Int. J. Nonlinear Anal. Appl.
Volume 12, Special Issue, Winter and Spring 2021, 1283-1291
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2021.5644

Secret information hiding in image randomly method using steganography and cryptography

Awad Kadhim Hammoud[a,*], Hatem Nahi Mohaisen[b], Mohammed Q. Mohammed[a,c]

[a] *University of Information Technology and Communications, Iraq, Baghdad*
[b] *Ministry of Higher Education and Scientific Research/Baghdad-Iraq*
[c] *Al-Esraa University College, Baghdad, Iraq*

(Communicated by Madjid Eshaghi Gordji)

Abstract

In this research paper, we will present how to hide confidential information in a color image randomly using a mathematical equation; by apply this equation to the number of image bytes after converting the image into a digital image, the number of randomly selected bytes depends on the length of the secret message. After specifying the bytes, we include the secret message in those selected bytes utilizing least significant bit (LSB) of steganography, and return the new bytes in the same place in the original image by using the same mathematical equation, after the hiding process using steganography, and then we encrypt the image and send it to the recipient. Several statistical measures applied to the original image, compared with the image after embedding, and after the image encrypted. The results obtained are very good. The statistical measures were used the histogram, mean square error (MSE) and the peak signal to noise ratio (PSNR). The system is designed to perform these processes, which consists of two stages, hiding stage and extract stage. The first stage contains from four steps, the first step of this stage reading the image and converting it to a digital image and make an index on each byte of the image bytes and the application of the mathematical equation to select the bytes by randomly, second step is the process of hiding the secret message in selected bytes and return those bytes to the original locations, third step is the calculation of the statistical measures to determine the rate of confusion after the inclusion of the confidential message, fourth step to encrypt the image of the message carrier and measure the rate of confusion after the encryption and compare with the original image. The extraction process consists of three steps, the first step is to use the private key to decrypt, and the second step is to apply the

[*] Corresponding author

Email addresses: awadkadhim@uoitc.edu.iq (Awad Kadhim Hammoud), ha19652010@yahoo.com (Hatem Nahi Mohaisen), dr.mohammed@uoitc.edu.iq (Mohammed Q. Mohammed)

Received: April 2021 *Accepted:* July 2021

same mathematical equation to extract the embedded bytes of the confidential message, third step use the same method of hiding the information and extracting the confidential message.

Keywords: Steganography, Encryption, Decryption, Cryptography, Image, LSB, Randomly.
2010 MSC: Please write mathematics subject classification of your paper here.

1. Introduction

At present, Protection of information is becoming very significant in the data saving and transmissions, especially those that require high confidentiality levels. Images are largely hired in many operations. Which is why, preservation of image data from prohibitive arrival is significant or any unknown user can able to decrypt the image. Image encryption has an important impact on the domain of information concealment. Image steganography or encryption approaches and methods are ranging from the simple approaches of the spatial domain to more complex and reliable frequency domain ones [10]. In the present study will present historical overview of the steganography and cryptography definition for you. The research details also which the method to implement idea in through applying this method and getting results, ratio of (MSE, PNSR, error histogram), what is the equation apply to get random pixel from image and how working the LSB. Also using MATLAB software to apply and development system. Figure 1 [8] shows all methods and techniques used in field of protect and secret of information on communication media.

2. Steganography

Steganography get most significant as most people joining internet rise. Steganography it is art of hiding information in methods which are preventing the detecting of concealed letters in digital media. Steganography consist a set of covert communication ways that conceal the letter from being looking or detected. The aim of steganography is to aloofness of from doubt to the existence of a concealing letter.

Recently this approach got of information hiding technique important in many of implementation areas [6]. Steganography techniques can be applying to image, video file or all audio file. As you explain in the figure 2 [4].

The concealing operation can be characterize as a mapping: $E : H \times L \longrightarrow H'$

The extraction operation includes a mapping:

$D : H' \longrightarrow L$

Extraction of the secret message out of the cover: Clearly, it is necessary that $\mid H \mid \geq \mid L \mid$. Both sender and recipient should have access to the concealing and extraction algorithm, but the algorithm have to not be general [12].

