n vertices is $\{V,\emptyset,\{v_1,v_n\},\{v_2,v_3,v_{n-1}\}\}$, where v_1 is the first vertex and v_n is the last vertex.

Proof: Assume that $P_n(V,E)$ is a path graph with the vertex set $V=\{v_1,v_2,\dots,v_n\}$, where v_1 is the first vertex and v_n is the last vertex. By definition of the path graph, the first vertex and the last vertex have degree one while the others vertices have degree 2.

We have $A_0=\emptyset$, $A_1=\{v_1,v_n\}$ and$A_2=\{v_2,v_3,v_{n-1}\}$, so that the basis for T_{deg} is$\{\emptyset,\{v_1,v_n\},\{v_2,v_3,v_{n-1}\}\}$and by taking all unions the degree topology generated by the path graph is$\{V,\emptyset,\{v_1,v_n\},\{v_2,v_3,v_{n-1}\}\}$. ■

Next, another new concept is initiated, namely the set-T_0space.

4 Set-T_0 space

4.1 Definition

Let X be a non-empty set and τ be a topology on X, then τ is called set-T_0space which is denoted by $T_{0(s)}$ if there exist non-empty sets $M_1,M_2,M_3,\dots M_K\in\tau$ with $M_i\neq X$ for all $i=1,2,\dots,k$ and k be any natural number such that $\bigcap_{i=1}^{k}M_i=\emptyset$ and, $\bigcup_{i=1}^{k}M_i=X$.

4.2 Example

Let $K_{1,3}(V,E)$ be a simple graph with $V=\{v_1,v_2,v_3,v_4\}$, we have $T_{0(s)}=\{\emptyset,V,\{v_1\},\{v_2,v_3,v_4\}\}$.

Then $T_{0(s)}$ is a set-T_0 space due to existing non-empty open sets $\{v_1\}$ and $\{v_2,v_3,v_4\}$ such that $\{v_1\}\neq V,\{v_2,v_3,v_4\}\neq V,\{v_1\}\cap\{v_2,v_3,v_4\}=\emptyset$ and $\{v_1\}\cup\{v_2,v_3,v_4\}=X$.

4.3 Example

Let $X=\{y,w,z\}$and $\tau=\{\emptyset,X,\{y\},\{z\},\{y,z\}\}$ be a topology on X. Then τ is not a set-T_0space because there are no open subsets of X which satisfy the conditions of a set-T_0 space.

4.4 Remark

1. The set-T_0space is not necessarily satisfied T_0space as in Example 4.2 is a set-T_0space but it is not aT_0space for $v_2 \neq v_1$ with $v_2, v_1 \in V$ and there is no open set containing either $v_1$or v_2, but not both.
2. The T_0space is not necessarily satisfied the set-T_0space as in Example 4.3 which is not a set-T_0space but it is satisfied a T_0-space for $x_2 \neq x_1$ with $x_2, x_1 \in V$ then there exists an open set that contains $x_2$but not x_1 or contains $x_1$but not x_2.

4.5 Theorem

Every degree topology is a set-T_0space/

Proof:

Let $(X, T_{0(s)})$ be a degree- topological space. Since the degree of any vertex is unique. The definition of a degree topology then, the intersection of every non-empty open subset set-T_0 space of the basis for degree topology is empty.

Consequently, we have $\bigcup_{i=1}^{k} M_i = X$, where k is the natural number. Hence $(X, T_{0(s)})$ is a set-T_0 space. ■

