Robust Method for Embedding an Image Inside Cover Image Based on Least Significant Bit Steganography

Sahera A. S. Almola[1], Najat H. Qasim[2] and Hamid Ali Abed Alasadi[2, 3, *]
E-mail: sahera.sead@uobasrah.edu.iq, najat.qasim@uobasrah.edu.iq, hamid.abed@uobasrah.edu.iq
[1]Department of information system, College of Computer sciences and Information Technology, University of Basrah, Iraq
[2]Department of computer Science, College of Education for Pure Sciences, University of Basrah, Iraq
[3]Communications Engineering Department, Iraq University College, Istqlal Street, Basra, 61004, Iraq

Keywords: Steganography; Cryptography; Image; Security; Hiding; LSB; MSB; Stego.

Received: August 27, 2022

According to the enormous evolution of the internet and communications, the security of private or sensitive information has become the important issue. The private information can be passed between a sender and a receiver with high security using Cryptography and Steganography. By the cryptography, as the information can be secured with the cipher key for encryption. By the Steganography, the secret information can hide within usual data such as images, videos, audios. In this paper we proposed the robust method that includes two phases. The first phase consists of two stages. In the first stage we encrypt a secret image using encryption algorithm in order of increasing security of information. In the second stage, we complete the first stage for embedding the most significant bits (MSB) of the encrypted image into the least significant bits (LSB) of the cover image for instituting the stego image. The second phase is the obverse of the first phase, where, the encrypted image is retrieved from the stego image and then, decrypted process construct the secret image. The proposed method is efficient in terms of security compare with the other methods. Where, both encryption and embedding algorithms have an efficient role for embedding the secret image and preserving the good visual quality of stego images. Furthermore, extraction algorithms obtained better and faster results to a restoration of the secret image.

Povzetek: Predstavljena je metoda skrivanja slike znotraj slike - steganografija.

1 Introduction

At present, the internet offers a lot of advantages, as people can easily send or receive confidential information in various forms to or from almost any remote place in the world. So, data security and privacy are internet problems, information security is required to transmit confidential data. Therefore, how to achieve secure communication is an important area of research. There are many techniques that are used in the process of hiding information, depending on the type carrier file. The secret file that we want to hide it can be any type of file types (image, audio, text, etc.). Encryption and steganography are used to secure the privacy of information. Encryption, is a technique of mixing information in order that prohibited people cannot retrieve it, while steganography areas conceal exists of information, in addition to protect confidential information from unlawful access. So, the most feature of steganography is that it conceals the real presence of secret information, making it an improbable target for the spy. A high level of security can be achieved by the collection between encryption and steganography. In this paper, an encryption algorithm is used to encrypt a secret image. Then, new least significant bits' algorithm introduced to embed the most significant bits (MSB) of the encrypted image in the least significant bits (LSB) of cover image pixels. That ensures a very high security technique for secret data transmission.

The rest of this research arranges as the following: Section 2 reviews the principles of the image cryptography. Section 3 reviews the principles of the image steganography. Section 4 describes the proposed method. Section 5, provides the experimental results and analyzes the results of the proposed method based on some parameters. Section 6 discusses the conclusions. Finally, future work presents in section 7.

2 Image cryptography

The cryptography is the science used to secure the privacy of information that stored on the media or transmitted over a web of the internet. According to the wide applications of images, image security becomes an important issue in security authorities and political affairs. Encryption is a technique to protect the particularity of images; therefore, many encryption algorithms have been advanced to achieve best image security.

In cipher systems, cryptography algorithms are classified for two types based on the cipher key: symmetric and asymmetric key algorithms. Where, symmetric cipher algorithms use the identical cipher key for encryption and decryption processes. In the suggested algorithm we will use the symmetric key to encrypt and decrypt a secret image. Figure1, illustrate the structure of image security.

