High Security Image Cryptographic Algorithm Using Chaotic Encryption Algorithm with Hash-LSB Steganography

May H. Abood*, Sarah W. Abdulmajeed**
*Computer Engineering Department, College of Engineering, Al-Iraqia University, Iraq
**Computer Engineering Department, College of Engineering, Al-Iraqia University, Iraq

Abstract

In the latest, digital images are frequently used for storage, communication, medical imaging, etc. Such images possibly involve private data, which accordingly handed an important role to information security. Image encryption and steganography are two widely used techniques for providing information security. Cryptography is the technique of protecting information by encryption and decryption. In steganography, the message is inserted in an image with changes entitled a cover image. The principal purpose of the study is to improve the current secure data communication techniques, by combining cryptography with steganography. Steganography and cryptography are two examples of the multiple methods used to guarantee secrecy and privacy throughout data communication. The suggested approach achieves encryption and decryption utilizing chaotic encryption technique and employing hash-least significant bit (HLSB) as steganography which is a significant method of embedding data bits in LSB bits of RGB pixels of the cover image. The suggested image encryption method is validated by experimental results to be highly secure and resistant to a variety of attacks. Additionally, compared to several conventional picture encryption techniques, it offers higher performance. Peak signal-to-noise ratio (PSNR) and mean square error (MSE)calculations are used to provide security evaluations. PSNR is infinite and MSE is 0 for a secret image. PSNR and MSE for the cover image are 65 and 0.02 dB respectively. The results of this research reveal a high level of similarities between stego and cover images, and between recovered and secret images, as seen in the histogram analysis of secret images. These techniques are accomplished effectively by using the MATLAB program.

Keywords- Image Encryption, Chaotic map, Cryptography, hash-lsb, Cover image , Stego image, Steganography.

I. INTRODUCTION

With the fast progress of computer networks and advances in information technology, switching an enormous amount of digital data over unsecured channels is being ubiquitous. To protect the user data there are many techniques used. One such method is cryptography which the technique of transforming identifiable initial data to obvious nonsense. The other is Steganographic technique, where the information is embedded into any audiovisual material, such as an audio, image, or video so that, Just the intended destination distinguishes the message content[1]

The two chief regions that aim to protect and hide data are cryptography and steganography[2].They are significant methods to offer secrecy and guard information sensitivity [3]. Cryptography method is securing the secret message when it is moved from one place to another through the networks. The cryptography include two main classes which are Symmetric key encryption -both sender and receiver concerned of the same secret key-, the second is Asymmetric key cryptography –which use encryption and decryption algorithm pair-. The cryptography technique demand some algorithms for encrypt the data [4]. To guarantee safety of transmitted data, in this research, Both steganography and cryptography are applied. By encrypting secret image is using Chaotic Encryption Algorithm, and with hash Least Significant Bits inserted in cover image(RGB) before being sent.

II. LITERATURE REVIEW

In [2] to assure the encryption and decryption an algorithm with RC4 stream cipher and RGB pixel shuffling were used, while a hash-least significant Bit (HLSB) was used for steganography that uses hash function to developed important method of including data bits in LSB bits of the cover color image pixels.

[5] proposes a scheme to randomly pick the coefficients for embedding a secret message by using a complex chaotic map.

In [1] the content were altered from its distinctive form (plain text) to nonsensical form (figure content) by employing the Advanced Encryption Standard (AES) scheme, then Least Significant Bit (LSB) were used to cover the figure content in the picture.

the goal of the study in [6] is to briefly present latest evolvement within the zone of data security employing combining steganography with cryptography (crypto-stego) approaches certifying two-layer security for secret communication. The advantages and disadvantages of the present image steganography methods and crypto-stego approaches were highlighted.

depends on chaotic map, scan method with cyclic shift operation, the study in [7] presents a new symmetric key encryption mechanism. Also, using Hilbert curve and Henon map to implement confusion and diffusion techniques.

[8] uses RC4 method to transfer data securely, to protect data on the common channel as it's cryptographic method is faster, simpler to appliance and the keystream is an random sequence of bits which guarantees the safety of used cipher.