5 References

[1] M. Shokry, Generating Topology on Graphs by Operations on Graphs, Applied Mathematical Sciences, vol. 9, no. 57, pp. 2843-2857, 2015.
[2] A. Aniyany and S. Naduvath, A study on graph topology, Communications in Combinatorics and Optimization (in press*)*,. pp. 1-13, 2022, DOI: 10.22049/CCO.2022.27399.1253.
[3] A.M. Hamza and S.N. Faisel, Construction a Topology on Graphs, Journal of Al-Qadisiyah for Computer Science and Mathematics, Vol. 5, no. 2, pp. 39-46, 2013.
[4] A. F. Hassan and Z. I. Abed, Independent (Non-Adjacent Vertices) Topological Spaces Associated with Undirected Graphs With Some Applications in Biomathematics, Journal of Physics: Conference Series, vol. 1591, pp. 1-11, 2020, doi:10.1088/1742-6596/1591/1/012096.
[5] A. F. Hassan and A. M. Jafar, Non- Incidence (Non-End Vertices) Topological Spaces Associated with Simple Graphs, PalArch's Journal of Archaeology of Egypt/Egyptology, vol. 17, no. 7, pp. 14336-14345, 2020.
[6] A K. S. Al'Dzhabri, A. M. Hamza, and Y.S. Eissa, On $\boldsymbol{DG}^{-}$ Topological operators Associated with Digraphs, Journal of Al-Qadisiyah for Computer Science and Mathematics, vol. 12, no. 1, pp. Math 60-71, 2020.
[7] S. Saha Ray, Graph theory with algorithms and its applications, Applied Science and Technology., 2013
[8] J. Sharma, General Topology, Krishan Prakashan Meerut UP, 1977.

Article submitted 29 November 2022. Published as resubmitted by the authors 25 December 2022.

On Hyperbolic Differential Equation with Periodic Control Initial Condition

Zainab Abdel Ameer
Al-Mustansiriya University, College of Education, Math Dep. Iraq.
zynbaldlal@gmail.com

Sameer Qasim Hasan
Al-Mustansiriya University, College of Education, Math Dep. Iraq.

Abstract. The aim of this paper to study the existence solution of some types of hyperbolic differential equation with periodicity of some controls function as nonlocal initial condition for the equation and the technical that are used with analytic depended on some interest iniquities, make advantage steps for proving with fixed point theorems to grantee of the solution.

Keyword. Periodic hyperbolic equation, control initial functions, periodic solution.

1. Introduction

In this section we assume the hyperbolic deferential with periodic control initial conditions, as follow:

$$\begin{cases} u_{tt} - div(\sigma\ (|\nabla u|^2)\ \nabla u^m) - (\nabla u)^p = |u|^{m-2} f(x,t,u)\ log|u|, \quad x \in \Omega, t > 0, & (1.1) \\ u(x,t) = 0, x \in \partial\Omega, \qquad t \in [0,1], & (1.2) \\ u(x,0) = u_0(x), u_t(x,0) = u_1(x)\ , x \in \Omega, & (1.3) \end{cases}$$

$u_0, u_1 \in L^2(\Omega)$, are periodic control functions, Ω is in a bounded domain $\mathbb{R}^n$ with $\partial\Omega$ as smooth bounded $Q_w = R \times (0,T]$, for $[0,1]$. The term $u^{m-2}\ log|u|$ is a logarithmic nonlinearity which can be applied to many branches [1], [2], [3]. Where $p > 0$ and $m \geq 1$.

Assume the following conditions:

a. $f(x,t,u)$ is Holder continuous in $\overline{\Omega} \times$ R $\times$ R, periodic in t with a period T and satisfied $f(x,t,u) \leq b_0|u|^{\alpha+1}$ with constant $b_0 \geq 0$ and $0 \leq \alpha \leq 1$.
b. $\sigma(\ |\nabla u|^2) = |\nabla u|^m$.
c. $div(\sigma\ (|\nabla u|^2)\ \nabla u^m)$ is the definition of rather slow.

There are many articles researched on some types of hyperbolic differential equations with some properties and important results such as in [4] the multipoint boundary value problems with nonlocal initial conditions for hyperbolic deferential problems with different approaches. Impulsive System with Periodic Problem for a hyperbolic equation in [5] has been studied extensively. The loaded third order equations as hyperbolic boundary value problems also with mixed types were presented in [6] and in [7] the optimal boundary control problems of the turnpike phenomenon corresponding to hyperbolic systems have been studied and computed. Finely in [8, 9, 10] Strict Lyapunov Function used to studied a boundary control of hyperbolic systems.

In this paper, the existence and unique solution of the hyperbolic problem with periodic functions as initial conditions (1.1) - (1.3), and shown that the solution is uniformly bounded, we establish the existence under some conditions are sufficiently conditions to satisfy Leray –Schauder fixed point theorem .

