An Efficient Data Security System Based on LSB Steganography and Symmetric Key Encryption

Seddeq E. Ghrare[1], Khaled H. Algharari[2], Ahmad R. Kobaiz[3]

[1] *Faculty of Engineering, University of Aljabal Algharbi, Libya, seddeq@jgu.edu.ly*
[2] *Faculty of Education, University of Aljabal Algharbi, Libya, kh_algharari@yahoo.com*
[3] *Dept. of Electrical Engineering, the Higher Institute of Polytechnics, Libya, ahkhobaiz@yahoo.com*

Received 16 January 2018; accepted 10 March 2018

Abstract

The rapid growth of internet and ICT has led to increase the amount of exchanged information over the internet and as a result, the research of information security technique is becoming more and more important. Various methods including cryptography, steganography, coding, etc. are used for protecting important information. Cryptography is the process of changing the original information into unreadable from, while Steganography is the process of hiding secret information in a cover media such as image or sound. In this paper, a new image steganography and encryption scheme is proposed. First, the secret message is hidden inside a cover image, and then the resulted steganographic image is encrypted. The main advantages of the proposed scheme are represented in the use of steganography and cryptography techniques respectively providing a high level of security since breaking cryptosystem depends on breaking its encryption and decryption key. The key is randomly generated in a form of binary matrix which makes it very hard even impossible to be broken. Experimental results show that the proposed scheme in this paper has a high security level and better image stego-image quality.

Keywords: Business Architecture, Enterprise Configuration, Application Layer, Mobile Enterprise Transition.

1. Introduction

Today security is the main concern about the transmission of information. Information security techniques can be classified into two main categories; Cryptography and Steganography. Cryptography consists of two subprocesses, which are Encryption and Decryption. Encryption is the process of converting the original information into an unreadable form using encryption key. Decryption is the process of recovering the encrypted information using decryption key. The strength of a cryptography process can usually be determined by how difficult it is to obtain the key value [1].

Steganography is the process of hiding secret information in a cover media so that the existence of the information is not apparent [2]. Techniques that are used for information hiding today include watermarking [3, 4] and steganography [5, 6, 22]. The major concern of watermarking is to protect the ownership of a digital content, while steganography is to embed secret messages into digital content so that the secret messages are not detectable. All digital media, such as digital images, videos and audio files, can be used to hide secret information. However, digital images are often used for steganography. This is because nature images usually have higher degree of redundancy, which are suitable to embed information without degrading the visual quality of the images. Moreover, images are widely used throughout the internet, which usually arouse little suspicion than other digital media [2].

In this paper, the secret information is first hidden in the cover image using Least Significant Bit (LSB) method at different bit positions, and then the resulted stego-image is encrypted in order to provide a high level security compared with that provided by LSB alone.

2. Cryptography Techniques

A cryptographic algorithm is a function used for both encryption and decryption processes. This function is dependent on a key value necessary for both encryption and decryption. The strength of a cryptographic algorithm can usually be determined by how difficult it is to obtain the key value [1].

There are two major types of cryptography techniques based on usage of keys. The first type is called symmetric key cryptosystems and these can be further divided into stream and block ciphers. Stream ciphers operate on a single byte of data, while block ciphers operate on groups of bytes. With these algorithms, keys used for encryption and decryption are the same. This requires that before sending a message, sender and receiver agree on the key [8]. Obviously, this requires the key be kept secret; anyone who knows the key can decrypt messages. Figure 1 shows a basic symmetric key encryption and decryption cryptosystem [7],[9].

On the hand, Asymmetric Key Cryptosystem, also called Public Key Cryptosystems, are designed so that the key used for encryption is different from the key used for decryption. The cryptosystems are called “Public Key” because the encryption key can be made public, so any person can use the encryption key to encrypt the information, but only a specific person with the corresponding decryption key can decrypt the information to its original form. The basic idea that led to Asymmetric Key Cryptography (AKC) was that keys could come in pairs of an encryption and decryption key and that it could be impossible to compute one key given the other. Figure 2 shows a basic asymmetric key encryption and decryption cryptosystem [10].