The technique in [3] support and improve the information security methods with more capacity and faster transmission.

The paper in [9] raised to treat the secrecy of applications, so it proposes a security scheme. It uses wavelet and genetic algorithm based steganography to embedding a secret text message over a secret image, then using a filter bank cryptographic algorithm on the resulted stego image for encryption, also to ensure data integrity the hashing algorithm is used.

The paper in [10] concentrate on a protected image steganographic technique based on Hash-based Message Authentication Code (HMAC) algorithm and Canny Magic LSB Substitution approach (CM-LSB-SM).

[11] combine RSA with ACM and then using inverted 2-bit LSB steganography, that modifies 2 bits in cover picture bit plane with bits of message, the outcome is hidden in the cover image.

[12] presents a new spatial domain chaotic steganograpic approach, also to hide Turkish texts were encoded and compressed using Huffman it employs a new fractal stream encryption algorithm.

[13] employs the AES cryptosystem combined with the Diffie-Hellman key exchange mechanism, as well as SPIHT compression, where wavelet transform of the image takes place for steganography, to provide increased security and speed of processing.

In [14] a new steganography algorithm is proposed, Improved Chaos Based Bit Embedding. It is based on two basic standards. The first involves using a logistic map to locate the bits where the secret data will be inserted, and the second is inserting the top-secret data into just one of the RGB channels, which is picked at random.

The study in [15] uses least significant bit hash method and supplies renovation on digital watermarking. and is evaluated using histogram analysis, data capacity analysis, and hamming distance.

[16] uses RGB photo and Magic LSB Substitution Method (M-LSB-SM) to maintain the primary goal of the study, which is increasing embedding capacity and providing good imperceptibility. For much enhancement of security level, Hash-based Message Authentication Code (HMAC) scheme is used to appending generated message authentication code to the secret message.

to advance a video steganography mechanism [17] uses 2D chaotic map and NLFSR, where the separated frames will contain embedded data.

By means of the hash value in image, the study in [18] targets to demonstrate a hash based LSB method where results are secured by using EXIF data through employing cryptography and steganography.

[19] proposes a combination of the Rivest Code 4 (RC4), Least Significant Bit (LSB)- Blowfish because it can offer layered security on confidential data.

[20] suggests a new cryptographic method that makes use of the benefits of both significant schemes – chaotic image encryption and steganography.

The article in [21] presents a plaintext-related images cryptosystem that changes the quantities of the logistic map parameter depending on the pixel intensities of the plain image.

By using steganography with encryption, [22] improves information security by formulating new effective image cryptography technique.

III. PROPOSED METHODOLOGY

In order to maintain the secrecy of transmission data and particularly photos, which is a crucial research field in various fields including data privacy and security, secured data transfer, and Copyright protection, security is one of the top three priorities for the next generation of internet users. Algorithms for concealing and encrypting images should be created to improve transmission efficiency and protect against outsider attacks. The highest level of data integrity, confidentiality, and security can therefore be attained using the suggested strategy. In this study, Chaotic Cryptosystem is used for cryptography with Hash-LSB for steganography in order to achieve the confidentially of a grayscale image. The mechanism of the suggested system is illustrated in the following diagrams in Fig. 1.