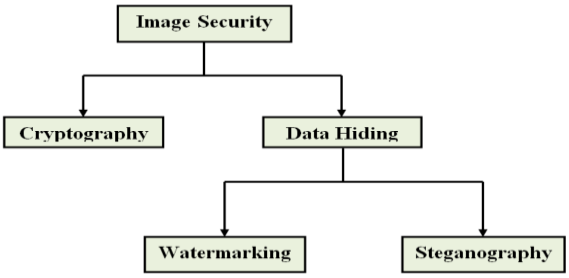


Figure 1: The image security structure

3 Image steganography

Hiding data is important in many applications to transfer confidential data, via electronic information networks. There are different types of hiding techniques where, confidential information can be concealed in text, audio, image or video. Image steganography in comparison to other types of steganography is widely used due to the large amount of excessive data in images that can be easily substituted of secret information. When, an image is selected to be applied to hide confidential data, it is called a cover image. The cover image that contains the confidential data is called a stego image. The cover image should be similar to the image of stego as it is difficult for the hacker to know the image of the stego. Many steganography approaches have appeared with different types of images such as: grayscale images, JPEG images, binary images, plate images.

Current research presents a robust method of embedding an encrypted image into a cover image using the least significant bits (LSB) of the cover image.

Figure 2 summaries the main processes of the proposed algorithm which represents a model of the image Steganography.

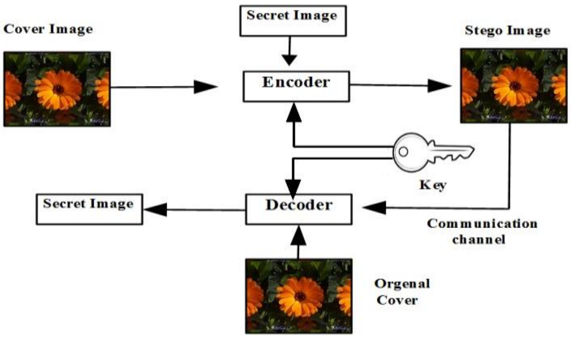


Figure 2: The model of image steganography.

4 Proposed method

This section consists of two phases as shown below.

4.1 The first phase

This phase aims, to apply the idea to encrypt a secret image and then, embed the encrypted image using the least significant bit of a cover image. We encrypt a secret image, in a new way of encryption using a new encryption algorithm, for the purpose of increasing security of information. The proposed method used a color image with different formats (BMP, JPEG, TIFF) to represent the secret and cover image. As shown in figure 3, the color image includes three colors: Red, Green and Blue (RGB) every color include 8 bits where, the value of each color represented by the numbers of binary system. Every image pixel consists of 3 bytes this number that locates the density of the color.

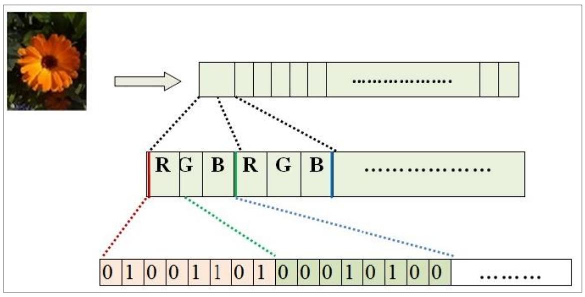


Figure 3: The binary color image form.

4.2 Encryption algorithm

The encryption algorithm includes four steps to encrypt the secret image as the following:

- Select the secret image as input.

1) The first step: For every pixel, flip the first bit of each byte in the pixel.
2) The second step: Perform the XOR function on each byte of the secret image using the first three most significant bits (MSB) as the encryption key.
3) The third step: Swap bits at (2, 3, 4) with bits at (5, 6, 7) respectively, for every byte of the secret image.
4) Fourth step: Reverse the direction of each byte in the secret image where, the most right bits substitute with bits of the most left.

- Obtains the encrypted image.

4.3 LSB steganography algorithm

The secret information can be hidden into digital images at different techniques. The better steganography technique is the least significant bits LSB which is in widely used today.

In this research, the spatial domain adopted by using the least significant bits LSB. The concept of the least significant bits (LSB) used to embed the encrypted image into the pixel values in a cover image, such that the embedding process will not affect the original pixel value. The most significant bit (MSB) is a set of bits at the most left of any binary number. The LSB level contains the least information associated with any image, while, the MSB level contains the most information of an image such as the image's shape and image's colors. So, we used the most significant bits of the encrypted image to embed in the least significant bits of a cover image.