2. Main results

In this section the results of explain existence of solution for the hyperbolic deferential of problem with initial periodic control functions now, we need the following definition.

Definition (2.1): A function $v \in L^p(0,w;\, w_0^{1,p}(\Omega)) \cap C_w(\overline{Q}_w)$ is called to be a weak solution of the problem (1.1) - (1.3) if $\frac{\partial^2 v}{\partial t^2} \in L^2(Q_w)$ and v satisfies

$\iint_{Q_T} \left(\frac{\partial^2 v}{\partial t^2}\ \varphi + m\, v^{1-\frac{1}{m}}\, \sigma(|\nabla u|^2)\nabla v \nabla \varphi\ \right) + (m-1)v^{-\frac{1}{m}}\, \sigma(|\nabla u|^2)\ \varphi - (\nabla v)^p\ \varphi - |v|^{m-2} f(\alpha,t,v)\ log|v|\ \varphi dx\ dt\ ) = 0,$ for any $\varphi \in C^2(\overline{Q}_w)$ with $\varphi(x,0) = u_0(t), \varphi(x,0) = u_1(t)$

And $\varphi \log \Omega \times (0,\tau) = 0$

Theorem(2.1): Let u be solution of $u_{tt} - div(\sigma\ (|\nabla u|^2)\ \nabla u^m) - (\nabla u)^p = |u|^{m-2} f(x,t,u)\ log|u|$

$u(x,t) = 0, x \in \partial\Omega,\ t \in [0,1],\ u(x,0) = u_0(x), u_t(x,0) = u_1(x) \in \Omega,$ with $\sigma \in [0,1]$, then there exists positive constant R independent of σ such that $\|u(t)\|_2^2 < R$.

Proof:

$\frac{1}{(m+2)(m+3)}\ \frac{\partial^2 u\, u^{m+3}}{\partial t^2} = \frac{1}{m+2}\left[(m+2)u^{m+1}\left(\frac{\partial u}{\partial t}\right)^2 + u^{m+2}\ \frac{\partial^2 u}{\partial t^2}\right] = u^{m+1}\nabla u + \frac{u^{m+2}}{m+2}\ \frac{\partial^2 u}{\partial t^2}$

Thus

$$\frac{1}{m+3}\ \frac{\partial^2 u}{\partial t^2}\ u^{m+3} - (m+2)\ u^{m+1}\ \nabla u = u^{m+2}\ \frac{\partial^2 u}{\partial t^2}$$

$= \frac{1}{m+3}\ \frac{\partial^2 u}{\partial t^2}\ u^{m+2} - (m+2)\ u^{m+1}\ \nabla u$

Multiply Eq. (1.1) by u^{m+2} , we get

$$\frac{1}{m+2}\ \frac{\partial^2 u}{\partial t^2}\ u^{m+2} - (m+2)\ u^{m+1}\nabla u - div(\sigma\ (|\nabla u|^2\ )\nabla u^m) - \nabla u^m\ u^{m+2}$$

$= |u|^{m-2} f(x,t,u)\ log|u|\ u^{m+2}$

Multiply Eq. (1.1) by $|u(t)|^p\ u(t),\ p > 0$, and integrating, we get

$\int_\Omega \frac{1}{m+2}\ \frac{\partial^2 u}{\partial t^2}\ u^{m+2}\ |u(t)|^p - \int_\Omega (m+2)\ u^{m+2}\ \nabla u\ |u(t)|^p + \int_\Omega \{(p+1)\ \sigma(\ |\nabla u|^2\ )|u(t)|^p\ \nabla u^m\ \nabla u - |u(t)|^p \nabla u^m\ u^{m+3}\}$

$= \int_\Omega\ |u|^{m-2} f(x,t,u)|u(t)|^p\ u(t)\ log|u|\ u^{m+2}$

$\int_\Omega \frac{1}{m+3}\ \frac{\partial^2 u}{\partial t^2}\ u^{m+3}\ |u(t)|^p - \int_\Omega\ (m+2)\ u^{m+2}\ \nabla u\ |u(t)|^p +$