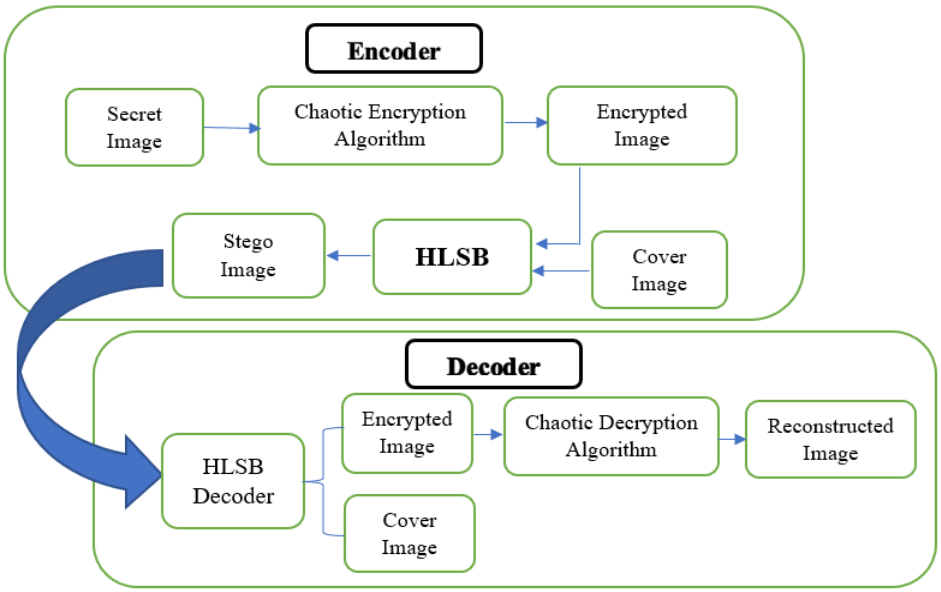


Fig.1 Encoder and decoder for the proposed system

A. Chaotic Encryption Algorithm

Chaotic cryptosystem has recently emerged as a popular field of study for image encryption. three groups that make up the current picture encryption techniques which are pixel position permutation, pixel value transformation, and combined methodology. The simple pixel position permutation strategy simply shuffles the original pixels in accordance with a predetermined pattern. Data security is typically poor with these methods. The pixel values of the image are changed through transformation scheme. The hardware cost and complication of operations are decreased with this type of alteration. High data security is provided by the combined method. [23].

Chaotic maps schemes are dynamic that are highly sensitive to initial states and control factors. Any small alteration in the initial setting. reasons a significant deviation. Our capacity to predict how chaotic systems will behave over a lengthy period of time has been seriously affected by this sensitivity. Initial situations are used by encryption systems as a cryptographic key based on chaos. both One-dimension and as well as high-dimension maps are two categories of chaotic maps. Typically, a one-dimension map has only one variable and few parameters.[7].

Figure 2 illustrates the presented cryptosystem's structure. It is divided into three stages pixel permutation, diffusion, and key stream generation. To ensure confusion, the pixel permutation stage is accomplished using a double scrambling process. first round of scrambling is done at the pixel level, and second round is done at the bit level . The scrambled image is encoded using the key stream K2 during the diffusion stage. The cipher image is the result of the diffusion stage. the encryption part is replayed R times to ensure security.

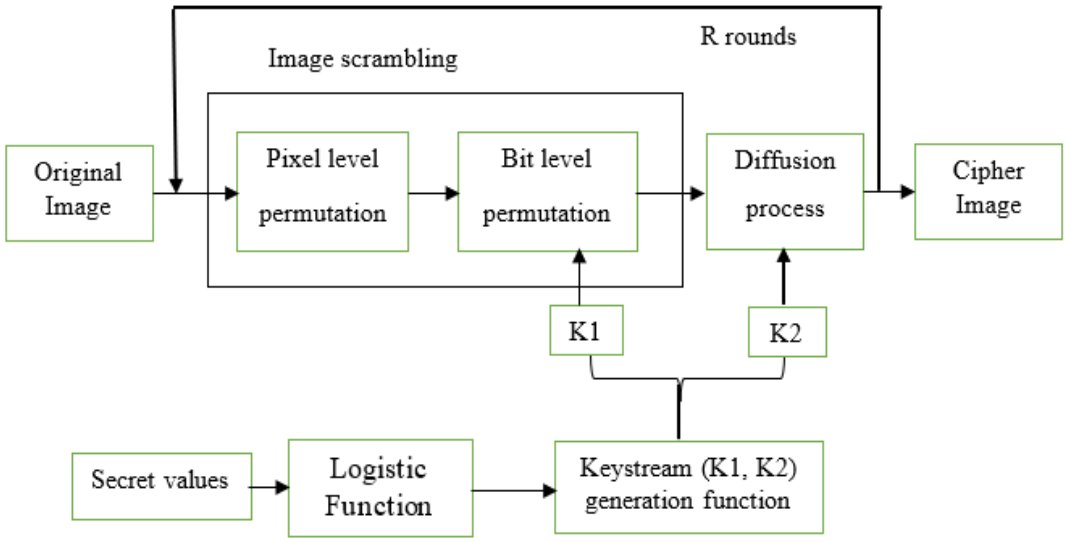


Fig.2 The proposed cryptosystem architecture

B.Hash-LSB Steganography

In the field of communications, The LSB image steganography technique is typically used to insert information or data inside a cover (such as an audio, image, or video). Before concealment, a secret message's characters are each transformed into an 8-bit binary series and changed with the eight least significant bits of the pixel containing the cover image [2].

