WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM
e-ISSN: 2788-5879 p-ISSN: 2788-5887

Cloud-Based Service for Fingerprint Image Matching

Ethar Abdul Wahhab Hachim [1]*

[1] Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, IRAQ

*Corresponding Author: Ethar Abdul Wahhab Hachim

DOI: https://doi.org/10.31185/wjcms.290
Received 21 Augest 2024; Accepted 25 September 2024; Available online 30 September 2024

ABSTRACT: Fingerprint matching is one of the most important services that related to the issue of identifying individuals, as it can be used to verify the validity of contracts, documents or in other security fields such as criminal investigations. Fingerprints are also one of the most common and accurate forms, as they are easy to obtain, it also has a unique features and cannot be identical to any individuals. The proposed service exploits the advantages provided by cloud computing, such as ease of use, availability of the service anytime and anywhere, and no need to own expensive devices with high specifications, in addition to being low cost. In this service, all fingerprint image preprocessing operations and images enhancement, in addition to the matching, verification and decision-making process are done with the help of tools which provided by cloud computing environment. While the client's role in this service is limited to feeding the system with the fingerprint to be matched. The experimental results proved that this service has achieved high accuracy in matching fingerprint images, in addition to greatly facilitating the matching process for the user, and it can be used anytime and anywhere thanks to the cloud environment facilities adopted by this service.

Keywords: Cloud environment, Fingerprint, Matching services, SVM

1. INTRODUCTION

Reliance on the cloud computing has grown-up exponentially due to and numerous services and applications that become driven and hosted over and done with the internet, because of increased number of users and growth the size of the databases that they need to use and deal with[1].

Cloud computing provides the facility for using services such as software, infrastructure or platform depending on the client requirements. It aids to decrease the overall cost by avoiding the installation of a high capacity servers more than clients need [2].

According to The National Institute of Stands and Technology(NIST), cloud computing can be defined as " model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources such as services, applications, servers, networks and storage that can be rapidly provisioned and released with minimal management effort or service provider interaction"[3]. Cloud computing has five fundamental service attributes, three service delivery methods, and four deployment strategies. Broad access to the network, measurable service, fast elasticity, resource pooling and on demand self service are crucial traits.

Software as a Service (SaaS) that deals directly with the end users while Platform as a Service (PaaS) facilitates business and projects for developers and Infrastructure as a Service (IaaS) considered the best choice for IT administers. The deployment methods are private cloud, public cloud, hybrid cloud, and community cloud through which the subscription method can be determined according to the needs of the clients or organizations [4]. Fig.1 depicts the four cloud deployment models, three cloud service models and five essential services attributes of cloud computing [5].

