Improve The Security of Confidential Messages by Combining Cryptography and Image Steganography

Graduation project submitted to Al-Furat Al-Awsat Technical University

Engineering Technical College - Najaf

Communications Techniques Engineering Department

By

Zeina Amer Hadi

Yasser Mohammad Jawad

Tabarak Hashem Mohammad

Zahraa Nasser Shareef

Supervised By

Assist. L. Huda Hussein Abed

Abstract

Cryptography and steganography are two issues in security systems. Cryptography scrambles the message to be incomprehensible while steganography shrouds the message to be invisible. Therefore, encryption of any private data before concealing it in the cover object will provide twofold security. In this project, a secure steganographic algorithm based on cover image encryption and Vigenère cipher is proposed, where the secret message is encrypted using Vigenère cipher then the cover image is encrypted using the logical XOR operation. After that, the encrypted form of the ciphered message is embedded within the encrypted cover image using the LSB algorithm in the spatial domain. The simulation consequence illustrates that the scheme provides better protection for confidential messages.

1. Introduction

The transfer of important and confidential data in our time via the internet has become one of the biggest challenges due to the development in technology as well as the accumulation of experience over the years among those interested [1]. Cryptography and steganography provide most significant techniques for information security [2].

Cryptography is a technique of transforming and transmitting private data in an encoded way so that only authorized and intended users can obtain or work on it. The word cryptography is derived from the Greek words “Κρυπτο” which means hidden or secret [3].

Steganography is the art and science of invisible communication. It is accomplished by hiding information in other information, thus hiding the existence of the information. Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning writing. Steganography and cryptography are techniques used to protect information from unwanted parties but neither technology alone is perfect. Once the presence of hidden information is revealed or suspected, the reason of steganography is partly defeated. The strength of steganography increases by combining it with cryptography [4].

2. Digital Image Steganography

A digital image is finite collection of elements called pixels; each of pixels is having a particular location and value [5]. The most popular medium used for hiding secret data is image files because of their high capacity and easy availability over the internet. At the sender's side, the image used for embedding the secret message is called cover image, and the secret information that needs to be protected is called a message. As soon as data are embedded using some appropriate embedding algorithm, then it is called stego-image. This stego-image is transferred to the receiver, and the receiver extracts out the secret message using extraction algorithm [6].

The main processes of a steganographic system can be graphically represented as in Fig.1 [7].

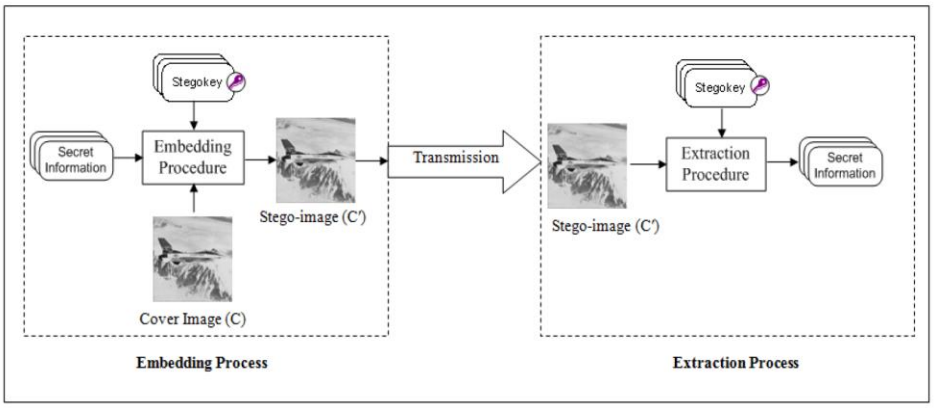

Fig.1: A general steganography system [7]

A general steganography system showing the embedding and the extracting processes. C denotes to the cover image and C' denotes to the stego-image (the cover C after embedding the secret information).

3. Least Significant Bit (LSB) Technique

The least interesting bit is a basic method for inserting data in the image file. Simple steganography requires embedding the bits of the message in the least important bits of the image [8]. In a gray scale image, each pixel is represented in 8 bits. The last bit in a pixel is called as least significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the

encryption process increases the time complexity, but at the same time provides higher security also [9].