$\int_\Omega \{(p+1)\ \sigma(\ |\nabla u|^2\ )|u(t)|^p\ \nabla u^m\ \nabla u - |u(t)|^p\ (\nabla u)^p\ u^{m+3}\}$

$= \int_\Omega\ |u|^{m+2} f(x,t,u)\ |u(t)|^{p+1}\ u^{m+2}\ log|u|$

$= \frac{1}{m+2}\ \frac{\partial^2 u}{\partial t^2}\ \int_\Omega \left|u^{\frac{m+3}{p}} u(t)\right|^p - \int_\Omega\ (m+2)\ \frac{1}{\frac{m+3+p}{p}}\ \left|\nabla\left(u^{\frac{m+3}{p}}\ u(t)\right)^p\right|$

$+ \int_\Omega (p+1)\ \sigma\ (\ |\nabla u|^2\ )\ m\, u^{m-1}|\nabla u|^2 - \left|u\ (t)\ u^{\frac{m+3}{p}}\ \nabla u\right|^p$

$$= \int_\Omega \left| u^{\frac{m+2}{p+1}}\, u(t)\, u^{\frac{m+2}{p+1}} \right| f(x,t,u)\, log|u| \tag{1.4}$$

$$\frac{1}{m+1}\frac{\partial^2}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|^p - \frac{p(m+2)}{m+3+p}\left| \nabla\left(u^{\frac{m+3+p}{p}} \right)^p \right|$$

$$+(p+1)\int_\Omega \left\{ m\,\sigma(|\nabla u|^2)\left| u^{\frac{m-1}{2}}\nabla u \right|^2 - \left| u^{\frac{m+3+p}{p}}\nabla u \right|^p \right\}$$

$$= \int_\Omega \left| u^{\frac{2m+5+p}{p+1}} \right|^{p+1} f(x,t,u)\, log|u|$$

$$\frac{1}{m+1}\frac{\partial^2}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|_p^p - \frac{p(m+2)}{m+3+p}\left| \nabla\left(u^{\frac{m+3+p}{p}} \right)^p \right|$$

$$+(p+1)m\,\sigma(|\nabla u|^2)\frac{2}{m+1}\left\| \nabla u^{\frac{m+1}{2}} \right\|_2^2 - \left\| \frac{p}{m+3+2p}\nabla u^{\frac{m+3+p}{p}}\nabla u \right\|_p^p$$

$$= \left\| u^{\frac{2m+5+p}{p+1}} \right\|_{p+1}^{p+1} f(x,t,u)\, log|u|$$

$$\frac{1}{m+1}\frac{\partial^2}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|_p^p - \frac{p(m+2)}{m+3+p}\left\| \nabla\left(u^{\frac{m+3+p}{p}} \right)^p \right\|_p^p$$

$$+(p+1)\frac{2}{2m+1}\left\| \nabla u^{\frac{2m+1}{2}} \right\|_2^2 - \left\| \frac{p}{m+3+2p}\nabla u^{\frac{m+3+2p}{p}} \right\|_p^p$$

$$= \left\| u^{\frac{2m+5+p}{p+1}} \right\|_{p+1}^{p+1} f(x,t,u)\, log|u|$$

Thus,

$$\frac{1}{m+1}\frac{\partial^2}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|_p^p - \frac{p(m+2)}{m+3+p}\left\| \nabla u^{\frac{2m+1}{2}} \right\|_p^p + (p+1)$$

$$\left(\frac{2m}{2m+1}\left\| \nabla u^{\frac{2m+1}{2}} \right\|_2^2 - \left\| \frac{p}{m+3+2p}\nabla u^{\frac{m+3+2p}{p}} \right\|_p^p \right)$$

$$= \left\| u^{\frac{2m+5+p}{p+1}} \right\|_{p+1}^{p+1} f(x,t,u)\, log|u| \tag{1.5}$$