*Corresponding author: *ethar201124@uomustansiriyah.edu.iq*

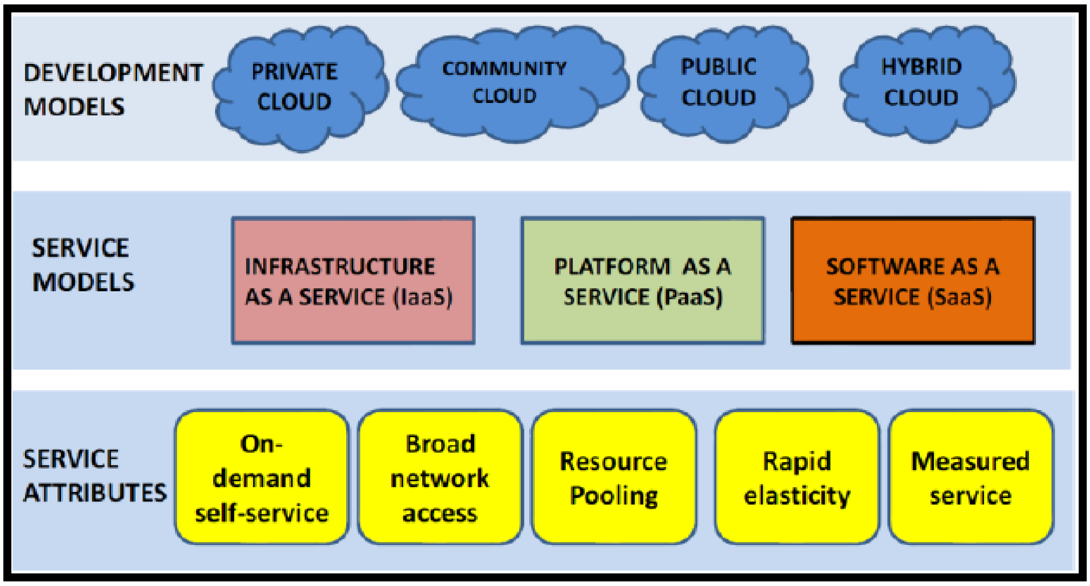

FIGURE 1. - Classical vision for the cloud computing

Fingerprint matching in cloud computing environment provides a great combination between the biometric accuracy and the cloud benefits to provide a scalable and secure easy to get identity authorization solution [6]. Like any other template matching, the fundamental structure of a fingerprint matching system can be summarizing in Fig. 2.

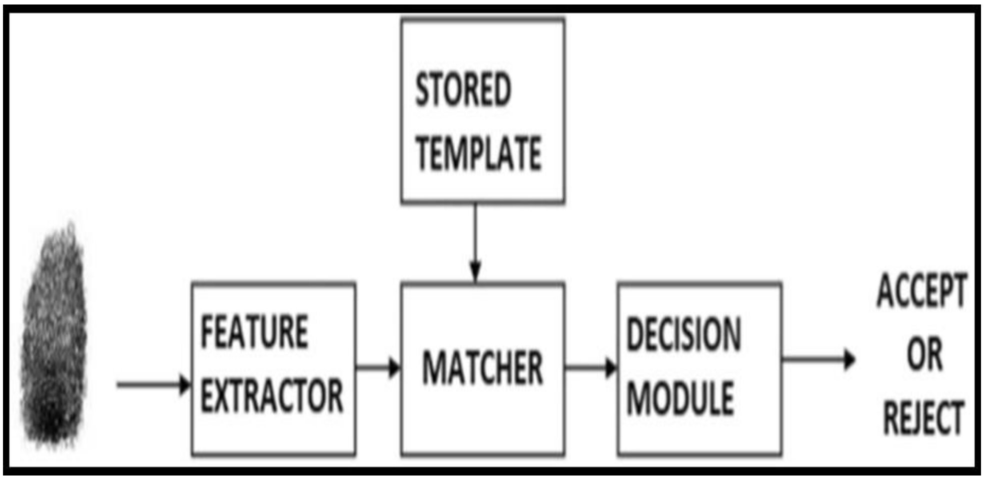

FIGURE 2. - Fingerprint matching general system [7].

As can be seen from figure 2, fingerprint matching system must go through several basic stagesafter obtaining the fingerprint image. These stages including carrying out initial preprocessing operations to enhancement the image, then get the basic deterministic features template. Finally making the decision is done based on the results of the comparison process. This paper was organized as the following parts: In the next section, related studies about biometric authentication via cloud environment are discussed. Section 3 presents the materials and methods that used to achieve this service while section 4 views the experimental results and outcomes. The final section concludes the proposed serves performance.

2. LITERATURE REVIEW

In 2018, Ehsan Nadjaran Toosi, et al., offer a method for matching the fingerprint by using “Aneka” , which consider as a platform used to develop the scalable several applications on cloud environment. They suggest constructing and implementing their method by employ a secure big data to search and find the matched fingerprint, then find all information attached to it. Through their method, they were able to reduce the time for matching information and obtain results with a good accuracy [8].

S Rajarajan, et al., designed in 2019 a system to accomplish a fingerprint matching in cloud computing server. In their system, the users register the fingerprint and the unique- key is created and then save in cloud server for the verification process. When the client wants to enter the eHealth systems, he registers his fingerprint so that the features extracted from it and matched with that previously stored in the cloud server. The results of their system showed speed of implementation and acceptable false-rejection rates [9].

In 2021, H O Lasisi, et al., implemented a procedure that helps the lecturers or teachers to register the attendance depending on cloud environment instead of traditional methods by using ESP32 microcontroller with development board. This procedure used the fingerprint for authenticate the attendance, by comparing them with previously stored fingerprints to be accessed remotely via the cloud. Their procedure is characterized by the ease of obtaining users attendance, which leads to adherence the schedule of appointments and classroom activities [10].