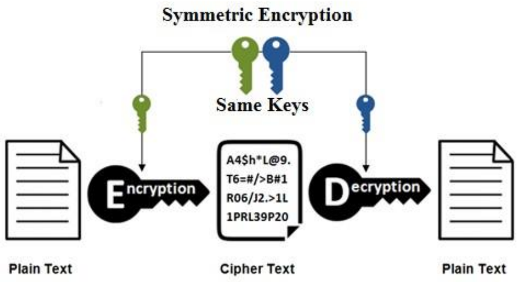

Figure 1. Symmetric Key Cryptosystem

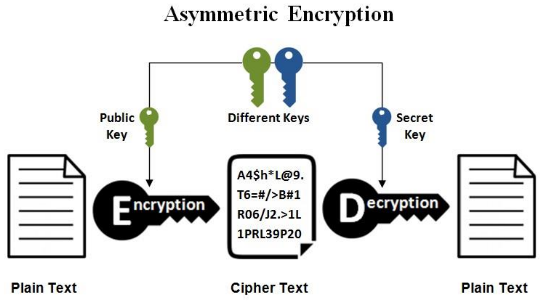

Figure 2. Asymmetric Key Cryptosystem

3. Steganography Techniques

Steganographic techniques can be classified based on the type of the cover media used to hide the secret information.

- Text-Based Steganography:

This involves anything from changing the formatting of an existing text, changing words within a text or generating readable texts. For example, a reformat of the text may destroy the information encoded in the text. Additionally, text messages can be stored in different formats such as HTML, Postscripts, or PDF; the change from one format to another might be harmful to the embedded messages. Text hiding techniques include: The Line-Shift Coding, the word shift coding, feature coding, syntactic techniques, semantic techniques, and cover generation techniques [11].

- Audio Steganography:

Like text files, sound files may be modified in such a way that they contain hidden information.

Such techniques embed data in sound files using the properties of the Human Auditory System (HAS). Examples of audio steganography techniques include least significant bit, phase coding and echo Hiding.[11,22]

- Image Steganography:

Compared to other types of steganography, image steganography has attracted extensive research as well as popular usability in recent years. This is due to the fact that huge amounts of data can be hidden without perceptible impact to the carriers and possibly because of the popularity of electronic images that have become widely available.

An early work on the image steganography is Least Significant Bit technique (LSB) [12, 13, 14]. This technique is simple in both the embedding and de-embedding (extracting messages) processes, but suffers several disadvantages. The recent advances in steganalysis have shown that LSB does not guarantee detestability, evidenced by the fact that they can be successfully attacked using statistical or even visual attacks [15,17, 22].

4. Proposed Scheme

The main steps of the proposed scheme are indicated in figure 3 and listed as follows:

- Convert the original secret text into ASCII then into binary form.
- Insert the converted secret text into cover image using LSB method, the resulted image is called stego image.
- Encode the stego image; the resulted encoded image will be in binary form.
- Generate an encryption and decryption key.
- Encrypt the encoded stego image using the encryption key.

The reverse steps will be followed in order to extract the secret text. These steps are as follows:

- Generate a decryption key.
- Decrypt the received encrypted encoded image, the resulted image is the original encoded stego image.
- Decode the encoded stego image; the resulted image is the original stego image.
- Extract the secret text from the stego image.
- Convert the secret text into its original form.

Note that the encryption and decryption process of the stego image is performed using the same key.

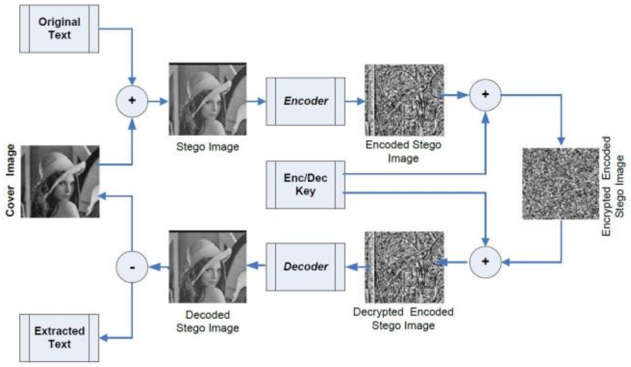

Figure 3. the main Steps of the Proposed Method

5. Evaluation of Image Quality

The quality of any processed mage is usually evaluated subjectively and objectively. Objectively MSE (Mean Square Error), and PSNR (Peak Signal to Noise Ratio) are the two most often used parameters to describe the quality of the image.

Mean Square Error depends strongly on the image intensity scaling. A mean squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks dreadful; but a MSE of 100.0 for a 10-bit image (pixel values in [0, 1023]) is barely noticeable.

PSNR is measured in decibels (dB). PSNR is a good measure of the distortion (noise) between the original image and the processed image. These two parameters can be calculated as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} (C(i,j) - S(i,j))^2$$

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

Where M, N are the image dimensions
C(i,j) is the cover (Original) image
S(i,j) is the stego image

Subjective evaluation depends on HVS (Human Visual System) and can be done by comparing the processed image with the original image.