3. History of Steganography

Considering Herodotus is the first used steganography up to 440BC, in the case where the Herodotus marks 2 examples in the history. Histiaeus shaved the head of more confidence serf and tattooed it by a letter that did not appear after grow the hair. The aim has been instigating a revolution contra Persians. From the amaze some German spies was still using this method in beginning 20th century. Also Herodotus tells how Demeratus, a Greek at Persian court, caveat Sparta of a proximate invading by Xerxes: he taken writing tablet and removed wax from it, wrote his letter on the wood under and after that covered letter by wax [15].

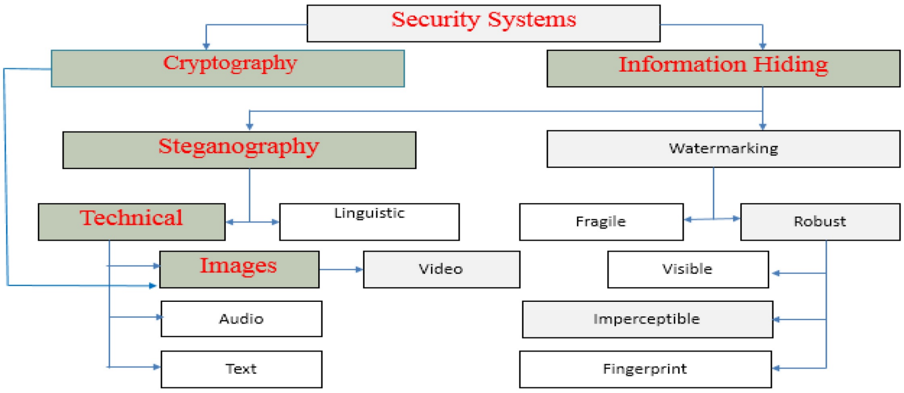


Figure 1: The different disciplines of security system, special focus on information hiding and cryptography techniques

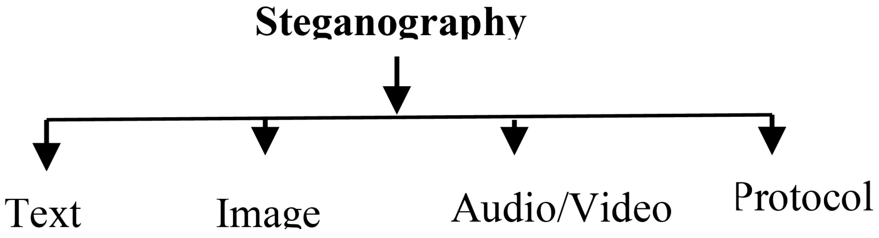


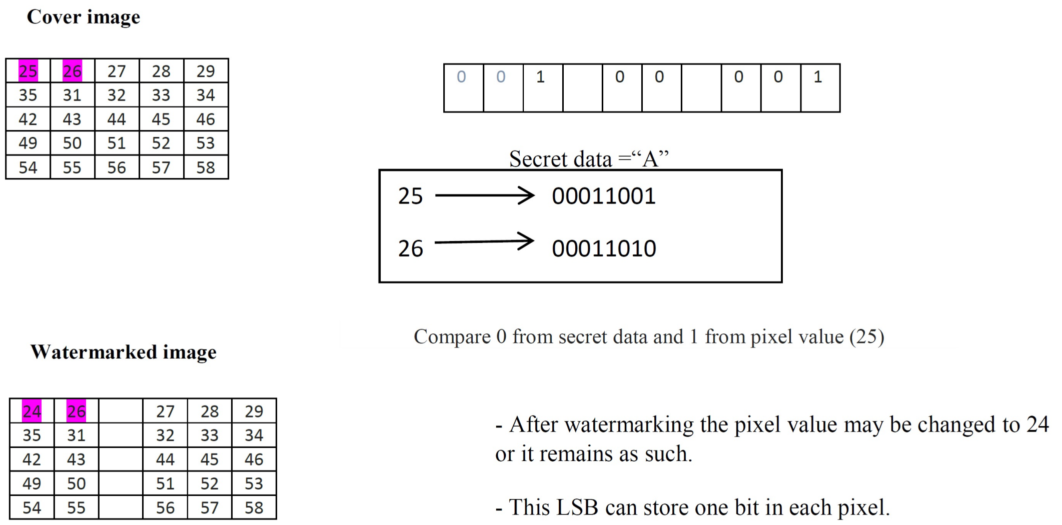
Figure 2: Type of Media Cover to the Hidden