Meennapa Rukhiran, et al., developed in 2023 a flexible- biometric system based on IOT technology for educational purposes. Their system used multimodal biometric including the fingerprint to verify the identity of students applying for university exams. The experimental results of the system showed a high quality when verifying the identity of the examinees [11].

3. MATERIALS AND METHODS

3.1 FINGERPRINT ANALYSIS

There are many factors or feature that has made fingerprints highly acceptable and widely popular, especially in identity verification processes. Uniqueness is one of these features which mean that the fingerprint is unique for every person; even the identical twins not have the similar fingerprint. Fingerprints stay constant through the person's life and not change over time and all humans have fingerprints which makes it universal method to identify individuals [12]. Fingerprints hold complex and fine details which could be a clearly distinguished, such as branches, endpoints and pattern, so it is actual challenging to forge the fingerprint and use it illegitimately compared with the other biometric measurements [13].

Recent techniques have made it easy to get or store fingerprints then use them in numerous applications also fingerprints provide an effective fast way to identify the individuals online[14].

Advanced fingerprint exploration systems are considered high level of accuracy for verifying the identity. As a result of these features, fingerprints are broadly used in various fields for instance security, biometric systems and law enforcement [15].

Any fingerprint consisting of numerous components or elements which identify the individuals and make them a unique for everyone. As shown in Fig.3, these elements include:

- Ridge Endings: Are the points where the lines in any fingerprint end.
- Bifurcations: Are the points where the lines branch to the form "Y" shape.
- Deltas: Are the points where the lines construct a small triangle, located close to the origin.
- Core Points: is the central points in every fingerprint around the lines revolve.
- Ridge Patterns: including the basic patterns such as loops, whorls and arches.

These components used by fingerprint verification systems to compare and investigate the fingerprints for correctly identify the individuals [16].

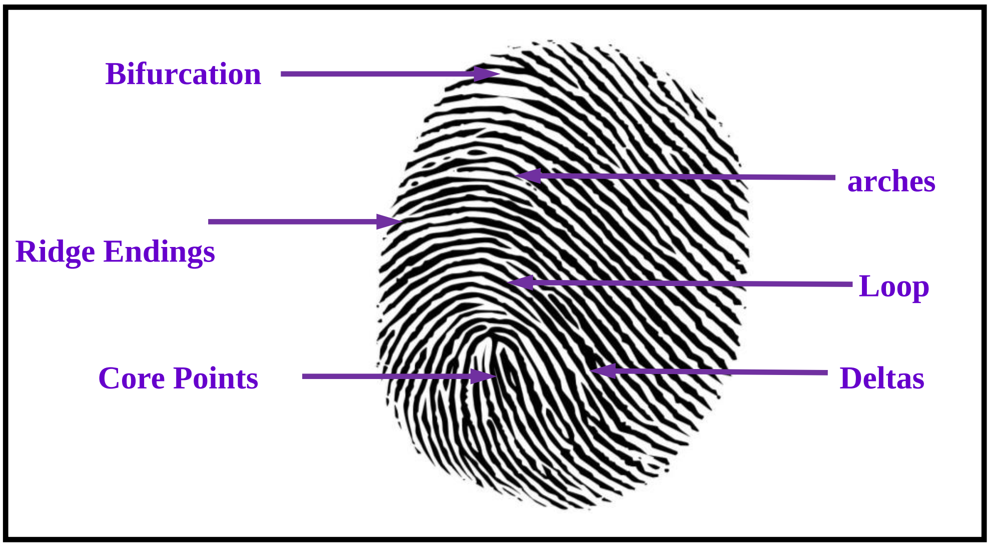

FIGURE 3. - Components of Fingerprint.

3.2 FINGERPRINT IMAGE PROCESSING

Image preprocessing consider as a procedures to manipulate the raw images data to a meaningful and usable format. It helps to remove undesirable noise and improve the specific merits necessary for different algorithms or computer vision uses [17]. Fingerprint image preprocessing is an essential starting step for preparing fingerprint images before sending them to the rest of the system parts. In Cloud Service for Fingerprint image Matching there are a number of procedures that used for fingerprint image preprocessing such as:

- **Grayscaling conversion:** is done by converting the RGB color images to grayscale which aid to simplify the images data and decrease computational requirements that needed for this service. Grayscaling fingerprint images offerings images where every pixel is the shade of the gray (the range of 0-256) also is responsible for smoother conversion from white to black [18]. There are three strategies for grayscaling conversion; namely average, luminosity and lightness methods. The lightness method that used in this work reduces the contrast between the averages of the most prominent colors and the least prominent colors, which reduces the effect of color distortion and avoid loss the color information. The formula is as follows:

$$GI = (\max(R, G, B) + \min(R, G, B)) / 2 \qquad (1)$$

- **Median filter:** noise removing consider as one of the most important procedures for image processing. key objective for these procedures is to obtain a clear and pure data from the images. Filtering is employed to enhanced and improve the images and to decrease the undesirable effect such as artifacts, inconspicuous lines, unrealistic edges, obscured objects, corners and some background scenes[19]. Median filter is one of the nonlinear filters that used in this work, which is developed to remove the salt and pepper noise and retains clearer edges from the fingerprint images and preserves the useful details in the fingerprint image [20]. The central pixels with size (3 × 3) neighborhood was replace by median value for the correspond window in gray level image, so all the values of noise pixels will be different from median value as showed in the following equation:

$$f(x, y) = \text{median}\,\{g(x, y)\} \qquad (2)$$

- **Hough Transform:** can be consider as mapping function that converts a points in the image space to a curves or lines in Hough Space. Then, the selected groups of the pixels that share a common properties like being on a similar line or crossing a set of lines can be detected and identified using properties of Hough Space that offer the necessary information for drawing these curves[21]. The pixel in image at point (x,y) can be represented by all possible lines pass through it by a curve at the point (r, θ) in Hough Space using the following equation:

$$r = x \cos\theta + y \sin\theta \qquad (3)$$

- **Quadtrees decomposition:** are tree data structures which created by recurring partitioning the two-dimension space into four sub-regions of the same size to store the information for every region in the node of this tree. In image processing it can be consider as an analysis procedure to speed up the edge detection by subdivide the fingerprint image to a structure blocks which are more homogeneous than the fingerprint image itself [22]. After fingerprint image is divided in to four equal square blocks, each block is tested to verify whether the pixels within this block belong to the same dynamic range. If the block is (homogeneous), it will not be divided again. Otherwise, the process of dividing and testing blocks continues until each block meets a specified criterion [23]. Fig.4 (a, b) shows the process of repeatedly dividing the original image (R) to reach the final quadtree.

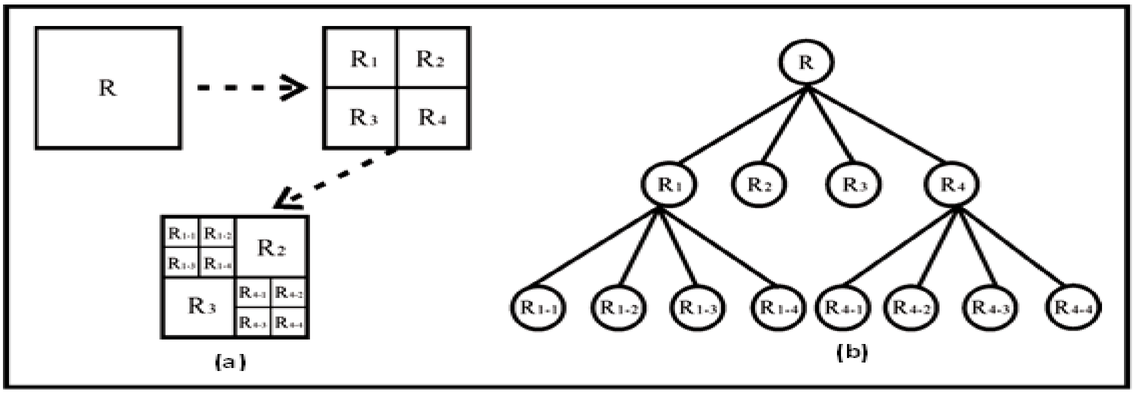

FIGURE 4. - (a) The original image (R) divided into several blocks using Quadtrees decomposition technique; (b) Final result represented by quadtree shape with leaf nodes [24].