The embedding algorithm includes several steps, as the following:

- Select the cover image as an input.
- The separation of the bit levels for the encrypted image (obtaining from the previous encryption steps) and the cover image.
- The four least significant bits (LSB) of the cover image is modified based on the values of the four most significant bits (MSB) of the encrypted image and according to the following cases :

1) Check if the values of two consecutive bits of MSB = 00, no modification is made in the two obverse values of LSB.

2) Check if the values of two consecutive bits of MSB = 11, the values of two consecutive bits of LSB are reversed.

3) Check if the values of two consecutive bits of MSB = 01, the first value of LSB is reversed.

4) Check if the values of two consecutive bits of MSB = 10, the second value of LSB is reversed.

- Repeat steps 1 to 4 to the next third and fourth LSB in the encrypted image.
- Continue to include the following pixels from the encrypted image until termination.
- Obtains the stego image.

An implementation of the LSB steganography algorithm is shown in figure 4.

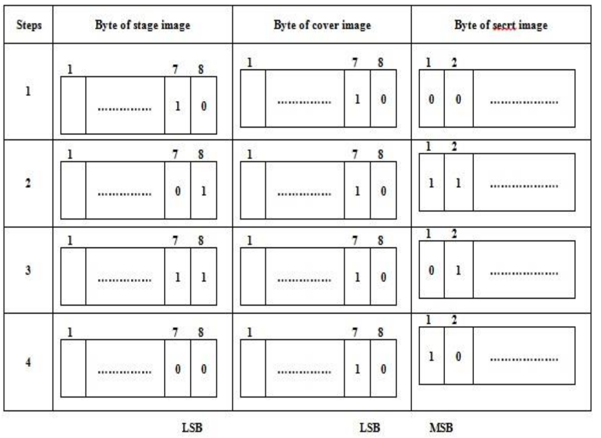


Figure 4: Implementation of LSB Steganography algorithm.

4.4 The second phase

This phase is the obverse of the first phase. Where, the encrypted image is regenerated from the stego image and then, retrieved the secret image. Thus, the recipient must be aware of the stego image, the cover image and cipher keys.

The strategy implemented in the second phase include the following two stages:

A. **The first stage**: At this stage, the cover image and stego image are used as input in this stage. To retrieve the encrypted image as the output of this stage, the original cover image needs to know the inverted bit of any pixel in the stego image.

- The generation procedure looks at each color in the least significant bits (LSB) matrices (red, green, and blue) of the stego image and compares it to the least significant bit (LSB) matrices of the cover image. Where, the values of four most significant bits (MSB) of the encrypted image are extracted based on the values of four least significant bits (LSB) of the cover image according to the following cases :

1) Two consecutive bits can be scanned into each pixel for the LSB. If the (1st and 2nd) LSB values of the cover image match the (1st and 2nd) LSB values of the stego image, be embedded, and both are zero, then the (1st and 2nd) MSB values of the encrypted image set to zero.

2) If the (1st and 2nd) LSB values of the cover image do not match the (1st and 2nd) LSB values of the stego image, be embedded, then the (1st and 2nd) MSBs values of the encrypted image set to one.

3) If the 1st LSB value of the cover image does not match the 1st LSB value of the stego image. Also, if the 2nd LSB value of the cover image matches the 2nd LSB value of the stego image, then reverse the 1st MSB value of the encrypted image.

4) If the 1st LSB value of the cover image matches the 1st LSB value of the stage image. Also, if the 2nd LSB value of the cover image does not match the 2nd LSB value of the stego image. Then reverse the 2nd MSB value of the encrypted image.

- Repeating the above four steps to the next third and fourth LSB of the cover image and the stego image to achieve the extraction the components of four MSB of the encrypted image. Continue with survey the next pixels and extract the encrypted image till up to terminating.
- Obtains the encrypted image.

B. **The second stage:** This stage describes the decryption algorithm of the encrypted image. Where, the cipher keys and the encrypted image are used as input in this algorithm.

