WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

An Improved Method for Hiding Text in Image Using Header Image

Nada Abdul Aziz Mustafa[1]*

[1]University of Baghdad / College of language, Iraq

*Corresponding Author: Nada Abdul Aziz Mustafa

DOI: https://doi.org/10.31185/wjcm.79
Received: September 2022; Accepted: November 2022; Available online: December 2022

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, stegoanalysis, 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.

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

*Corresponding author: nada@colang.uobaghdad.edu.iq

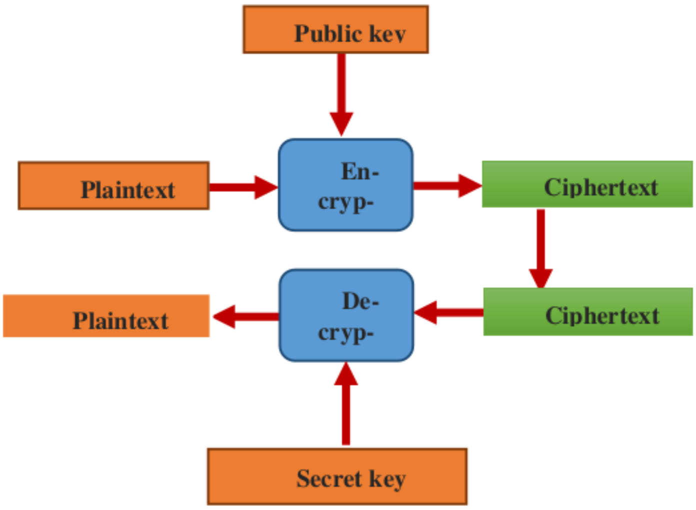


FIGURE 1. **The general idea of cryptography.**

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.

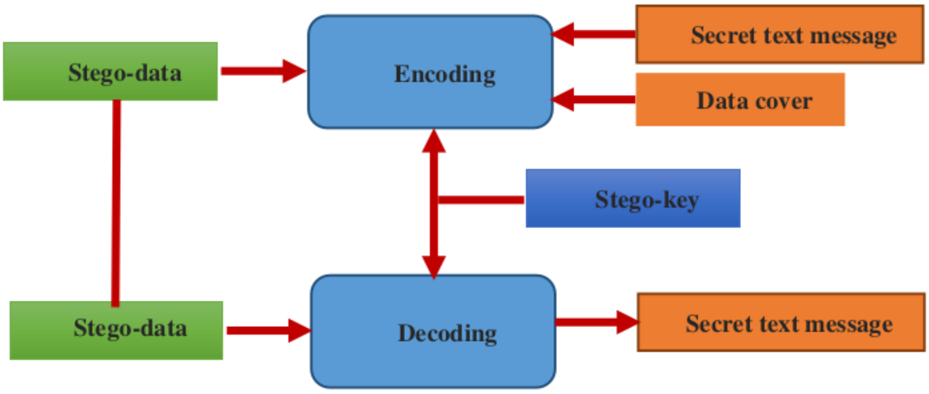


FIGURE 2. **The general idea of secret key steganography.**

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.

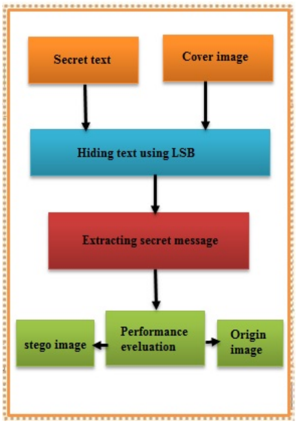


FIGURE 3. **The framework of proposed systematic approach.**

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.

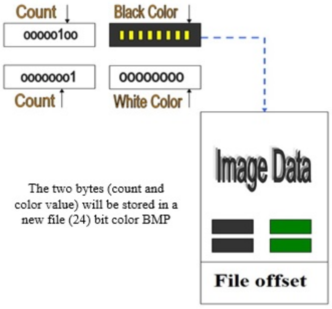

Count
Black Color
00000100
00000001
00000000
Count
White Color
Image Data
The two bytes (count and color value) will be stored in a new file (24) bit color BMP
File offset

FIGURE 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.

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.

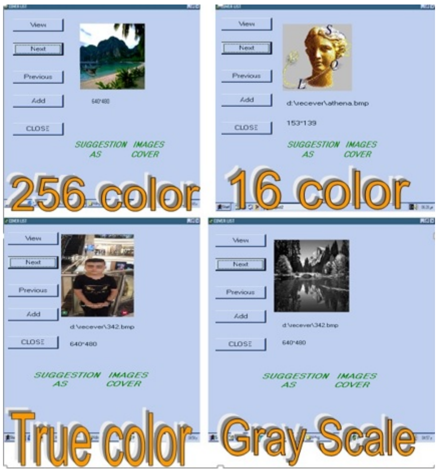


FIGURE 5. **Database images of colored image or gray scale image.**

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

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.

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

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.

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.