Thus,

$$\frac{1}{m+1}\frac{\partial^2 u}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|_p^p - \frac{p(m+2)}{m+3+p}\left\| \nabla\left(u^{\frac{m+3+p}{p}} \right)^p \right\|_p^p +$$

$$+(p+1)\left(\frac{2m}{2m+1}\left\| \nabla u^{\frac{2m+1}{2}} \right\|_2^2 - \left\| \frac{p}{m+3+2p}\nabla u^{\frac{m+3+2p}{p}} \right\|_p^p \right)$$

$$\leq \left\| u^{\frac{2m+3+p}{p+1}} \right\|_{p+1}^{p+1} b_0\,|u|^{\alpha+1}\log|u|$$

Therefore,

$$\frac{1}{m+1}\frac{\partial^2 u}{\partial t^2}\left\| u^{\frac{m+3+p}{p}} \right\|_p^p - \frac{p(m+2)}{m+3+p}\left\| \nabla\left(u^{\frac{m+3+p}{p}} \right) \right\|_p^p + (p+1)$$

$$\left(\frac{2m}{2m+1}\left\|\nabla u^{\frac{2m+1}{2}}\right\|_2^2-\left\|\frac{p}{m+3+2p}\nabla u^{\frac{m+3+2p}{p}}\right\|_p^p\right)$$

$$\leq b_0\left\|u^{\frac{2m+6+p+\alpha}{p+1}}\right\|_{p+1}^{p+1}\log|u|$$

Suppose that

$\left\|\nabla u^{\frac{2m+1}{2}}\right\|_2^2<\frac{p(m+2)}{m+3+p}\left\|\nabla(u^{\frac{m+3+p}{p}})\right\|_p^p+\frac{(p+1)p}{m+3+2p}\left\|\nabla u^{\frac{m+3+p}{p}}\right\|_p^p$, and

Set $m=p$, we get that,

$$\frac{1}{p+1}\frac{\partial^2}{\partial t^2}\left\|u^{\frac{p+3+p}{p}}\right\|_p^p+(p+1)\frac{2p}{2p+1}\left\|\nabla u^{\frac{2p+1}{2}}\right\|_2^2$$

$$=\left\|\nabla u^{\frac{2p+1}{2}}\right\|_2^2\leq b_0\left\|u^{\frac{2p+6+p+\alpha}{p+1}}\right\|_{p+1}^{p+1}log|u|$$

$$\frac{1}{(p+1)}\frac{\partial^2}{\partial t^2}\left\|u^{\frac{2p+3}{4p}}\right\|_p^p+\frac{2(p+1)p}{2p+1}\left\|\nabla u^{\frac{2p+1}{2}}\right\|_2^2-\left\|\nabla u^{\frac{2p+1}{2}}\right\|_2^2$$

$$\leq b_0\left\|u^{\frac{3p+6+\alpha}{p+1}}\right\|_{p+1}^{p+1}log|u|$$

Thus,

$$\frac{1}{(p+1)}\frac{\partial^2 u}{\partial t^2}\left\|u^{\frac{2p+3}{p}}\right\|_p^p+\left(\frac{2(p+1)p}{2p+1}-1\right)\left\|\nabla u^{\frac{2p+1}{2}}\right\|_2^2\leq b_0\left\|u^{\frac{3p+6+\alpha}{p+1}}\right\|_{p+1}^{p+1}\log|u| \quad (1.6)$$

Let $u_k=\frac{2p+1}{u^2}$ and $0<\alpha\leq 1$, we have

$$\frac{1}{(p_k+1)}\frac{\partial^2}{\partial t^2}\|u\|_p^{\frac{2p_k+3}{p_k}}+\left(\frac{2(p_k+1)p_k}{2p_k+1}-1\right)\|\nabla u_k\|_2^2$$

$$\leq b_0\|u_k\|_{p_k+1}^{\frac{3p+7}{p+1}}\ log|u_k|\ \frac{1}{p_k+1}\frac{\partial}{\partial t^2}\|u_k\|_2^2+\left(\frac{2(p_k+1)p_k}{2p_k+1}-1\right)$$

$$\|\nabla u_k\|_2^2\leq b_0\|u_k\|_2^{2^{\frac{(3p+7)}{p+1}}}\ log|u_k|\frac{\partial}{\partial t^2}\|u_k\|_2^2+\left(\frac{2(p_k+1)^2p_k-p_k+1}{2p_k+1}\right)$$

$$\|\nabla u_k\|_2^2\leq b_0(b_k+1)\|u_k\|_2^2\ \frac{(3p_k+7)}{p_k+1}\ log|u| \quad (1.7)$$

$$\frac{\partial}{\partial t^2}\|u_k\|_2^2\leq\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\|\nabla u_k\|_2^2+b_0(b_k+1)\|u_k\|_2^{\frac{2(3p_k+7)}{p_k+1}}\ log|u_k|$$