- The output of this algorithm is a secret image.
- The decryption algorithm includes four steps can be summarized as the following:

1) Return the direction in each byte of the encrypted image to its original. Where, the most left bits of the image substituted with bits in the most right.

1) For each byte of the encrypted image, swapping bits from (2, 3, 4) with bits (5, 6, 7) respectively.

2) Execute the XOR function with each byte of the encrypted image by using symmetric cipher key.

3) For all pixels, revert the first bit of each byte in the pixel.

- Obtains the secret image.

5 Results and Analysis

In this section, we first describe the performance of the proposed method in two phases, in terms of stego image quality, then we will analyze effectiveness and efficiency of the proposed algorithm. We start with some experimental results that will be given to demonstrate the effectiveness of integration between the encryption algorithm and LSB steganography algorithm to significantly improve stego image quality. We tested this algorithm using various formats for the secret image and cover image. Figure.5(a), illustrates the results of first phase, as shown, the cover and stego images are without any plain variances. Thus, the proposed method can successfully embed the encrypted image in the cover image without deformation. The encrypted image can be absolutely generated from the stego image, and then decrypted by using symmetric cipher key, when the stego image is received, the experimental results present in figure. 5(b).

- **Mean Square Error (MSE)**

The mean square error (MSE) is used to measure the amount of image distortion that represents the difference between the cover image and the stego image. If the MSE value is low, the image quality is good. MSE is defined as follows equation:

$$(1) MSE = \frac{[I_1(M,N) - I_2(M,N)]^2}{M \times N}$$

Where M and N denote the number of rows and columns of the cover image, respectively. And I_1(M, N) denotes the pixel of the cover image at the point (M, N). And I_2(M, N) represents the stego image pixel at the point (M, N). Table 1 shows the experimental results of the proposed algorithm. As shown, the quality of the stego images is very good due to the low MSE values.