4. Cryptography

Cryptography can be defined as a technique for coding and decoding secret messages for preservation message from prohibitive user's arrival the messages. In network environment, cryptography has an important impact on the preservation of the data in the running applications. In Greek, cryptography is translated "hidden Secret". In addition to that, in past, the cryptography has been utilized by political sectors of military and intelligence, however, it is now widely used for e-commerce, ATM cards, email, computer passwords, as well as other application. With the time there is a variety of the algorithms are utilized for the message modification with encryption key that is declared only to the recipient and the transmitter [11]. This message cannot be decrypted unless we use the encryption key. A problem that had emerged with the cryptography is that a message is always evident to the intermediate person that this message has been encrypted. Which indicates the fact that the message sender doesn't want it read by an unauthorized individual. In the present day, there is a high number of the cryptographic approaches that have the ability of data encryption [2].

5. Encryption

Encryption can be defined as a certain cryptographic element where one hides the information or the data through the transformation of that element to some undecipherable code. Usually, encryption utilizes certain key or parameter for performing transformation of the data. Some algorithms of encryption need the key to be of an identical size as the message that will be encoded, however, other algorithms of encryption may operate on considerably smaller keys that the message. The decryption is usually categorized along with the encryption as the opposing operation. Decrypting the encrypted data produces original data [17].



Cover image

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

0	0	1		0	0		0	0	1

Secret data ="A"

25 → 00011001

26 → 00011010

Compare 0 from secret data and 1 from pixel value (25)

Watermarked image

24	26		27	28	29
35	31		32	33	34
42	43		44	45	46
49	50		51	52	53
54	55		56	57	58

- After watermarking the pixel value may be changed to 24 or it remains as such.

- This LSB can store one bit in each pixel.

Figure 3: Least Significant Bit Technique

6. Least Significant Bit

Least Significant Bit (LSB) Insertion represents the simplest approach, where every 8bit pixel's LSB is overwritten by a watermark bit. In a digital image, data may be directly inserted to each one of the image data bits or may more busy regions of image may be calculated in order to conceal those letters in less perceptible image portions. This approach has been based upon modifications of pixel value's LSB [9].
The concept of the embedding is fairly effective and simple. In the case where grayscale bmp picture are using, which is 8 bit, it would require reading in file and after that, adding the information to every pixel's LSB, in each one of the 8 bit pixels. Each pixel in the gray-scale picture is represented by 1 byte include 8bits. Between the black which is 0 to white which is 255 it can represent 256 gray colors. Uses the LSB of every one of those bytes, the bit on the far right side, it is the principle of encoding. If use only the last 2 significant bits to the data encoding(first and 2nd LSB) of every one of the color components not going to be detectable most likely; it becomes retina the human the limiting factor in viewing picture. This example only the LSB of every one of the pixels will be used for concealing data. If the value 10000110 in binary for the pixel value is 134 and watermark bit is 1, it will be the value 10000111 to the pixel in binary which represents 135 in decimal [18, 16, 5, 1, 14]. Figure 3 clear the LSB technique.

7. Fidelity Measure

The type of measure used to estimate of the level of difference between original image choosing and image after embedded the information. The most of used fidelity criteria are:

A – Mean Square Error (MSE) MSE it is similar to the absolute value, it is the average of the square of errors (pixel differences) of two images. Measure (MSE) between two images by equation (7.1) [3]:

$$MSE = \frac{1}{mh}\sum_{y=1}^{h}\sum_{x=1}^{m}(f_{org}(x,y) - f_{embed}(x,y))^2 \tag{7.1}$$

B – Peak Signal to Noise Ratio (PSNR) The values PSNR are utilized only to compare the performance of loss coding scheme. PSNR is determined using equation 7.2 or (7.3) [3]:

- In color image the equation is:

$$PSNR = 10\log_{10}\left(\frac{(\max_{xy} f_{org}(x,y) - \min_{xy} f_{embed}(x,y))^2}{MSE}\right) \tag{7.2}$$

- In gray scale image with eight bits the equation is:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{7.3}$$

Where $\max_{xy} f_{org}(x,y) = 255$, and $\min_{xy} f_{org}(x,y) = 0$.