3.3 THE PROPOSED SERVICE

The proposed Cloud Service For Fingerprint image Matching aims to offer a secure, efficient and easy to use service for matching fingerprint images in official transactions and documents. Depending on the facilities that provided by the cloud, all fingerprint image processing, feature extraction, classification and matching process are done within the cloud, while the service user's role is limited to entering the fingerprint image that needs to be matched. The starting step for the client to upload the fingerprint image to the system that available as a cloud service. After that, the service converts this image to gray level to speed up the processing process.

Then the gray image passes through a median filter to remove noise and thus obtain more accurate results. After enhancing the image and removing the noise, Hough transform identifies the points that form the extended edges in the image. Edges detection consider as an essential step for this service to support the identification of objects (fingerprint) boundaries and thus, it is easy to extract the discriminating features.

Then Quadtrees decomposition technique discloses the important information about the features of fingerprint image. Moreover it is very useful step to feed a classifier with more abstract features to achieve more accuracy in the classification process. Fig.5 explains the details of the proposed service.

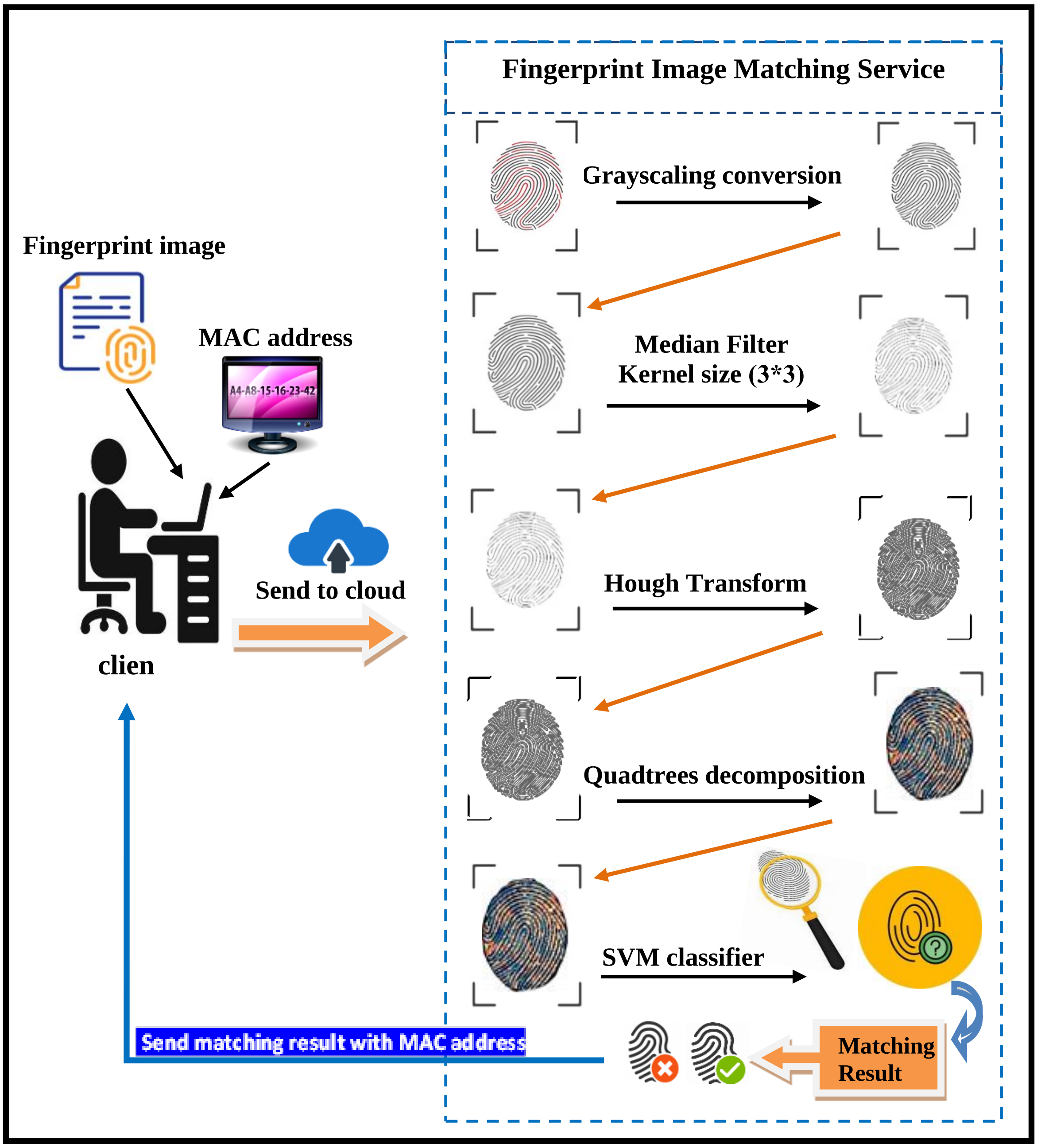

FIGURE 5. – Steps of the proposed service.