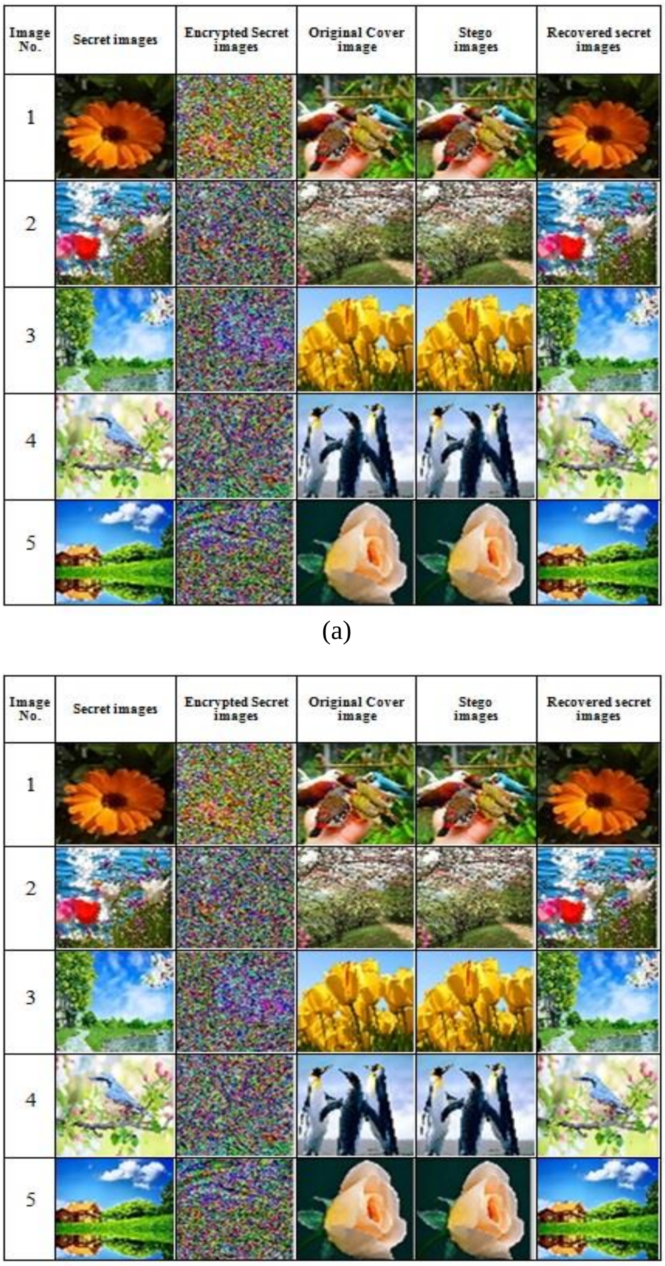
- **Peak Signal to Noise Ratio (PSNR)**

The PSNR is a criterion applied to gauge of imperceptibility in decibels. This is a quality comparison between the original cover image and the stego image. When, the PSNR value is high, refers to a slight different between a cover and stego images. The steganography algorithms aim to increase PSNR value. PSNR defined as the following equation:

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE} \qquad (2)$$

The above analysis and the experiments' results showed in table 1. The proposed method gives highest PSNR values, this means, the secret image hard to be detected. This indicates, algorithm provides better security and more robustness against attacks.

Figure 5: Illustrates the results of the first and second phase,
(a) the results of the first phase, and (b) the results of the second phase.



(a)

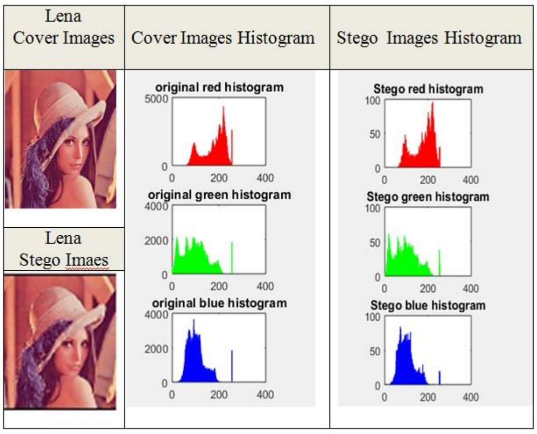
(b)

Table 1: Illustrates the experimental results of PSNR and MSE

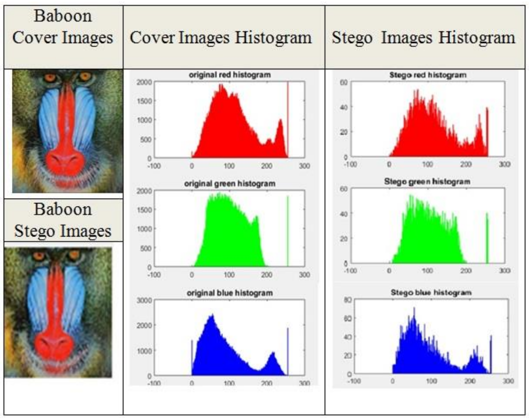
Cover Images	Image Size	MSE	PSNR
	480 × 480	0.0034	62.2145
	709 × 960	0.000780	74.9963
	1024 × 768	0.000889	68.0115
	1024 × 768	0.0018	65.0021
	265 × 190	0.0008892	68.0111

- **Histogram Analysis**

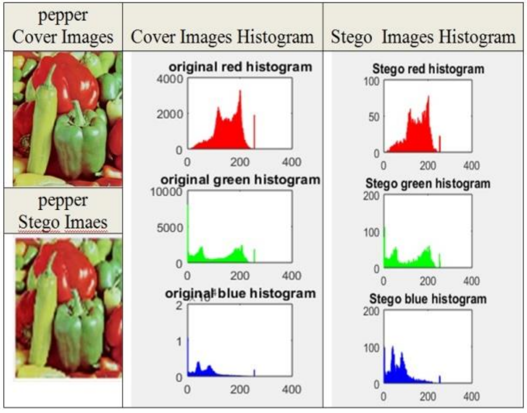
A histogram or qualitative analysis is used to investigate the quality of the proposed algorithm. This analysis is one of the significant types to comparison the quality of a steganography techniques which use the pixel-by-pixel comparison. Figure 6 shows the original image and the stego image for the (Lena, baboon and pepper) with their histograms. As shown, the stego images possess high quality, with no perceptible distortion. So any attack is improbable in the proposed method. The proposed method has been experimented on many cover images with various secret images where, the excellent results are obtained as in figure 5.