8. Pseudo-Random Number Generator

In the title of this section notice the word “pseudo” in it, this word it means false, so are being generated false random numbers. In this case, the ”pseudo” is used imply that the very act of random numbers generating by a known method eliminate the likelihood for true randomness. The linear Congenital method is the most widely technique used for random numbers generating. We also report an extension of this method that yields sequences with longer period [16]. Linear congenital Random Number Generator, initially proposed by Lehmer [13], generating a sequence of integers, $x_1, x_2, ...$ Between (0-n-1). The initial value x_0 has been referred to as seed number, a constant multiplier, b increment, and n modulus. Every one of the successive random numbers x_{i+1} is produced by [7]:

$$x_{i+1} = mod(a^* x_i + b, n); i = 0, 1, 2, ... \tag{8.1}$$

9. Proposed System

First of all there are some outlines for the proposed system is briefly listed below:

A. Preparing cover media (image).

B. Secret information to hide in the cover image

C. Arithmetic the size of secret information.

D. Transform the cover image to digital cover and separating every color (RGB) in array.

E. Combining the matrixes in (D) to product one matrix with index every pixel $(n^* M^* 3, 1)$.

F. Applying equation (8.1) to choosing number of random pixel from E depending to size of secret information and seed number.

j. Hiding the secret information using (LSB) algorithm on F.