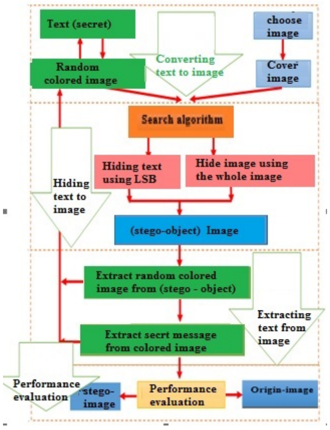
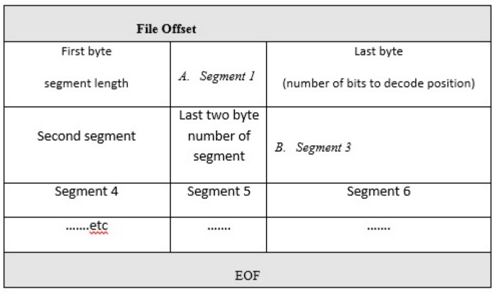


FIGURE 6. **Hiding the Secret Text Message in Cover Image**



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.

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:

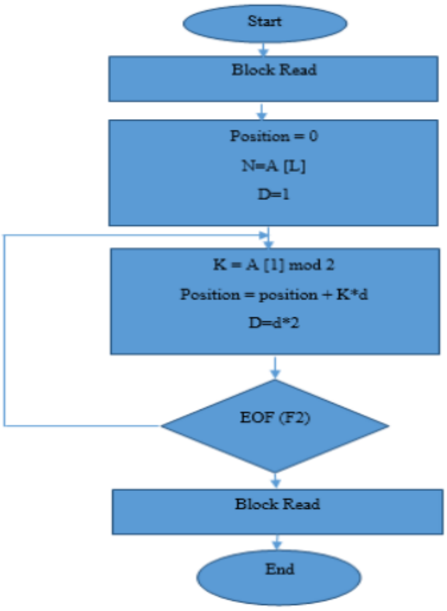


FIGURE 7. **Flow chart of extracting text from image.**

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:

$$v(g) = \sqrt{\sum_{g=0}^{L-1} \left(g - \dot{\bar{g}}\right) p(g)} \tag{3}$$

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:

$$Entropy = -\sum_{g=0}^{L-1} p\,(g) * logp(g) \tag{4}$$

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:

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

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:

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

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:

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

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:

$$p\,(g) = N(g)/m \tag{8}$$

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], as shown in Equation 9 as follows:

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

where:

I (r,c) = The original image.

Î(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.

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.

Table 1. **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		

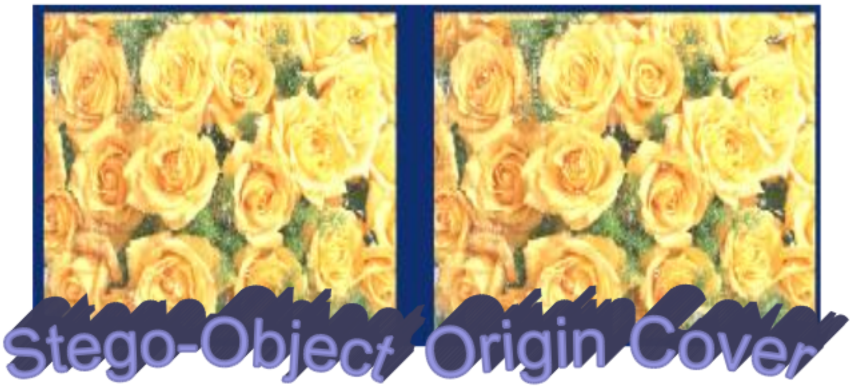


FIGURE 8. **The comparison between the origin cover with the stego-object.**

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.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

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*, vol. 8, pp. 2088–8708, 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,” *Computer and Information Security Handbook*, pp. 843–856, 2017.

[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,” *Advances in Computers*, vol. 83, pp. 51–107, 2011.

[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,” *International Conference on Recent Advances and Innovations in Engineering*, pp. 1–5, 2014.

[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, pp. 5218–5218, 2019.

[12] R. Din, M. Mahmuddin, and A. J. Qasim, “Review on steganography methods in multi-media 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,” *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pp. 511–516, 2011.

[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, pp. 175–175, 2020.

[18] A. Behura, “Congruence of deep learning in biomedical engineering: Future prospects and challenges,” *Handbook of Deep Learning in Biomedical Engineering*, pp. 1–24, 2021.

[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,” *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 749–755, 2014.

[21] R. Ibrahim and T. S. Kuan, “Steganography algorithm to hide secret message inside an image,” 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, pp. 45–45, 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, K. Bigham, and 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, pp. 3550–3550, 2020.

[26] N. K. E. Abbadi, “Cover Optimization for Image in Image Steganography,” *International Journal of Computer Science Issues (IJCSI)*, vol. 10, pp. 556–556, 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,” *Applications of Digital Image Processing XLII*, pp. 111371–111371, 2019.

[29] E. Noroozi, S. B. M. Daud, and A. Sabouhi, “Critical Evaluation on Steganography Metrics,” *Advanced Materials Research*, pp. 927–931, 2013.