Consider an 8-bit grayscale bitmap image, where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray values:

01010010

01001010

10010111

11001100

11010101

01010111

00100110

01000011

To hide the letter **H** whose binary value of ASCII code is 01001000, we would replace the LSBs of these pixels to have the following new values:

01010010

01001011

10010110

11001100

11010101

01010110

00100110

01000010

4. Vigenère Cipher

The Vigenere cipher is a polyalphabetic substitution cipher in which each letter of the alphabet is replaced with a different letter according to a table of key values [10]. It can be expressed as follows [11]:

$$\text{Encrypt } (c_i) : E(p_i) = (p_i + k_i)\ mod\ 26$$
$$\text{Decrypt } (p_i) : D(c_i) = (c_i - k_i)\ mod\ 26$$

where:

p_i is plaintext; c_i is ciphertext. *And* k_i is key.

For example, to encrypt the message COMPUTING GIVES INSIGHT with the keyword LUCKY. Vigenère proceed by repeating the Keyword as many times as needed above the Message as follow Fig. 2 [12].

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T

Fig.2: Message and Key example [12]

5. Image Encryption

Image encryption techniques play a significant role in multimedia applications to secure and authenticate digital images. Fig.3 illustrates the general framework of image encryption techniques. An input image that needs to be encrypted is called a plain-image and encrypted image is known as a ciphered image. The plain and ciphered images are represented by P and C, respectively. The image encryption techniques can be divided as symmetric and asymmetric techniques. In case of symmetric image encryption, the encryption and decryption keys are same, i.e., EK = DK. The keys are to be kept secret during the communication. When different keys are used for encryption and decryption, the image encryption is known as asymmetric image encryption [13].

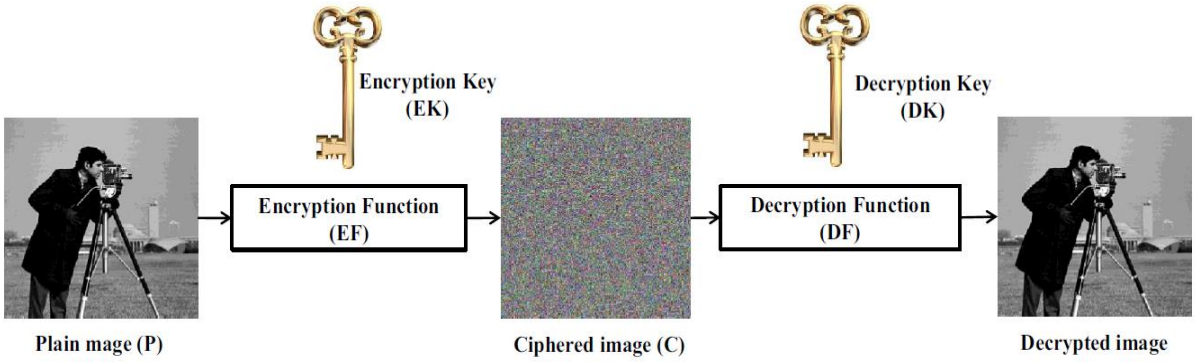

Fig. 3: Generic framework of image encryption techniques [13]