6. Results Presentation

In this paper, five gray-level images “Lena”, “Baboon”, “Cameraman”, “Bird”, and “Moon” shown in Figure 4, were tested to show the effectiveness of our scheme. These images are 8 bits per pixel, grayscale; the size of the used test images is 256x256 and 512x512 pixels.

Figure 4. Test Images

The above test images were used as a cover to hide the secret information. Two secret messages of a size 3.9 KB and 39 KB were hidden. The resulted image that contains on the hidden message is called a stego-image which in turn is encrypted in order to provide more protection to the secret message. The following figures show the original image, stego image, encrypted stgo image and the recovered stego image.

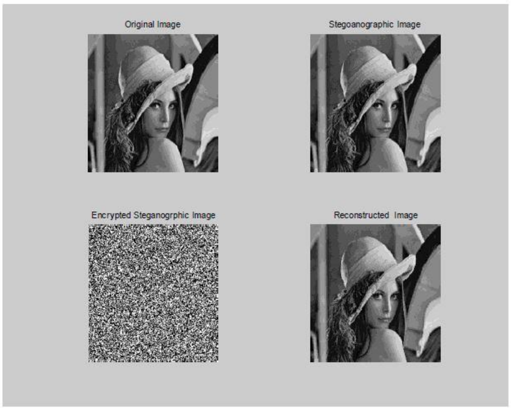

Figure 5. Original image, Stego image, Encrypted stgo image and Recovered stego image. (Lena)

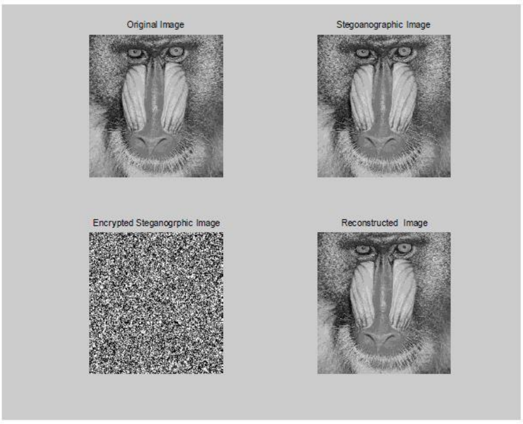

Figure 6. Original image, Stego image, Encrypted stgo image and Recovered stego image. (Baboon)

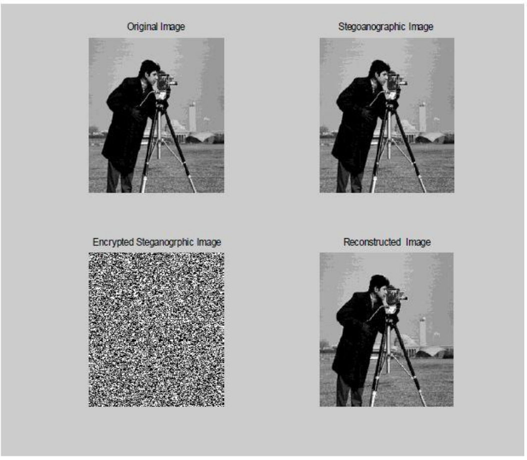

Figure 7. Original image, Stego image, Encrypted stgo image and Recovered stego image. (Cameraman)

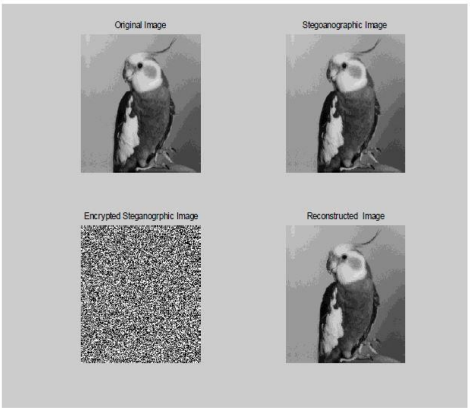

Figure 8. Original image, Stego image, Encrypted stgo image and Recovered stego image. (Bird)

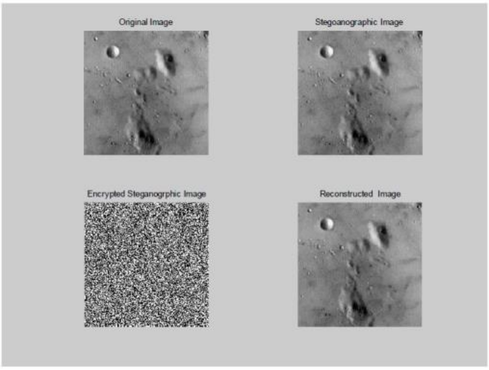

Figure 9. Original image, Stego image, Encrypted stgo image and Recovered stego image. (M00n)

The quality of the stego-image is evaluated objectively and subjectively. Objectively the MSE and PSNR are calculated using the above equations. The obtained MSE and PSNR are shown in Table 1 and Table 2.