By the Gagliardo-Nirenbery inequality, we have that

$\|u_k(t)\|_2^2\leq C\|\nabla u_k(t)\|_2^\theta\|u_k)(t)\|_1^{1-\theta}$, where $\theta=\frac{N}{N+2}\in(0,1)$ (1.8)

Noting that $\|u_k(t)\|_1=\|u_{k-1}(t)\|_2^2$

$$\frac{\partial^2}{\partial t^2}\|u_k(t)\|_2^2\leq\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\|\nabla u_k(t)\|_2^{\frac{2}{\theta}}$$

$$\|u_k(t)\|_1^{\frac{2(\theta-1)}{\theta}}+b_0(b_k+1)\|u_k(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}}\ log|u_k| \quad (1.9)$$

Set $\lambda_k=\max\{1,sup_\epsilon\ \|u_k(t)\|_2^2\}$, then

$$\frac{\partial^2}{\partial t^2}\|u_k(t)\|_2^2\leq\|u_k(t)\|_2^2$$

$$\left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\,\|u_k(t)\|_2^{\frac{2}{\theta}-\frac{2(3p_k+7)}{p_k+1}}\,\lambda_{k-1}^{\frac{4(\theta-1)}{\theta}}+b_0(b_k+1)\,log|u_k|\right\} \quad (1.10)$$

$$\frac{\partial^2}{\partial t^2}\,\|u_k(t)\|_2^2 \le \|u_k(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}}$$

$$\left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\,\|u_k(t)\|_2^{\frac{2}{\theta}-\frac{2(3p_k+7)}{p_k+1}}\,\lambda_{k-1}^{\frac{4(\theta-1)}{\theta}}+b_0(b_k+1)\,log|u|\right\}$$

$$p_{k+1}\,\frac{\partial^2}{\partial t^2}\,\|u_k(t)\|_2^{\frac{2}{p_{k+1}}} \le \left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\,\|u_k(t)\|_2^{\frac{2}{\theta}-\frac{2(3p_k+7)}{p_k+1}}\,\lambda_{k-1}^{\frac{4(\theta-1)}{\theta}}$$

$$+b_0(b_k+1)\,log|u_k| \quad (1.11)$$

Since $u_1(t), u_2(t)$ are periodic control functions.

$$\|u_k(t)\|_2 \le \left\{C\left[b_0(b_k+1)\,log|u_k|+\left(\frac{1-2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\;\ell_{k-1}^{b_k}\right]\lambda_{k-1}^{\frac{4(1-\theta)}{\theta}}\right\}^{\frac{1}{C_k}}$$

Where $C_k=\frac{2}{\theta}-\frac{2(p_k+1)}{p_k+2}=\frac{2\ell_k}{p_k+2}$

Since $\lambda_{k-1}\ge 1,\ k=1,2$, we get

$$\|u_k(t)\|_2 \le \left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\;\lambda_{k-1}^{b_k+4\frac{(1-\theta)}{\theta}}\right\}^{\frac{1}{C_k}}$$

$$=\left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\;\right\}^{\frac{p_k+2}{2\ell_k}}\;\lambda_{k-1}^{\frac{4(1-\theta)(p_k+2)}{2(\ell_k-1)\theta}}$$

$$\|u_k(t)\|_2 \le \left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\;\right\}^{ka'}\;\lambda_{k-1}^2$$

Where a' is a positive constant independent of k, and $A=2^{a'}$

$$\ln\|u(t)\|_2 \le \ln \ell_k \le \ln\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)+k\ln A+2\ln\ell_k-1$$