(a)



(b)



(c)

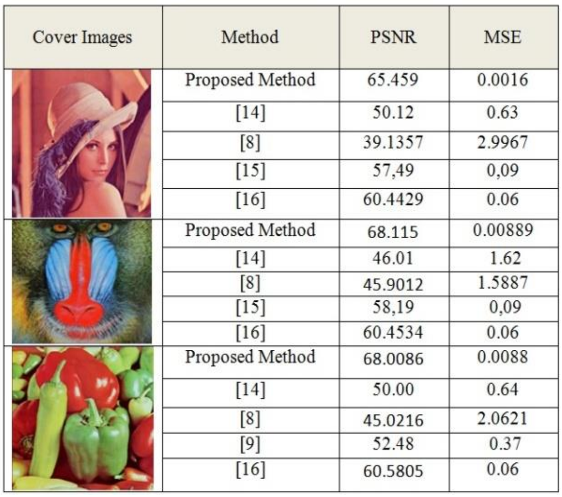
Figure 6: Histogram comparison of the cover and the stego images of the three components for (Lena, baboon and pepper).

6 Comparison results of the proposed method with existing techniques

In this section, the proposed method has been evaluated using three well-known images (Lena, baboon and pepper) with different image sizes, and with different formats based on using the proposed idea. To test the performance of the proposed method, the stego image's visual quality Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used. The MSE metric is widely used to locate the quality of the image. It is to estimate the mean squares of the error between the stego image and the cover image. PSNR is mostly used to determine the degradation of the stego image relative to the original image, that represents, the variance between the stego image and the original image.

The comparison results between the proposed method and existing methods illustrate in table 2. As clearly shows that the proposed method obtains high PSNR and best MSE results compared with the other methods.

Table 2: PSNR and MSE comparison for the proposed method with other methods using the same-colored images (Lena, Baboon and pepper).



Cover Images	Method	PSNR	MSE
	Proposed Method	65.459	0.0016
	[14]	50.12	0.63
	[8]	39.1357	2.9967
	[15]	57,49	0,09
	[16]	60.4429	0.06
	Proposed Method	68.115	0.00889
	[14]	46.01	1.62
	[8]	45.9012	1.5887
	[15]	58,19	0,09
	[16]	60.4534	0.06
	Proposed Method	68.0086	0.0088
	[14]	50.00	0.64
	[8]	45.0216	2.0621
	[9]	52.48	0.37
	[16]	60.5805	0.06

7 Conclusions

In this article a new method of image Steganography has been introduced. Where, the secret image has been encrypted and then embedded under the cover image. The proposed method based on color images (RGB) with various sizes and formats. From the above results we conclude the following:

1) The current work focused on hiding a color image inside another color image, and this is missing in the previous works.

2) Cooperation between Cryptography and steganography are used to protect the secret images during transmission over the internet.

3) The suggestion method provides more security for the detection of secret images within another image which is a convention between sender and receiver.

4) It is observed that through two phases, the results obtained in encrypting and hiding the image is perfect.

5) The test results showed that the proposed work achieves pretty, as shown by the high PSNR when embedding and MSE is less, table 1 present their results.

6) It is hard to distinguish between the original cover image and stego image by human eyes; experimental results are shown in figure 5 and 6.

7) The table 2 presents the comparison results that showed the proposed method contributes to achieve high robustness, gives better security and more reliable compared with the results of the other prevailing methods.

8 Future works

In the future, we can develop this work to be extended to include audio or video which varies according to the content and format.