6. The Proposed Method

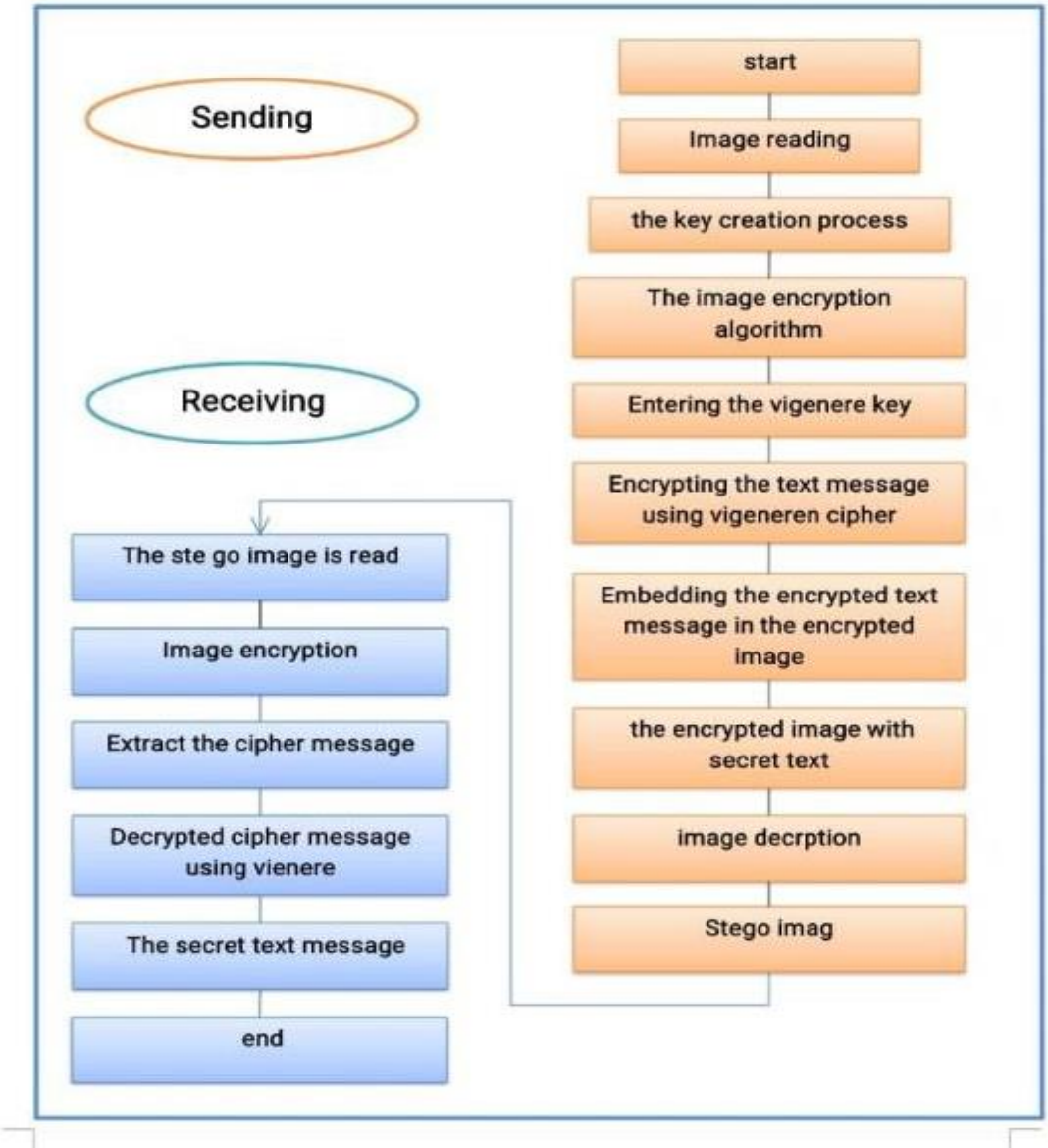

Fig. 4: Steps of the proposed method

7. Simulation Results and Discussions

The major goal behind this study is to conceal a large quantity of information with a high security and preserve the image quality at the same time. The image quality and the payload of data that are inserted within the image and the robustness of the scheme to face the electronic assaults and the security are the most important factors to evaluate the methods of steganography.

Mean Square Error (MSE) is utilized to quantify the average of mean square mistake among pixels of the cover image and stego-Image whose value is calculated by utilizing Equation below

$$MSE = \sum_{i=1}^{M*N} (g_i - g_i')^2 / (M * N)$$

Where gi is a pixel value before inserting the information within the image and gi' is a pixel value after inserting the information within the image, while, M*N denotes the size of image. The lower value of images MSE means better quality of image [14].

The visual quality of the sending side exhibits that the cover image and the stego image are similar, as demonstrated in Fig. 5.