Where $A=2^{a'}>1$, then

$$\ln\|u(t)\|_2 \le \ln \ell_k \le \ln\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)$$

$$\sum_{i=1}^{k-2}2^1+2^{k-1}\ln \mathrm{I}_1+\ln A\left(\sum_{j=0}^{k-2}(k-j)2^j\right)$$

$$\le (2^{k-1}-1)\ln\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)+2^{k-1}\ln\lambda_1+f(k)\ln A\text{ , with}$$

$f(k)=2^{k+1}-2^{k-1}-k-2$

That is

$$\|u(t)\|_{p_k+2} \le \left\{\left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\,\lambda_1^{2^{k-1}}\;A^{f(k)}\right\}^{\frac{2}{p_k+2}}$$

Letting $k\to\infty$, we get

$$\|u(t)\|_\infty \le \left(1-\frac{2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)\lambda_1^2 \le \left(\frac{1-2(p_k+1)p_k}{2p_k+1}\right)(p_k+1)(\max\{1, sup_t\|u(t)\|_2\})^2 \quad (1.12)$$

From (1.7)

$$\frac{\partial}{\partial t^2}\,\|u(t)\|_2^2+\left(\frac{2(p_k+1)^2p_k}{2p_k+1}-p_k+1\right)$$

$\|\nabla u(t)\|_2^2 \le b_0(b_k+1)\|u(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}} \quad log|u_k|$

According to the Poincare's inequality, we have

$C_p\|u(t)\|_2^2 \le \|\nabla u\|_2^2$, for sufficiently small $|\Omega|$, we have that

$\frac{\partial^2}{\partial t^2}\|u(t)\|_2^2 + \left(\frac{2(p_k+1)^2 p_k}{2p_k+1} - p_k + 1\right) C_p \|u(t)\|^2 \le b_0(b_k + 1)\|u(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}} \quad log|u|$

Let $\frac{2(p_k+1)\,p_k}{2p_k+1} < 1$, then

$\frac{\partial^2}{\partial t^2}\|u(t)\|_2^2 \le \left(\frac{-2(p_k+1)p_k}{2p_k+1} + p_k + 1\right)\|u(t)\|_2^2 + b_0(b_k+1)\|u(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}} \quad log|u_k|$

$\frac{\partial^2\|u(t)\|_2^2}{\partial t^2} + (p_k + 1 - \frac{2(p_k+1)^2 p_k}{2p_k+1}\|u(t)\|_2^2 \le b_0(b_k+1)\|u(t)\|_2^{\frac{2(3p_k+7)}{p_k+1}} \quad log|u_k|$

$p_k = 0$. To estimate $\|u(t)\|_2^2$ as follows

$\frac{\partial^2\|u(t)\|_2^2}{\partial t^2} + \|u(t)\|_2^2 \le b_0(b_k+1)\|u(t)\|_2^{14} \quad log|u_k|$

By young inequality, we obtain

$\frac{\partial^2\|u(t)\|_2^2}{\partial t^2} + \|u(t)\|_2^2 \le C$

Where C is a constant independent of u. By u_0, u_1 are periodic control function, we get $\|u(t)\|_2^2 \le R$, where R is a positive constant.

Theorem (2.2): If (a),(b) and (c) hold, then the problem (1.1)-(1.3) admits at least one periodic solution u

Proof First, we define a map by considering the following problem:

$u_{tt} - div(\sigma\,(|\nabla u|^2)\ \nabla u^m) - (\nabla u)^p = |u|^{m-2} f(x,t,u)\ log|u|, \quad x \in \Omega, t > 0,$

$u(x,t) = 0, x \in \partial\Omega, \qquad t \in [0,1],$

$u(x,0) = u_0(x), u_t(x,0) = u_1(x)\ , x \in \Omega,$

Where $f(x,t,u)$ is a given function in$C_T(\overline{Q}_T)$. If follows from a standard argument similar to [11] that the problem (1.1)-(1.3) admits a unique solution. So, we define a map $T: C_T(\overline{Q}_T) \to C_T(\overline{Q}_T)$. By $u = Tf$ is compact and continuous. In fact, by the method in [15], we can infer that $\|u\|_{L^\infty(Q_T)}$ is bounded if $f \in L^\infty(Q_T)$ and $u, \nabla u \in C^\infty(\overline{Q}_T)$. For some $\alpha > 0$. Then (by the Arzela-Ascoli theorem) the compactness of the map T comes from $\|u\|_{L^\infty(Q_T)}$ and Holder continuity of u. The continuity of the map T comes from the Holder continuity of ∇u.