K. Feeding back every pixel to place depended on index of E, product to the (steg_image).

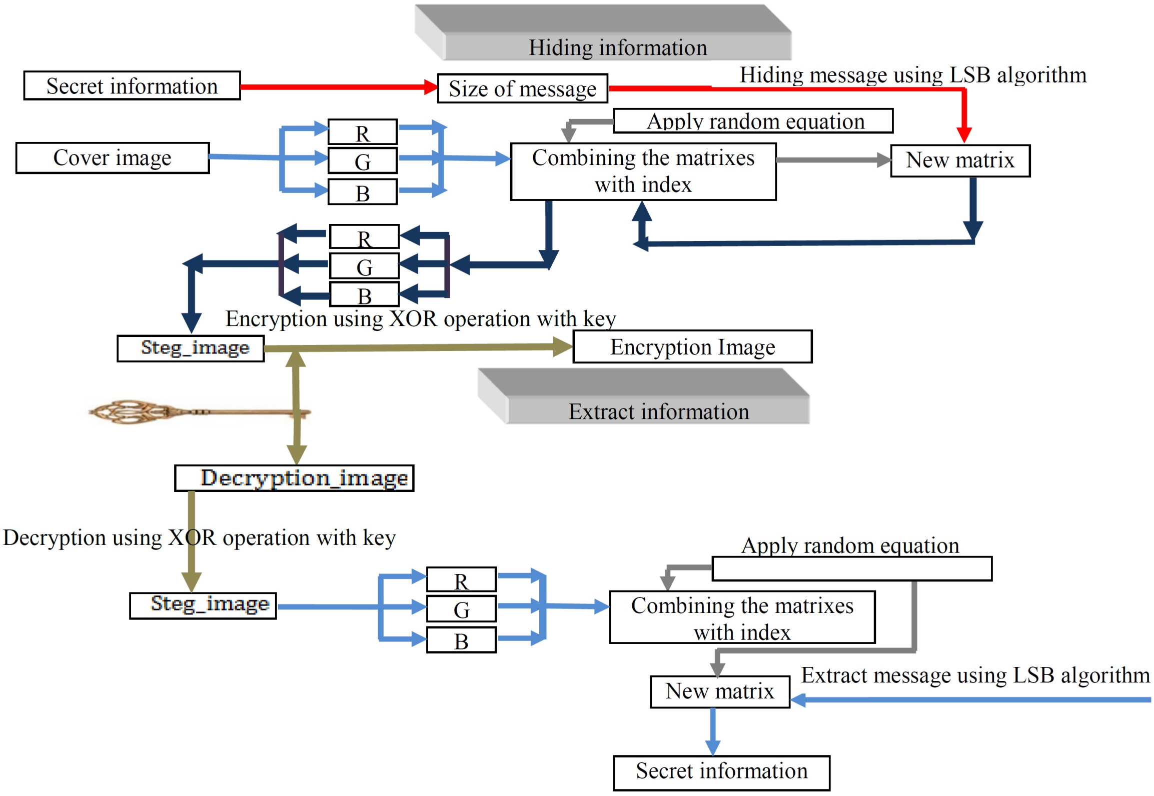


Figure 4: Data flow of the proposed system

L. To ensure that the media (image) is not significantly effective to human eyes after embedded message, many measurement values are calculates for image steganography such as histograms, mean square error (MSE), Hist_Err (Histogram Error normalization) and PSNR.

M. Choosing the secret key to encryption (Steg_image).

N. The extracting phasing begging to enter the secret key and decryption to obtain the (Steg_image) and continue from (D) to (F), using (LSB) to extract secret information.

O. The figure 4 explain this steps.

Front-page system

The front page of the programming which using of suggested system consist six faces and divided two cases:

Case 1 Embedded information and encryption (sender):

1. The first face containing the display the cover image, seed number and the secret message to seeking hiding.
2. The second face is display the output the cover image after hiding and the ratio of (MSE, PSNR, Histogram error).
3. The third face display encryption of the carrier image.

Case 2 Decryption and extract information (receiver):

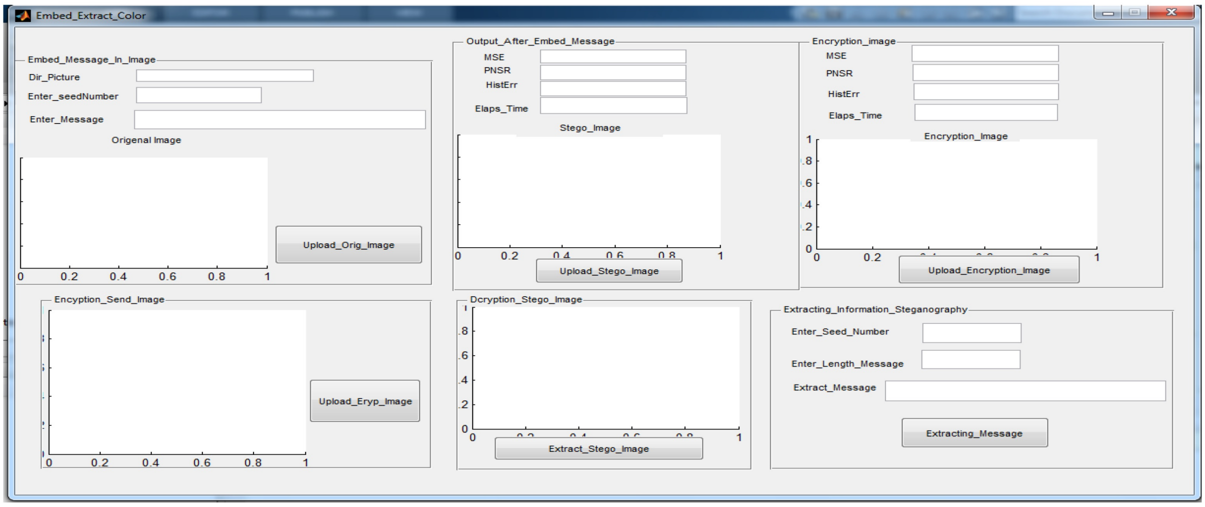


Figure 5:

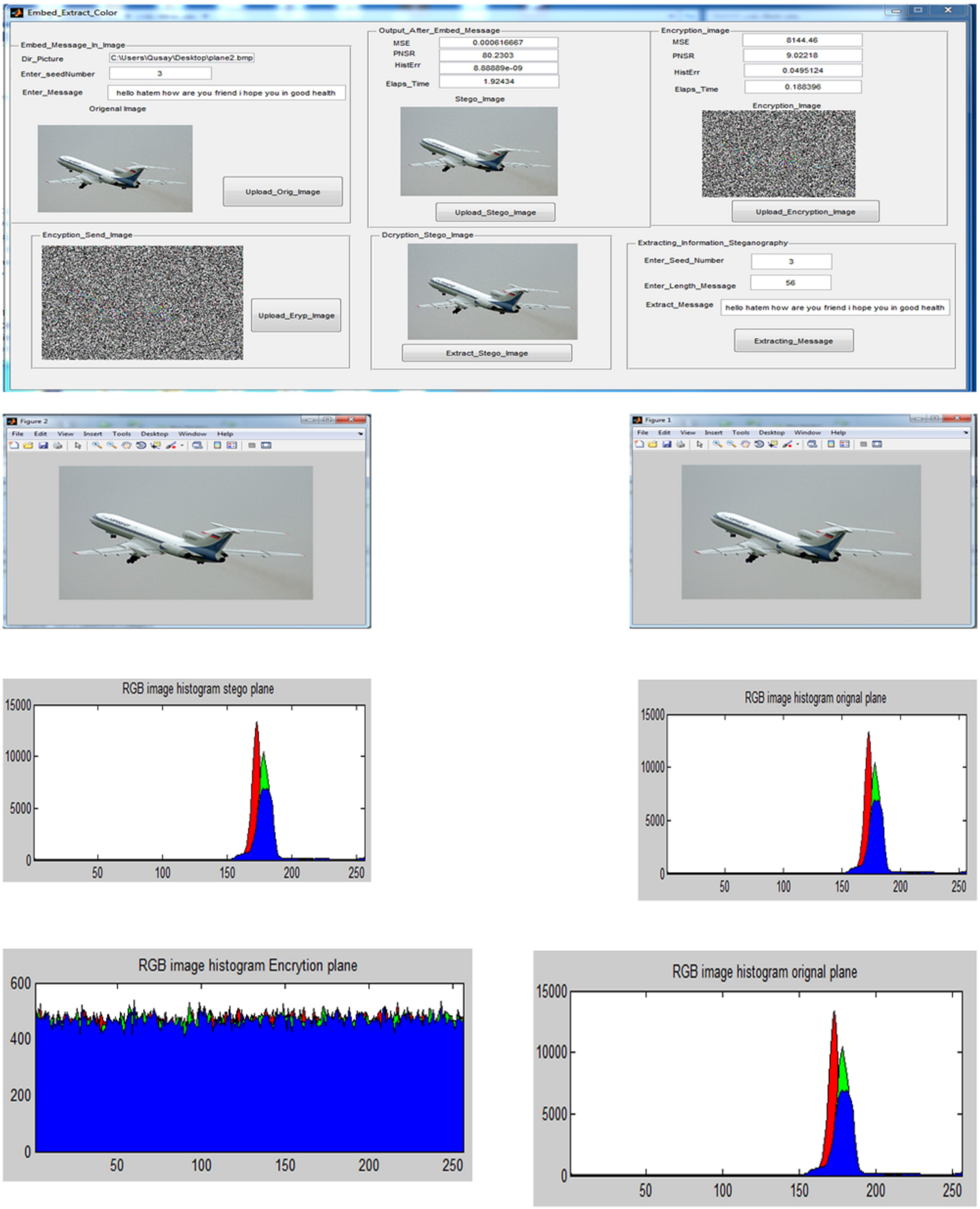
type	Mse_Hide	Pnsr_Hide	Hist_Error_hide	Time_Hide
Plane.bmp	0.000616667	80.2108	8.88889e-09	1.92434
type	Mse_Encryp	Psnr_Encryp	Hist_Error_Encryp	Time_Encryp
Plane.bmp	8144.46	9.02218	0.0495124	0.188396

1. The first face display decryption of image send.
2. The second face decryption image carrying information.
3. The third face it is the extract secret information after entering the seed number and length of message.

The front page of system explaining in figure 4 and the executed of the suggested system explained in figure 5 and figure6.

10. Conclusions

1. The encoding LSB is a good way to implement Steganography.
2. By the view the original image and Steg_image is difficult to characteristic deference between them.
3. The hacker jobs are being more and more difficult to access the hiding secret message.
4. Using the random method of the pixel cover media support the trust the hacker can't to access the secret message.
5. Using encryption to the carrier image and key increase difficult to access the secure information.
6. The use of steganography technique, randomization and cryptography is a coherent force to protect information from hackers.
7. The destination he need only key to decryption of Steg_image, seed number and length of secret message.