We can notice from Figure 5 that the client's role in this service is limited by sending fingerprint image that needs to be matched, in addition sending the MAC address to achieve more integration when receiving the result of the matching process. This information is sent to the service that is available via the cloud for the purpose of starting the matching processes.

As a first step, the service converts the fingerprint image to the gray level in order to reduce the number of channels of the image and thus speed up the processing, which is one of the priorities of this service. The median filter plays an important role in enhancing the image and removing noise from it.

It is considered a preemptive step to the process of edges detection in the image, which is considered a complement to the process of extracting features from it. The quadtree technique performs a quad-repetitive division of the image for the purpose of representing regions and distinguish between neighboring pixels and boundaries, thus obtaining more features.

After detect the edges and extract the distinctive features from fingerprint image, it must be classified to determine whether the fingerprint matched or not. The extracted features can be consider as the input to Support Vector Machine (SVM) classifier algorithm rather than a raw data fingerprint images to increase the discriminative power of the model and reduce computational expenses.

In registration phase for this service the extracted features for all fingerprint images divided as training set and testing set to be used later for SVM supervised classifier. To build SVM model, the hyperparameters must de define and tune before training it using the training set which accounts 80% of the total data while the remaining percentage represents the test set. The predictions and accuracy are assigned and calculated after testing the model on the test set. All steps of this service can be summarized by the following algorithm:

Fingerprint Image Matching Service Algorithm
Input: fingerprint image, MAC address.
Output: matching result

Begin
Step 1: Get fingerprint image with MAC address in the same file.
Step 2: send the file to the service on the cloud.
Step 3: Separate fingerprint image and perform preprocessing operations as follows:
Step 3.1: convert image to gray scale level using Grayscaling conversion
Step 3.2: Remove noise using Median filter
Step 3.3: Edge detection using Hough Transform
Step 3.4: Feature extraction using Quadtrees decomposition
Step 4: Repeat step 3 for all fingerprint images to extract features dataset.
Step 5: Split features dataset into training set (80%) and test set (20%)
Step 6: Define and tune the hyperparameters to build SVM model and training it using the training set.
Step 7: Test the model using testing set and solving the optimization problem to find the optimal hyperparameters.
Step 8: Send the final matching result with MAC address to the client.
End.

4. EXPERIMENTAL RESULTS

The accuracy of the matching results for the fingerprint image can be verified by using different metrics that are integrated together to obtain the final accuracy of the proposed service. To show a performance of SVM classifier, confusion matrix table has been used to describe the false positives (FP), false negatives (FN), true positives (TP) and true negatives (TN) where the predicted classes are compared with the actual classes for the testing set.

The actual classes are represented in the rows of confusion matrix while predicted classes are represented in the columns of this matrix. As shown in figure 6 (a, b), the confusion matrix outcomes can be given in training set as FP=27, FN=17, TP= 1117 and TN= 279 and in tasting set as FP=9, FN=6, TP=210 and TN=144 and in for 1800 fingerprint image dataset from FVC2006 database.