A distinction between the hash-based LSB method and simple LSB method is based on the hash function, which allows for the hiding 8-bit of a secret data in the LSB locations of the RGB pixels of the cover image. The division order of the bits is 3,3,2. The first three bits of the secret picture are inserted into the R pixel, the second three bits are inserted into the G pixels, and the final two bits are inserted into The eight bits were arranged in the manner described before because the chromatic effect of blue color on the human eye is greater than that of red and green color [24].

According to Fig. 3, the secret message pixels is inserted in the following order: (3,3,2). Each pixel in secret image is inserted in the LSB of the cover image (RGB) as shown in z, where z is the position of the LSB bit for each pixel.
For red pixels, z=1 ,2 and 3.
For green pixels, z=1, 2 and 4.
For blue pixels, z=3 and 4.

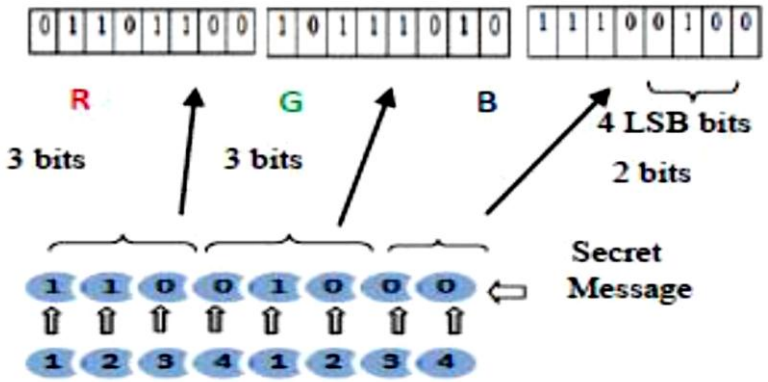


Fig.3. Bits distribution of Secret mage pixel

The following formula can be used to identify the positionsto hide information in each RGB pixel of the cover image:

$$Z = P \,\%\, N \quad (1)$$

Where, Z is the LSB bit positions in each pixel,
P represent the location of any hidden picture pixels,
N stands for the number of LSB bits, which in this instance is 4.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

By using the suggested method, we have created a system that utilises the MATLAB program to perform the suggested algorithms. The Mean squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) are investigated as a target measures.

$$\mathbf{MSE} = \frac{1}{h*m}\sum_{1}^{h}(\boldsymbol{p}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{s}(\boldsymbol{i},\boldsymbol{j}))^2 \quad (2)$$

Where, H and W are the height and the width of is original image(P(i,j)) and stego-image (S(i,j)) .

$$\mathbf{PSNR} = 10\log_{10}\frac{L^2}{\mathbf{MSE}} \quad (3)$$

Where, L is signal level of image (255).

The execution time is also calculated using MATLAB instructions by use ***tic*** instruction in the biggening of the code ***toc*** instruction in the end of the code that we need to measure it's execution time.

A. The sender's side

1. The following photos will be used for grayscale image (secret) and RGB image (cover).

Secret images


1.png


2.tif


3.jpg

RGB cover images


1


2


3

2. Encrypt secret image using Chaotic Encryption Algorithm

3- Insert 8 bits of coded image into the forth LSB of each RGB image pixels respectively in order of 3, 3, and 2