TABLE 1. PSNR AND MSE OF STEGO-IMAGE EMBEDDED WITH 3.9 KB INFORMATION

Image	LSB1		LSB2		LSB3		LSB4	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Lena 256x256	54.4978	0.2327	48.4440	0.9377	42.4734	3.7080	36.4368	14.8867
Bird 256x256	54.5060	0.2322	48.3998	0.9473	42.4711	3.7100	36.3791	15.0859
Moon 256x256	54.4838	0.2334	48.4874	0.9284	42.4059	3.7661	36.3895	15.0498
Lena 512x512	66.5140	0.0585	60.5338	0.2318	54.5155	0.9268	43.3558	12.1049
Baboon 512x512	66.5387	0.0582	60.5298	0.2320	54.4952	0.9312	48.4627	3.7349

TABLE 2. PSNR AND MSE OF STEGO-IMAGE EMBEDDED WITH 39 KB INFORMATION

Image	LSB1		LSB2		LSB3		LSB4	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
Lena 512x512	60.3919	0.2395	54.3824	0.9556	48.3952	3.7933	42.3276	15.3384
Cameraman 512x512	60.4123	0.2384	54.4189	0.9477	48.3784	3.8080	42.1489	15.9827
Baboon 512x512	54.3907	0.9538	48.3662	3.8187	42.3428	15.2847	36.0912	64.4786

Subjectively, in our case, when the secret message is hidden in the first LSB, second LSB, third LSB and forth LSB, it is very hard to distinguish the stego-image from the cover image, which means that the visual quality is very good. The following figures show a comparison between the original cover images and their corresponding stego images using the first LSB through the fourth LSB.

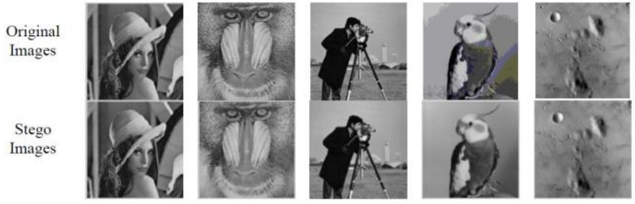

Figure 10. Cover Images and Corresponding Stego-Images using First LSB

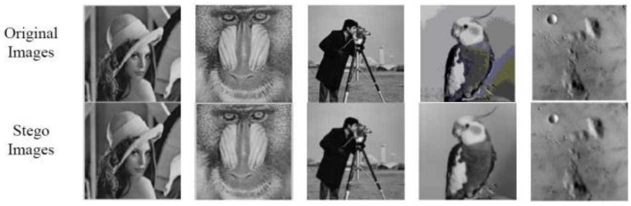

Figure 11. Cover Images and Corresponding Stego-Images using Second LSB

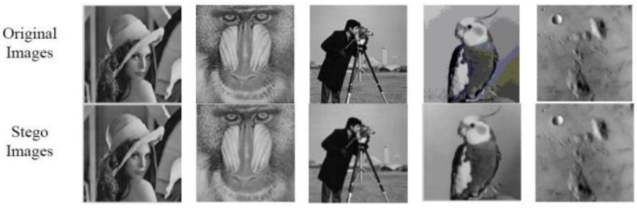

Figure 12. Cover Images and Corresponding Stego-Images using Third LSB

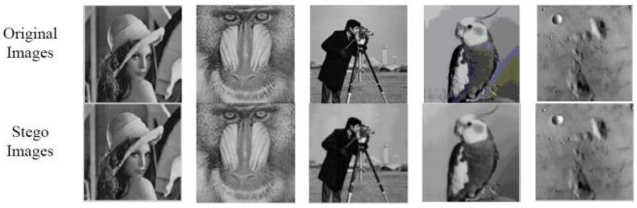

Figure 13. Cover Images and Corresponding Stego-Images using Forth LSB

The quality of the stego-image is degraded when the secret message is hidden in the fifth LSB through eighth LSB. The following figure shows the effect of hidden message when it is hided in fifth LSB through the last LSB which is represents the MSB.