Dir_Picture C:\Users\Qusay\Desktop\plane2.bmp

Enter_seedNumber 3

Enter_Message hello hatem how are you friend i hope you in good health

MSE 0.000616667

PNSR 80.2303

HistErr 8.88889e-09

Elaps_Time 1.92434

MSE 8144.46

PNSR 9.02218

HistErr 0.0495124

Elaps_Time 0.188396

Enter_Seed_Number 3

Enter_Length_Message 56

Extract_Message hello hatem how are you friend i hope you in good health

Histogram Encryption Plane

Histogram Original Plane

Figure 6:

References

[1] A.S. Abdulbaqi, A.J. Obaid and A.H. Mohammed, *ECG signals recruitment to implement a new technique for medical image encryption*, J. Discrete Math. Sci. Crypt. 24(6) (2021) 1663–1673.

[2] A.M. Abdullah and R.H. Hama, *New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm*, Int. J. Comput. Appl. 143(4) (2016).

[3] Z.J. Ahmed, *Selective Watermarking Based on Interframe coding and Mean Modulation for Sprite Blocks*, M.Sc. Thesis College of Science, Baghdad University, 2014.

[4] O.M. Al-hazaimeh, *Hiding data in images using new random technique*, IJCSI 9(4) (2012).

[5] W.T. Ali and A.S. Hamed, *Data hiding using steganography and cryptography techniques*, Int. J. Mechat. Elect. Comput. Tech. 8(30) (2018) 3988–4001.

[6] M.M. Amin, M. Salle, S. Ibrahim, M.R. Katmin and M.Z.I. Shamsuddin, *Information hiding using steganography*, 4th National Conference of Telecommunication Technology, NCTT 2003 Proceedings, (2003) 21–25.

[7] J. Banks, J. Carson, B. Nelson, D. Nicol, *Discrete-event System Simulation*, Pearson Education International Series in Industrial and System Engineering, Third Edition, 2002.

[8] A. Cheddad, J. Condell, K. Curran and P.M.C. Kevitt, *Digital steganography survey and analysis of current method*, Signal Proces. 90(3) (2010) 727–752.

[9] R. Goyal and N. Kumar, *LSB based digital watermarking technique*, Int. J. Appl. Innov. Engin. Manag. 3(9) (2014).

[10] R. Hiral, S.S. Mahendra and K.S. Sanjay, *Design and implementation of image encryption algorithm by using block based symmetric transformation algorithm (hyper image encryption algorithm)*, Int. J. Comput. Tech. Elect. Engin. 1(3) (2011).

[11] K. Kadam, A. Koshti and P. Dunghav, *Steganography using least significant bit algorithm*, Engin. Res. Appl. 2(3) (2012) 338–341.

[12] S. Katzenbeiss, F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, Computer Security Series, Boston-London, 2000.

[13] D.H. Lehmer, *Proceedings of a Second Symposium on Large-Scale Digital Calculating Machinery*, Harvard University press, Cambridge, MA, 1951.

[14] A.J. Oabid, S. AlBermany and N.O. Alkaam, *Enhancement in S-Box of BRADG Algorithm*, In: V. Solanki, M. Hoang, Z. Lu and P. Pattnaik, *Intelligent Computing in Engineering*, Advances in Intelligent Systems and Computing, 1125, Springer, Singapore, 2020.

[15] F.A.P. Pititcolas, R.j. Anderson and M.G. Kuhn, *Information hiding: A survey*, Proc. IEEE, Special Iissue on Protection of Multimedia Content 87(7) (1999) 1062–1078.

[16] K. Priya, *Steganography techniques used to hide the information*, IOSR J. Comput. Engin. 20(6) (2018) 16–19.

[17] M. Qureshi, *Cryptography: A Silent Weapon for Encryption/Decryption of Data*, https://www.linkedin.com/pulse/cryptography-silent-weapon-encryptiondecryption-data-qureshi, (2018).

[18] R. Shanthakumari, E.M.R. Devi, R. Rajadevi and B. Bharaneeshwar, *Information hiding in audio steganography using LSB matching revisited*, J. Phys. Conf. Ser. IOP 1911(1) (2021) 012027.