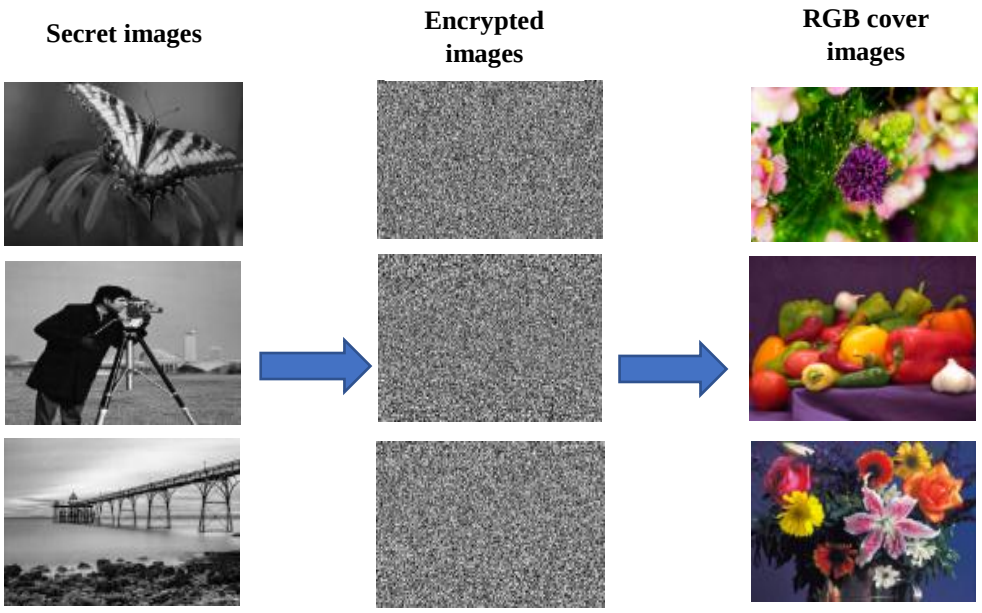


Fig.4.Image Encryption process

B. The Receiver's side

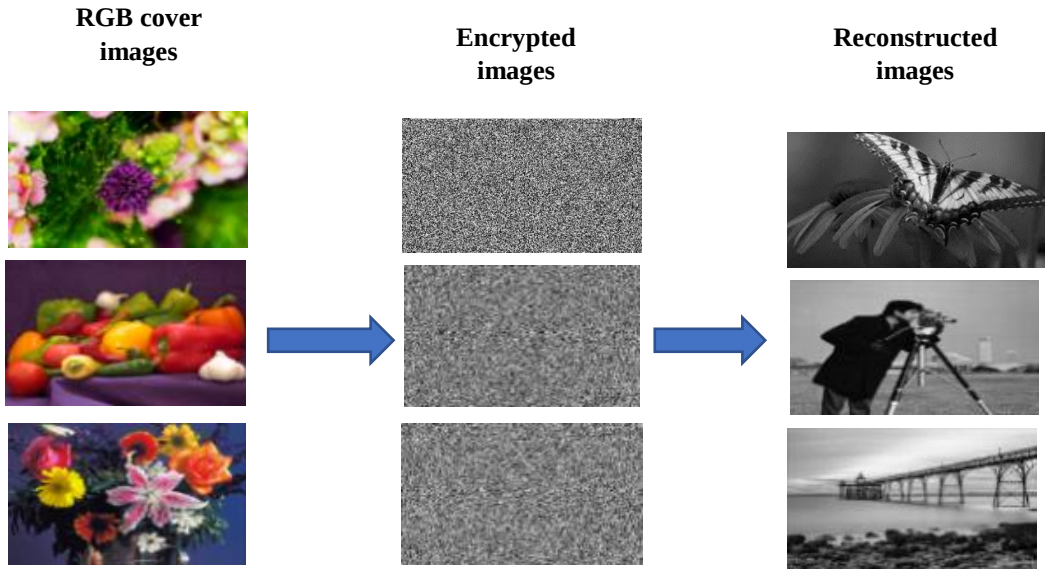
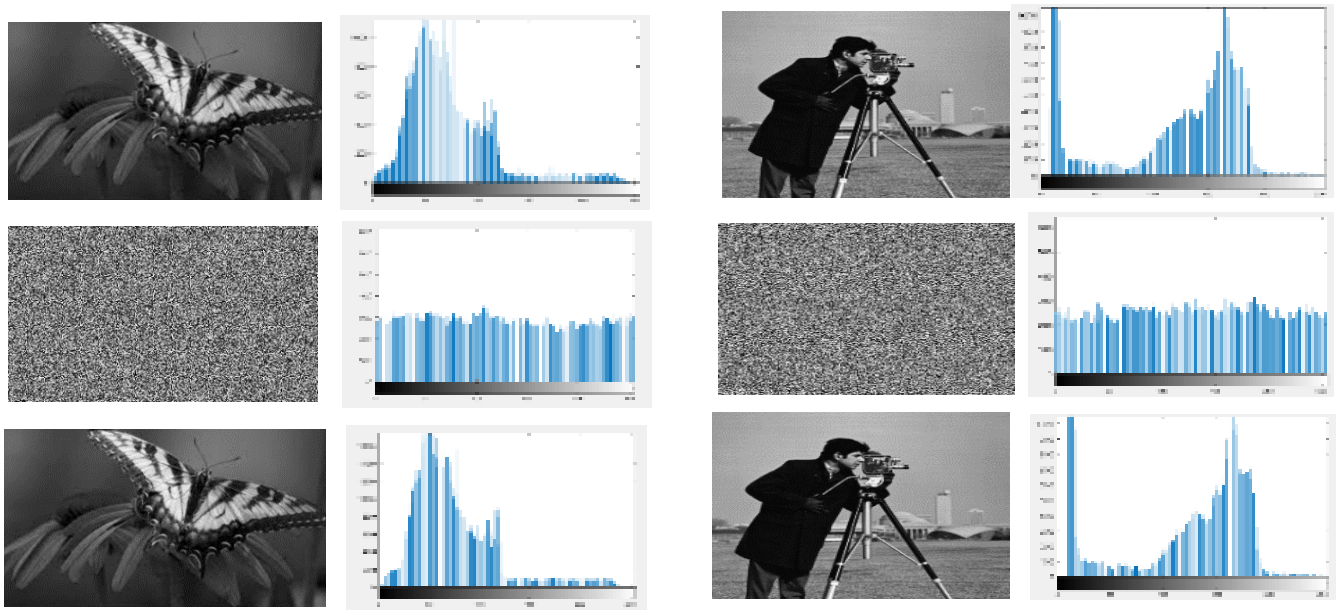