3. Conclusion:

In conclusion, this paper aimed to study the existence of solutions for certain types of hyperbolic differential equations with periodicity of certain control functions as nonlocal initial conditions. The techniques used in this study were based on analytic dependencies and made use of fixed point theorems to ensure the existence of solutions. This work represents a significant advancement in the field of hyperbolic differential equations and the application of nonlocal initial conditions.

4. References:

[1] Buljan h, Šiber A, Soljačić M, Schwartz T, Segev M, Christodoulides DN. Incoherent white light solitons in logarithmically saturable noninstantaneous nonlinear media. *Phys Rev E*. 2003;68(3):036607.

[2] De Martino S, Falanga M, Godano C, Lauro G. Logarithmic Schrödinger-like equation as a model for magmatransport. *Europhys Lett*. 2003;63(3):472-475.

[3] Królikowski W, Edmundson D, Bang O. Unified model for partially coherent solitons in logarithmically non- linear media. Phys Rev E. 2000;61(3):3122-3126.

[4] Ashyralyev A. and Yildirim O., On Multipoint Nonlocal Boundary Value Problems For Hyperbolic Deferential and Difference, equation, Taiwanese Journal of Mathematics Vol. 14, No.1, pp. 165-194,February 2010.

[5] Assanova A. T. and Kadirbayeva Z. M., Periodic Problem For An Impulsive System Of The Loaded Hyperbolic Equations, Electronic Journal of Differential Equations, Vol. 2018 (2018), No.72, pp. 1–8.

[6] Baltayeva U.I and B.I. Islomov, Boundary Value Problems For The Loaded Third Order Equations of the Hyperbolic and Mixed Types, Ufa Mathematical Journal. Volume 3. 3(2011). Pp. 15-25.

[7] Gugat M., Hante F. M., On The Turnpike Phenomenon For Optimal Boundary Control Problems with Hyperbolic Systems, arXiv:1806.04438v3 [math.AP] 7 Nov 2018.

[8] Littman. W., Boundary Control Theory For Hyperbolic and Parabolic Partial Differential Equations With Constant Coefficients. Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 5, no 3 (1978), p. 567-580.

[9] Michel Coron. J, d'Andréa-Novel B., and Bastin G, A Strict Lyapunov Function for Boundary, Control of Hyperbolic Systems of Cnservation Laws, IEEE Transactions on Automatic control, Vol 52, No. 1, January 2007.

[10] Sano H. and Nakagiri Akagiri S., Backstepping Boundary Control of First-order Coupled Hyperbolic Partial Integro-differential Equations, Recent Advances in Applie Mathematics, 2009

[11] ZQ W., JN Z., Jx Y. and Hl L., Nonlinear Diffusion Equation World Scientific, Singapore (2001).

[12] Dg G., Nonlinear Functional Analysis. Shandong Science and Technology Press, Jinan (2001).

[13] Ladyzenskaja O., Solonnikov V. and Uraltseva N., Linear and Quasilinear Equations Parabolic Type Translations of Mathematics Monographs, Vol 23 Am. Math. Soc. Providence (1968).

[14] Hameed R. A., Wu B., and Sun J. Periodic Solution of a Quasilinear Parabolic Equation with Nonlocal terms and Neumann Boundary conditions, Boundary value problems, 2013: 34.

[15] Li S. and Hui X. Periodic Solution of a quasilinear Parabolic Equation with Nonlinear Convection terms. Advances in Difference Equations, 2012:206.

Article submitted 25 December 2022. Published as resubmitted by the authors 30 December 2022.

رقم الإيداع في دار الكتب والوثائق العراقية 2499
في 2021

Print-ISSN : 2788-5887
Online-ISSN: 2788-5879

Wasit Journal
OF COMPUTER AND MATHEMATICS

A Quarterly Academic Refereed Journal
Issued by Computer Sciences and Information Technology College