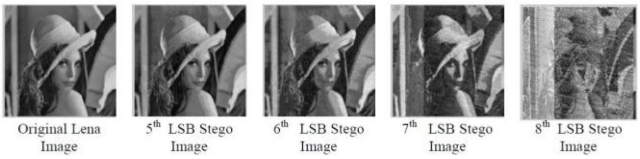

Figure 14. Cover Images and Corresponding Stego-Images using Forth LSB

7. Conclusion

In this paper, a new image steganography and encryption scheme is proposed. Two different secrete messages of different sizes are hidden into a set of cover images. The cover images are of 256x256 and 512x512 gray scale images. The resulted stego images are then encrypted to provide more protection to the secrete message. The main advantages of the proposed scheme are represented in the use of steganography and cryptography techniques respectively providing a high level of security since breaking cryptosystem depends on breaking its encryption and decryption key. The key is randomly generated in a form of binary matrix which makes it really hard even impossible to be broken. Experimental results show that the proposed scheme in this paper has a high security level and better image stego-image quality.

References

[1] M. B. Pramanik, “implementation of cryptography technique using columnar transposition”, international journal of computer applications, (0975-8887) – Jan. 2014.

[2] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, “Information Hiding—A Survey,” Proceedings of the IEEE, special issue on protection of multimedia content, 87(7), 1999, pp. 1062–1078.

[3] Shieh, J. M., Lou, D. C. and Chang, M. C., “A Semi-blind Digital Watermarking Scheme Based on Singular Value Decomposition,” Computer Standards & Interfaces, Volume 28, Issue 4, 2006, pp. 428440.

[4] Lin, P. L., Hsieh, C. K. and Huang, P. W., “A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery,” Pattern Recognition, Volume 38, Issue 12, 2005, pp. 2519- 2529.

[5] Lin, C. C. and Tsai, W. H., “Secret Image Sharing with Steganography and Authentication,” Journal of Systems and Software, Volume 73, Issue 3, 2004, pp. 405-414.

[6] Chang, C. C., Chen, T. S., and Chung, L. Z., “A Steganographic Method Based upon JPEG and Quantization Table Modification,” Information Sciences, 2002, pp. 123-138.

[7] J. J. Amodar and R. W. Green, “Symmetric key block cipher for image and text cryptography”, international journal of Imaging and Technology, June 2005.

[8] K. R. Saraf, V. P. J and A. K. Mishra, “Text and Image Encryption decryption using advanced Encyption standard”, international journal of Emerging trends and technology in computer science, vol.3, Issue. 3, may-June 2014.

[9] William Stallings. 2005. “Cryptography and Network Security” , 4th edition Principles and Practice

[10] Vineet Sukhraliya1, Sumit Chaudhary2, Sangeeta Solanki3, “Encryption and Decryption Algorithm using ASCII values with substitution array Approach”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[11] Hassan Mathkour. Batool Al-Sadoon, Ameur Touir, A New Image Steganography Technique” , 2008 IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, October 12-17, 2008, Dalian, China.

[12] Johnson, N.F. and S. Jajodia. "Exploring Steganography: Seeing the Unseen." IEEE Computer Mag., February 1998.

[13] Kessler, G. “An Overview of Steganography for the Computer Forensics Examiner “, Computer &

[14] Digital Forensics Program, Champlain College, Burlington, Vermont, February 2004

[15] Bennett, K. “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text“ Technical Report, Center for Education and Research in Information Assurance and Security (CERIAS), 2004.

[16] Westfield, A., and A. Pfitzmann. “Attacks on Steganographic Systems - Breaking the Steganographic

[17] Utilities EzStego, Jsteg, Steganos, and Stools - and Some Lessons Learned,” Lecture Notes in Computer Science, 1768: 61-75 (2000).

[18] Fridrich ,J, M. Goljan, and R. Du, “Detecting LSB steganography in color and grayscale images,” IEEE Multimedia Special Issue on Security, pp. 22–28, October-November 2001.

[19] Avcibas, I. , N. Memon, and B. sankur, “Steganalysis using image quality metrics.” Security and Watermarking of Multimedia Contents, San Jose, Ca., Feruary 2001.

[20] El-Ebiary, Y. A. B., Al-Sammarraie, N. A., Al Moaiad, Y., & Alzubi, M. M. S. (2016, October). The impact of Management Information System in educational organizations processes. In *e-Learning, e-Management and e-Services (IC3e), 2016 IEEE Conference on* (pp. 166-169). IEEE.

[21] Hilles, S., & Maidanuk, V. P. (2014). Self-organization feature map based on VQ components to solve image coding problem. ARPN Journal of Engineering and Applied Sciences. Vol. 9,№ 9: 1469-1475.

[22] Hilles, S. M., & Hossain, M. A. (2017). English Steganography Techniques: A Review Paper. International Journal of Contemporary Computer Research, 1(3), 22-28.