Fig.4.Image Decryption process

C. Histogram Analysis

By using histogram that represent the statistical features of the image , plotted the images' pixel frequency of occurrences for both original and cipher images.the analysis show that the two images histogram are totally different as shown in fig.5



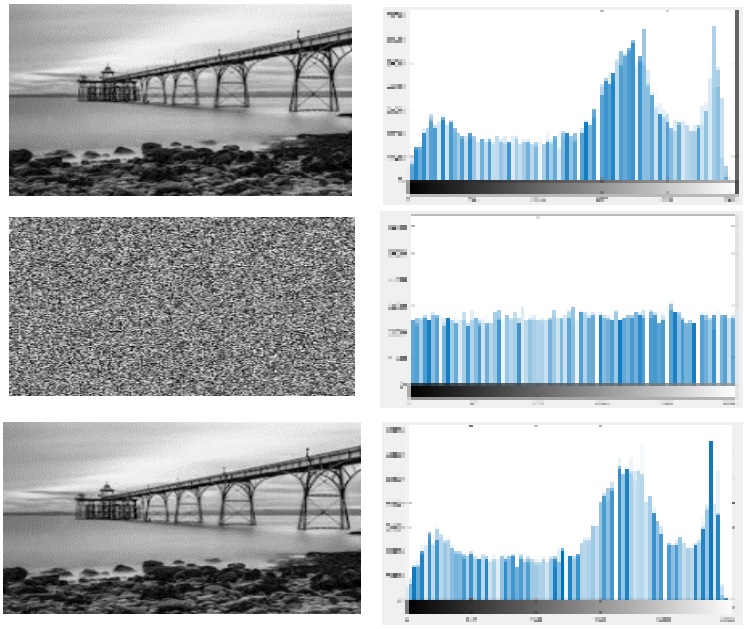


Fig.5. Histogram analysis for secret images

The cover image and stego-image are shown in the aforementioned photos to be unchanging, as shown in figure 4. Produces the cover images when applying the Chaotic Encryption Algorithm and HASH LSB. We can see that the cover and stego-images are identical when we compare them after embedding the ciphered image into that cover image.