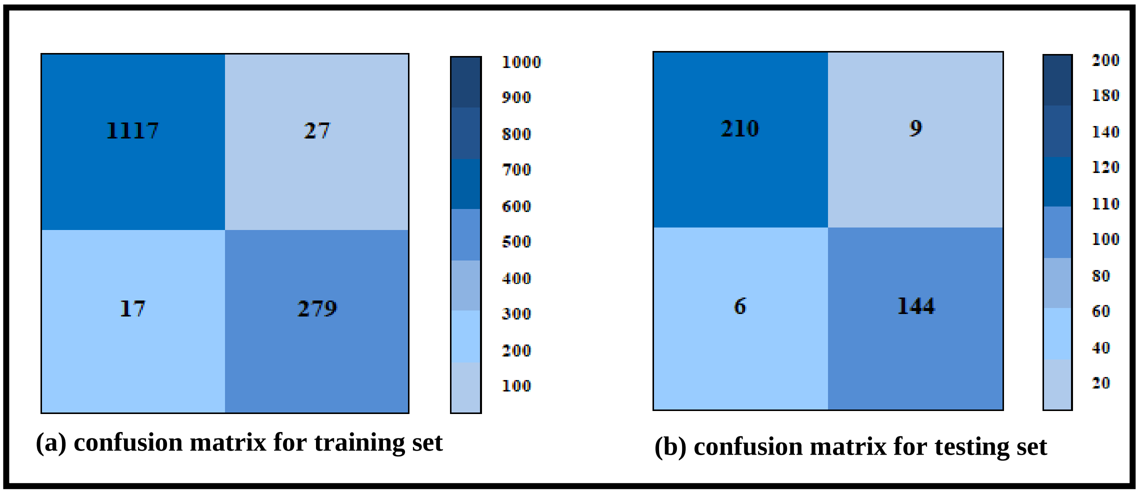

FIGURE 6. - (a) confusion matrix outcomes for training dataset; (b) confusion matrix outcomes for testing dataset

As noted in figure 6, The quality of service performance can be measured through the outcomes of confusion matrix which has high TP and TN rates, while low FP and FN rates. Confusion matrix can be used to calculate the True Positive Rate or (TPR) which consider as a proportion of the actual matching fingerprint images that are correctly identified in the service can be calculate from the following equation:

$$\text{TPR} = \frac{TP}{TP+FN} \qquad (4)$$

It can also be calculate a proportion of not matching fingerprint images that are incorrectly identified as matches for the service which called False Positive Rate or (FPR) by the following equation:

$$\text{FPR} = \frac{FP}{FP+TN} \qquad (5)$$

While accuracy of the classifier can be calculate from the following equation:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \qquad (6)$$

Therefore the SVM classifier accuracy for training set is 0.969, while the result for testing set has an accuracy of 0.959. General accuracy of the proposed services reached to 0.964.

Table 1 can provide a summary of the results that were achieved by testing this service on the data set, as follows:

Table 1. - Accuracy results of the proposed service

	TPR	FPR	Accuracy
Training set	0.985	0.088	0.969
Testing set	0.972	0.058	0.959

As it noted from table 1, the high value of true positive rate indicates that the classifier is identify the most of the positive examples correctly while the law value of false positive rate indicates that the service is working perfectly, and this has been proven by the results of the service's accuracy.

5. CONCLUSION

The proposed service embodies an attractive progression in the biometric verification technology via the cloud environment. The proposed service provides an efficient and trustworthy way to address the requirements of numerous applications and industries, from the law administration to the consumer computer electronics. As security concerns and the need for reliable identification continue to grow, this cloud service offers a robust solution for fingerprint matching and verification. Accuracy score evaluates the ratio for correctly matching fingerprint images out of all the images by using deferent metrics such as confusion matrix, TPR, FPR and Accuracy. The experimental results showed that there were high rates of fingerprint image matching while reducing the rate of false matches, which means that the proposed service works with high efficiency and accuracy.