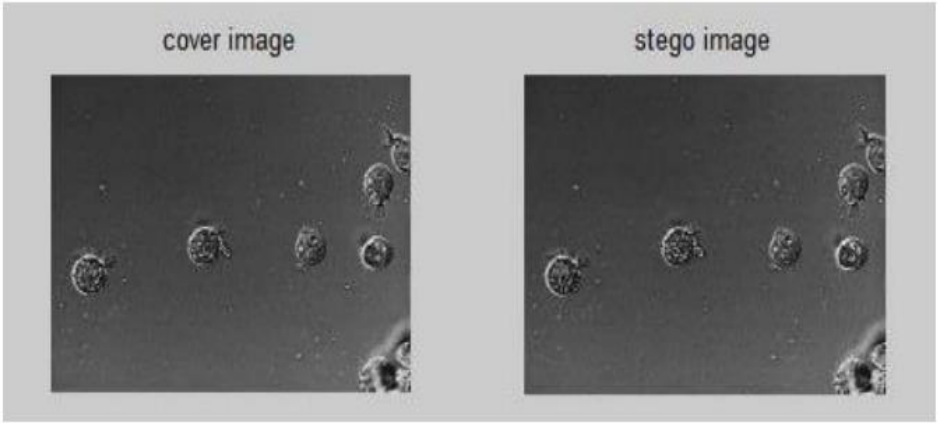

Fig. 5: Grayscale cover image with stego image

MSE value is **9.1146e-05** very small which means the proposed method is good in hiding the information inside the image and preserving the image quality. Table 1 shows the secret message before and after encryption, and the key used for the encryption process.

Table 1: The secret message before and after encryption with the encryption key

Text before encryption	welcome
Text After encryption	nextoyv
Key	ram

Histogram analysis is an important image analysis method, which can reflect the frequency distribution of pixel values in the image [15]. Fig.6 shows that encrypted images have completely different histograms against the original

images. It shows that the encrypted image has no relationship with the original image. Therefore, the proposed image encryption algorithm can resist histogram analysis attacks.