So it is evident that for increased security and privacy, we can embed the picture or message in cover image utilizing the Steganographic approach. Both the PSNR and MSE are calculated for the recommended system in this section. Table 1 and Table 2 both display the measures for hidden photos and cover images respectively. The results of the two specific tests demonstrate that in compared to an unencrypted system, coding is more secure that's because the values for secret and stego images with high PSNR values . This indicates that there is a high degree of similarities between the retrieved photos and hidden images as well as between stego-images and cover images.

Table 1. Secret images MSE, PSNR and Elapsed time

Secret Images	MSE	PSNR	Time
Sec1	0	Inf.	2.066 s
Sec 2	0	Inf.	2.155 s
Sec 3	0	Inf.	2.065 s

Table 2. Cover images MSE, PSNR and Elapsed time

Cover Images	MSE	PSNR	Time
Cov1	0.0198	65.1701	2.066 s
Cov2	0.0193	65.2824	2.155 s
Cov3	0.0199	65.1724	2.065 s

VI. CONCLUSION

This study deals with two topics to Improve authentication of data transmission. The suggested system is Considered the best for hiding the encrypted data before transmission from sender to receiver in unsecured media. The secret image (a png, gif, or jpg) is encrypted using the Chaotic Encryption Algorithm before being included in the RGB cover image to prevent hackers from detecting the encrypted data. The proposed encryption technique strength is the confusion and diffusion properties and its protection from statistical attack. H-LSB steganography was applied to embed secret image into the RGB cover image. By concealing data in an image with less change in image bits, the proposed HLSB technique is the idea of an enhanced steganalysis, which increased system security and efficiency and allowed the system authorization to function with Cryptosystem. we use test images as a secret images(png,tif,jpg) and RGB cover images in the proposed Algorithms and the system is evaluated using the measurements of (MSE , PSNR and Execution time).Experimental results showed that the System is efficiently provide High security and Authentication without effected the secret and cover images quality as appeared in our measurements.

REFERENCES

[1] M. H. Abood and Z. K. Taha, "Secure and hidden text using aes cryptography and lsb steganography," *J. Eng. Sci. Technol.*, vol. 14, no. 3, pp. 1434–1450, 2019.

[2] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," *2017 Annu. Conf. New Trends Inf. Commun. Technol. Appl. NTICT 2017*, no. March 2017, pp. 86–90, 2017, doi: 10.1109/NTICT.2017.7976154.

[3] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using lsb algorithm and 5d hyper-chaotic system," *Bull. Electr. Eng. Informatics*, vol. 10, no. 2, pp. 689–698, 2021, doi: 10.11591/eei.v10i2.2747.

[4] A. S. Al Najjar, "Implementation Color-Images Cryptography Using RSA Algorithm," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 11, p. 181, 2017, doi: 10.23956/ijarcsse.v7i11.500.

[5] N. I. R. Yassin, "D Igital I Mage D Ata H Iding," vol. 08, no. 03, pp. 242–255, 2022.

[6] A. Jan, S. A. Parah, M. Hussan, and B. A. Malik, "Double layer security using crypto-stego techniques: a comprehensive review," *Health Technol. (Berl).*, vol. 12, no. 1, pp. 9–31, 2022, doi: 10.1007/s12553-021-00602-1.

[7] K. U. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Appl. Soft Comput. J.*, vol. 90, p. 106162, 2020, doi: 10.1016/j.asoc.2020.106162.

[8] أ. ع. موسى and م. ح. عبود, "Telecommunication Of A Secure Data In Optical Fiber," *مجلة المنصور*, vol. 72, no. 27, p. 119, 2017, doi: 10.36541/0231-000-027-009.

[9] S. Saraireh, J. Al-Saraireh, Y. Al-Sbou, and M. Saraireh, "A hybrid text – Image security technique," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 9, pp. 2414–2422, 2018.