Funding

None

ACKNOWLEDGEMENT

Thanks for Department of Computer Science, College of science, Mustansiriyah University, Baghdad –Iraq.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] A. A. Talabi et al., "Cloud-Based Approaches to Multi-Modal Biometric-Based Authentication in Identity Management Systems," Int. J. Intell. Comput. Res., vol. 13, no. 1, 2022, doi: 10.20533/ijicr.2042.4655.2022.0139.
[2] S. Juman TP, "Advantages and Security Challenges of Cloud Computing– Overview," Int. J. Comput. Sci. Mobile Comput., vol. 9, no. 12, pp. 76-85, Dec. 2020.
[3] M. P. Nath, "Cloud Computing: An Overview, Benefits, Issues & Research Challenges," Int. J. Res. Sci. Innov., vol. 6, no. 2, Feb. 2019.
[4] M. H. Qabazard, "Cloud Computing the New Age of Computing," Int. J. Res. Eng. Sci., vol. 8, no. 12, pp. 1-9, 2020.
[5] S. J. Abdallah and G. K. Ouda, "Using Integrated Library Management Systems for the Improvement of Information Services Based on Cloud Computing," Tikrit J. Pure Sci., vol. 25, no. 4, 2020.
[6] A. A. Talabi, "Cloud-Based Approaches to Multi-Modal Biometric-Based Authentication in Identity Management Systems," Int. J. Intell. Comput. Res., vol. 13, no. 1, 2022, doi: 10.20533/ijicr.2042.4655.2022.0139.
[7] A. Sarkar and B. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," Multimedia Tools Appl., vol. 79, 2020, doi: 10.1007/s11042-020-09197-7.
[8] E. N. Toosi, "Integrated IoT and Cloud Environment for Fingerprint Recognition," arXiv:1807.08099v1, 2018.
[9] S. Rajarajan, "Privacy Preserving Fingerprint Authentication at the Cloud Server for eHealth Services," EAI Endorsed Trans. Pervasive Health Technol., 2019, doi: 10.4108/eai.13-7-2018.162688.
[10] H. O. Lasisi et al., "Implementation of Cloud-Based Biometric Attendance System for Educators in a Developing Country," J. Phys. Conf. Ser., vol. 2034, 2021, doi: 10.1088/1742-6596/2034/1/012018.
[11] M. Rukhiran et al., "IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach," IEEE Access, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3253024.
[12] S. E. M. Elshafie et al., "Types of Fingerprints Characteristics and their Association with Gender and Blood Groups in Sudan," Int. J. Med. Sci., vol. 9, 2022, doi: 10.15342/ijms.2022.613.
[13] Y. Yu et al., "A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications," Micromachines, vol. 14, 2023, doi: 10.3390/mi14061253.
[14] V. Kirvel, "Fingerprint Analysis (AFIS) and Biometric System of Identification by Fingerprints: Issue of Artificial Papillary Pictures," Soc. Innov., no. 3, 2020.
[15] B. Arslan and S. Sagiroglu, "Fingerprint Forensics in Crime Scene: A Computer Science Approach," Int. J. Inf. Secur. Sci., vol. 8, no. 4, pp. 88-113, 2019.
[16] M. O. Ezegbogu and P. I. O. Omede, "The admissibility of fingerprint evidence: An African perspective," Can. Soc. Forensic Sci. J., vol. 56, no. 1, pp. 23-41, 2023, doi: 10.1080/00085030.2022.2068404.
[17] A. Calantropio et al., "Image Pre-Processing Strategies for Enhancing Photogrammetric 3D Reconstruction of Underwater Shipwreck Datasets," Int. Arch. Photogramm. Remote Sens. Spatial Inf. Sci., vol. XLIII-B2-2020, 2020.
[18] P. Kaler, "Study of Grayscale Image in Image Processing," Int. J. Recent Innov. Trends Comput. Commun., vol. 4, no. 11, Nov. 2016.
[19] B. Kanchanadevi and P. R. Tamilselvi, "Preprocessing Using Image Filtering Method and Techniques for Medical Image Compression Techniques," ICTACT J. Image Video Process., vol. 10, no. 3, Feb. 2020.
[20] S. S. Mohanty and S. Tripathy, "Application of Different Filtering Techniques in Digital Image Processing," J. Phys. Conf. Ser., vol. 2062, 2021, doi: 10.1088/1742-6596/2062/1/012007.
[21] S. Rahman et al., "Analysis and Comparison of Hough Transform Algorithms and Feature Detection to Find Available Parking Spaces," J. Phys. Conf. Ser., vol. 1566, 2020, doi: 10.1088/1742-6596/1566/1/012092.

[22] M. D. Braun, "The Usage of Quadtree in Deep Neural Networks to Represent Data for Navigation From a Monocular Camera," thesis, Université Bourgogne Franche-Comté, 2022. [Online]. Available: https://theses.hal.science/tel-04121867.
[23] L. Akrour et al., "Fast Hyperspectral Image Encoder Based on Supervised Multimodal Scheme," Int. J. Image Graph., vol. 21, no. 1, 2021, doi: 10.1142/S0219467821500078.
[24] D. Jiang et al., "Three-Dimensional Magnetic Inversion Based on an Adaptive Quadtree Data Compression," Appl. Sci., vol. 10, 2020, doi: 10.3390/app10217636.