References

[1] Singh, P., & Singh, K. “Image encryption and decryption using blowfish algorithm in MATLAB”, International Journal of Scientific & Engineering Research,4(7),150-154,2013. https://www.ijser.org/onlineResearchPaperViewer.aspx?Image-encryption-and-decryption-using-blowfish-algorithm-in-matlab.pdf

[2] Zynab M. jasim, “ Image Encryption Using Modification Blowfish Algorithm “, International Journal of Advances in Scientific Research and Engineering (ijasre), Vol 6 (3), March -2020. https://www.ijasre.net/index.php/ijasre/article/view/523

[3] Khan, J., Ahmad, J., & Hwang, S. O. , “An efficient image encryption scheme based on: Henon map, skew tent map and S-Box”, In 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO) (pp. 1-6). IEEE,May-2015. https://ieeexplore.ieee.org/document/7152261

[4] Abdelfatah A., Ayman M., Omaima Al-Allaf. "Hiding an Image inside another Image using Variable-Rate Steganography" , International Journal of Advanced Computer Science and Applications,2013. https://thesai.org/Publications/ViewPaper?Volume=4&Issue=10&Code=IJACSA&SerialNo=4

[5] Sally A. Mahdi & Maisa’a A. Khodher, “ An Improved Method for Combine (LSB and MSB) Based on Color Image RGB”, Engineering and Technology Journal, Vol. 39, No. 01, 2021. https://etj.uotechnology.edu.iq/article_168168.html

[6] Kothari, L. , Thakkar, R., & Khara, S. , “ Data hiding on web using combination of Steganography and Cryptography”, In 2017 International Conference on Computer, Communications and Electronics (Comptelix). 448- 452, IEEE, July 2017. https://ieeexplore.ieee.org/document/8004011

[7] Namrata S.,“High PSNR based Image Steganography”, International Journal of Advanced Engineering Research and Science, Vol. 6, No. 1, 2019. https://ijaers.com/detail/high-psnr-based-image-steganography

[8] Ashwak A. , Maisa'a Abid Ali K. Al-Dabbas , and Adnan S. , “Image steganography using the least significant bit and secret map techniques”, Int. J. Electr. Comput. Eng., Vol. 10, 2020. https://ijece.iaescore.com/index.php/IJECE/article/view/20793

[9] Yu Y. Wai and Ei. E. Myat, “Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image”, International Journal of Engineering Trends and Applications, Vol. 5, No. 4, 2018. http://www.ijetajournal.org/volume-5/issue-4/IJETA-V5I4P3.pdf

[10] Astuti, Y. P., Rachmawanto, E. H., & Sari, C. A. “Simple and secure image steganography using LSB and triple XOR operation on MSB”, In 2018 International Conference on Information and Communications Technology (ICOIACT), 191-195, IEEE,2018. https://ieeexplore.ieee.org/document/8350661

[11] Shehzad, D., & Dag, T. “A novel image steganography technique based on similarity of bits pairs”, In 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), 99-104, IEEE,2017. https://ieeexplore.ieee.org/document/8070576

[12] Jain, Y. K., & Ahirwal, R. R. “A novel image steganography method with adaptive number of least significant bits modification based on private stegokeys”, International Journal of Computer Science and Security, 4(1), 40-49, 2010. http://www.cscjournals.org/manuscript/Journals/IJCSS/Volume4/Issue1/IJCSS-230.pd

[13] Majeed, M. A., & Sulaiman, R. “an improved lsb image stenography technique using bit-inverse in 24 bit colour

image", Journal of Theoretical & Applied Information Technology, 80(2), 2015. http://www.jatit.org/volumes/Vol80No2/16Vol80No2.pdf

[14] Nisreen I. R. Yassin "data hiding technique for color images using pixel value differencing and chaotic ", Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 08, No. 03, September 2022. https://jjcit.org/paper/168/data-hiding-technique-for-color-images-using-pixel-value-differencing-and-chaotic-map

[15] Danish, S., Tamer, D., "LSB Image Steganography Based on Blocks Matrix Determinant Method", ksii transactions on internet and information systems vol. 13, no. 7, Jul. 2019.

http://itiis.org/digital-library/manuscript/2447

[16] Shreenandan K., Suman K., Sucheta P., Tushar S., & Anuja Kumar A., "Image Steganography using Index based Chaotic Mapping", International Journal of Computer Applications (0975 – 8887), 2015. https://www.ijcaonline.org/proceedings/icdcit2015/number1/19406-4001