[10] C. Paper, "Secure Image Steganography using Canny Magic LSB Substitution Method and Secure Image Steganography using Canny Magic LSB Substitution Method and HMAC Algorithm," no. August, 2019.

[11] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "A combination of inverted LSB, RSA, and arnold transformation to get secure and imperceptible image steganography," *J. ICT Res. Appl.*, vol. 12, no. 2, pp. 103–122, 2018, doi: 10.5614/itbj.ict.res.appl.2018.12.2.1.

[12] M. C. Kasapbasi, "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption with Post-Quantum Security," *IEEE Access*, vol. 7, no. October, pp. 148495–148510, 2019, doi: 10.1109/ACCESS.2019.2946807.

[13] M. Malathi, M. Rahul, N. Sathish Kumar, and R. Thamaraiselvan, "Enhanced image steganography using AES & SPIHT compression," *Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017*, vol. 2018-Janua, no. March, pp. 1–5, 2018, doi: 10.1109/ICIIECS.2017.8276029.

[14] K. Tutuncu and B. Demirci, "Adaptive LSB steganography based on chaos theory and random distortion," *Adv. Electr. Comput. Eng.*, vol. 18, no. 3, pp. 15–22, 2018, doi: 10.4316/AECE.2018.03003.

[15] S. D. Muyco and A. A. Hernandez, "Least significant bit hash algorithm for digital image watermarking authentication," *ACM Int. Conf. Proceeding Ser.*, no. April, pp. 150–154, 2019, doi: 10.1145/3330482.3330523.

[16] M. M-lsb-sm, "Color Image Steganography using Cryptography and Magic LSB Substitution Color Image Steganography using Cryptography and Magic LSB Substitution Method (M-LSB-SM)," no. July, 2019.

[17] N. Kar, M. A. A. A. Aman, K. Mandal, and B. Bhattacharya, "Chaos-based video steganography," *ICIT 2017 - 8th Int. Conf. Inf. Technol. Proc.*, pp. 482–487, 2017, doi: 10.1109/ICITECH.2017.8080046.

[18] S. D. Muyco and A. A. Hernandez, "A modified hash based least significant bits algorithm for steganography," *ACM Int. Conf. Proceeding Ser.*, no. July, pp. 215–220, 2019, doi: 10.1145/3335484.3335514.

[19] A. D. Putri Ariyanto, E. H. Rachmawanto, D. R. Ignatius Moses Setiadi, and C. A. Sari, "Performance Analysis of LSB Image Steganography Combined with Blowfish-RC4 Encryption in Various File Extensions," *Proc. 2019 4th Int. Conf. Informatics Comput. ICIC 2019*, no. March 2020, 2019, doi: 10.1109/ICIC47613.2019.8985848.

[20] A. A.S, "High Security Cryptographic Technique Using Steganography and Chaotic Image Encryption," *IOSR J. Comput. Eng.*, vol. 12, no. 5, pp. 49–54, 2013, doi: 10.9790/0661-1254954.

[21] J. Oravec, L. Ovsenik, and J. Papaj, "An image encryption algorithm using logistic map with plaintext-related parameter values," *Entropy*, vol. 23, no. 11, 2021, doi: 10.3390/e23111373.

[22] M. H. Abood, "Steganography with RC4 and Pixel Shuffling Encryption Algorithms," no. March, pp. 7–9, 2017.

[23] J. C .Yen., and J. I. Guo, ,"A new image encryption algorithm and its VLSI architecture". In IEEE Workshop on Signal Processing Systems, SiPS 99. Design and Implementation ,Cat. No. 99TH8461,pp. 430- 437, 1999.

[24] P. R. Deshmukh and B. Rahangdale, "Hash Based Least Significant Bit Technique For Video Steganography", Int. Journal of Engineering Research and Applications, vol. 4, no. 1, pp. 44–49, January 2014.

AUTHORS

First Author – May H.Abood, Computer Engineering dept,College of Engineering, Al-iraqia University, may.hattim@gmail.com.

Second Author – Sarah w. Abdulmajeed, Computer Engineering dept,College of Engineering, Al-iraqia University, sarah.waleed2222@gmail.com