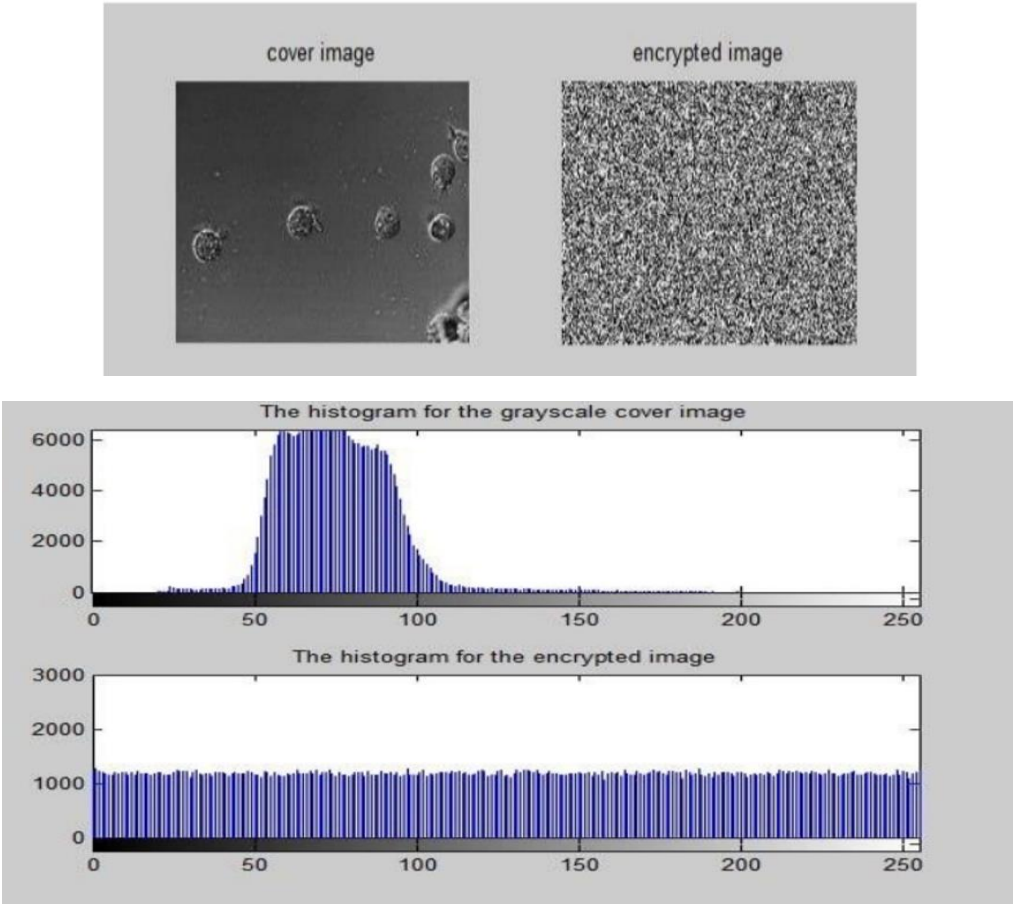

Fig. 6: Histograms for the grayscale cover image and the encrypted image

8. Conclusion

This project offers a secure method to hide confidential messages with multiple levels of security: firstly, the secret message is encrypted using Vigenère cipher. Secondly, the cover image is encrypted using the logical XOR operation after creating an array containing the keys of the same size as the cover image to provide another level of security. Thirdly, the encrypted form of the ciphered message is embedded within the encrypted cover image using the LSB algorithm in the spatial domain. The proposed scheme creates better camouflage to evade intruder attention and realize better performance in terms of measurement the steganographic system as demonstrated according to the performance analysis.

References

[1] Halboos, Estabraq Hussein Jasim, and Abbas M. Albakry. "Hiding text using the least significant bit technique to improve cover image in the steganography system." Bulletin of Electrical Engineering and Informatics 11.6 (2022): 3258-3271.

[2] AL-Shaaby, Ahmed Ali, and Talal AlKharobi. "Cryptography and steganography: new approach." Transactions on Networks and communications 5.6 (2017): 25.

[3] Agrawal, E., and J. Jain. "A Review on Various Methods of Cryptography for Cyber Security." Int. J. Recent Innov. Trends Comput. Commun 6.7 (2018): 5.

[4] Shelke, Falesh M., Ashwini A. Dongre, and Pravin D. Soni. "Comparison of different techniques for Steganography in images." International Journal of Application or Innovation in Engineering & Management 3.2 (2014): 171-176.

[5] Jagetiya, Anurag, and C. Rama Krishna. "Digital Image Steganography." CSI Communication 38.3 (2014): 22-25.

[6] Joshi, Kamaldeep, Swati Gill, and Rajkumar Yadav. "A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image." Journal of Computer Networks and Communications 2018 (2018).

[7] Atawneh, Samer, and Putra Sumari. "Hybrid and Blind Steganographic Method for Digital Images Based on DWT and Chaotic Map." J. Commun. 8.11 (2013): 690-699.

[8] Voleti, Lasya, et al. "A secure image steganography using improved Lsb technique and vigenere cipher algorithm." 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). IEEE, 2021.

[9] Singh, Arun Kumar, Juhi Singh, and Harsh Vikram Singh. "Steganography in images using lsb technique." International Journal of Latest Trends in Engineering and Technology (IJLTET) 5.1 (2015): 426-430.

[10] Nezami, Zahid Iqbal, et al. "An efficient and secure technique for image steganography using a hash function." PeerJ Computer Science 8 (2022): e1157.

[11] Rojali, and Afan Galih Salman. "Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary-based compression methods." AIP Conference Proceedings. Vol. 1867. No. 1. AIP Publishing LLC, 2017.

[12] Hlaing, Htike Ayar, and Soe Soe Aye. Data Encryption by Using Vigenere Algorithm with Stegonargaphic Technique. Diss. MERAL Portal.

[13] Kaur, Manjit, and Vijay Kumar. "A comprehensive review on image encryption techniques." Archives of Computational Methods in Engineering 27 (2020): 15-43.

[14] Younus, Zeyad Safaa, and Mohammed Khaire Hussain. "Image steganography using exploiting modification direction for compressed encrypted data." Journal of King Saud University-Computer and Information Sciences 34.6 (2022): 2951-2963.

[15] He, Yi, et al. "A new image encryption algorithm based on the OF-LSTMS and chaotic sequences." Scientific reports 11.1 (2021): 6398.