A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY

Saleh Saraireh

Department of Communications and Electronic Engineering, Philadelphia University, Amman,Jordan.

saleh_53@yahoo.com

ABSTRACT

The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography and steganography can be combined. This paper proposes a secure communication system. It employs cryptographic algorithm together with steganography. The jointing of these techniques provides a robust and strong communication system that able to withstand against attackers. In this paper, the filter bank cipher is used to encrypt the secret text message, it provide high level of security, scalability and speed. After that, a discrete wavelet transforms (DWT) based steganography is employed to hide the encrypted message in the cover image by modifying the wavelet coefficients. The performance of the proposed system is evaluated using peak signal to noise ratio (PSNR) and histogram analysis. The simulation results show that, the proposed system provides high level of security.

KEYWORDS

Steganography, Cryptography, DWT, Filter bank, PSNR.

1. INTRODUCTION

The security of data transmission is a vital problem in communication networks. A communication system is reliable as long as it provides high level of security. Usually, users exchange personal sensitive information or important documents. In this case; security, integrity, authenticity and confidentiality of the exchanged data should be provided over the transmission medium. Nowadays, internet multimedia is very popular; a significant amount of data is exchanged every second over a non secured channel, which may not be safe. Therefore, it is essential to protect the data from attackers. To protect the data; cryptography and steganography techniques can be used.

Cryptography is the science of keeping the transmitted data secure. It provides data encryption for secure communication [1]. The encryption process is applied before transmission, and the decryption process is applied after receiving the encrypted data. Steganography is the science of writing hidden messages inside a different digital content; it conveys the data by concealing it in other medium such as image or audio which is called the cover object. The information hiding process is applied before transmission and the extraction process is applied after receiving.
The main difference between cryptography and steganography based on the existence of the secret message. Cryptography encrypts the message and transmits it; anyone can view the encrypted message, but is very difficult to be understood, especially if it has been encrypted with strong cryptographic algorithm. Steganography conceals the secrete message existence by hiding

DOI : 10.5121/ijcnc.2013.5310

it in a cover object. The cover object can be classified as Text-based Steganography in which the secret message is embedded in a text file, audio Steganography to hide the secret message in audio signal and image steganography in which the secret data is embedded in an image.

Cryptographic algorithms are classified as symmetric key algorithm and public key algorithm. Symmetric key algorithm uses the same key for encryption and decryption, while public key algorithm uses different keys for encryption and decryption. Steganography system can be implemented using two techniques. Firstly, the spatial domain based steganography, where the least significant bits (LSB) of the cover object is replaced by the secret message bits. Secondly, the transform domain based steganography; in this case, the secret message is embedded with the coefficient of the cover object. The most common transform domains are discrete Fourier transform and discrete wavelet transform.

To improve the reliability of the communication system; cryptography and steganography can be combined to implement a robust and secure system; in this case, the encryption and hiding are achieved in the transmitter, while the extraction and decryption are achieved in the receiver.
There are some issued that should be addressed in the designing of a steganography system [2]:

a) Invisibility: This means that the stego image should not be noticed by human.
b) Security: The steganography process should provide high level of security, therefore, the stego image should be very close to the original cover image, and the attacker could not detect the hidden information. Peak signal to noise ratio (PSNR) is employed to measure the difference between the cover image and the stego image. PSNR can be calculated using:

$$PSNR=10\log\frac{L^2}{MES} \qquad 1$$

L is the maximum value the samples and MES is the mean error squre.

The remainder of this article is organized as follows. The related work is introduced in section 2. Section 3 presents the proposed system. The experimental results and discussions are presented in section 4 and the paper is concluded in section 5.

2. RELATED WORK

In [3] a steganographic scheme was proposed, it uses human vision sensitivity to hide secret bits. To make this, the secret data firstly are converted into a series of symbols to be embedded in a notation system with multiple bases. In this case, the particular bases used are determined by the degree of local variation of the pixel magnitudes in the host image. A modification to the least significant bit matching (LSBM) steganography was introduced in [4]. This modification provides the desired choice of a binary function of two cover pixels rather than to be random as in LSBM. To increase the level of security, a combined data encoding and hiding process was proposed in [5]. This process was used to overcome the problem of image color changes after the embedding process. The LSB steganography technique was developed in [6], it based on embedding the secret message into the sharper edge regions of the image to ensure its resistance against image steganalysis based on statistical analysis. A novel image steganography was proposed in [7], it is based on integer wavelet transform [IWT], it is used to embed multiple secret images and keys in color cover image. A quantization based steganography system presented in [8] embedded the

secret message in every chrominance of a color image to increase the hiding capacity. DWT based frequency domain steganographic technique was proposed in [9], the data is hidden in horizontal, vertical and diagonal components of the sub – image. In [10] a secret data communication system was presented, it employs RSA with asymmetric keys and AES with symmetric key to encrypt the data, after that the encrypted data is embedded into the cover image using smart LSB pixel mapping and data rearrangement method. In [11] and [12] two secure communication systems were proposed to be used for voice over IP (VOIP) applications. LSB based steganography was employed to hide the information over an audio cover signal. An extended version of SHA-1 (Secure Hash Algorithm) was introduced in [13]; this system can be used to encrypt two dimensional data such as image. It is developed to increase the resistance of image based steganography against the attackers and hackers. A chaotic signal was employed in [14] for image steganography, which presents a scattering format for the embedded data through the cover image. A high capacity and security steganography using discrete wavelet transform (HCSSD) was developed in [15]; the wavelet coefficients for the cover image and the payload image were fused to obtain a single image.

3. PROPOSED SYSTEM

The main objective of this paper is to introduce a secure communication system that employs both cryptography and steganography to encrypt and embed the secret message to be transmitted over a non secure channel. In this system, the encryption process is achieved using the filter bank cipher, which presents a high speed and level of security. The embedding process is achieved using the discrete wavelet transform based steganography. The proposed system consists from four stages as shown in Figure 1. Note that the main stages are encryption, embedding, extraction and decryption. The following algorithm describes these stages.

Algorithm

Input: Embed the message.
Output: Message is embedded safely in an image and reconstructed properly.

Begin

1. Message.
2. Encrypting message.
3. Implementing DWT based steganography
4. Embedding data.
5. Stego image.
6. Extraction of embedded message.
7. Encrypted message generation.
8. Decryption.
9. Original Message.

End

3.1 Encryption and Decryption Process

The cryptographic algorithm used in this paper is filter bank cipher over Galois field (GF (2^8)) [16]. In this cipher the encryption process consists from two layers. Firstly, the diffusion layer is represented by the analysis filter bank to introduce a high diffusion rate. Secondly, the substitution layer which is represented by the lifting scheme over GF (2^8) to add the required nonlinearity to increase the resistivity of the cipher against the differential and linear cryptanalysis attacks. The lifting scheme is shown in Figure 2, where S is the inverse function over GF (2^8). The filter bank cipher consists from two rounds to improve its security. Figure 3

shows one round filter bank cipher. In this stage, the message is encrypted using filter bank cipher, where its filters coefficients are generated from the key [16].

The decryption process is achieved at the receiver. In this case, the synthesis filter bank and perfect reconstruction lifting scheme are used to reconstruct the original message. The perfect reconstruction lifting scheme is shown in Figure 4. And one Round filter bank cipher decryption System is shown in Figure 5 which satisfies the perfect reconstruction property to recover the original message properly.

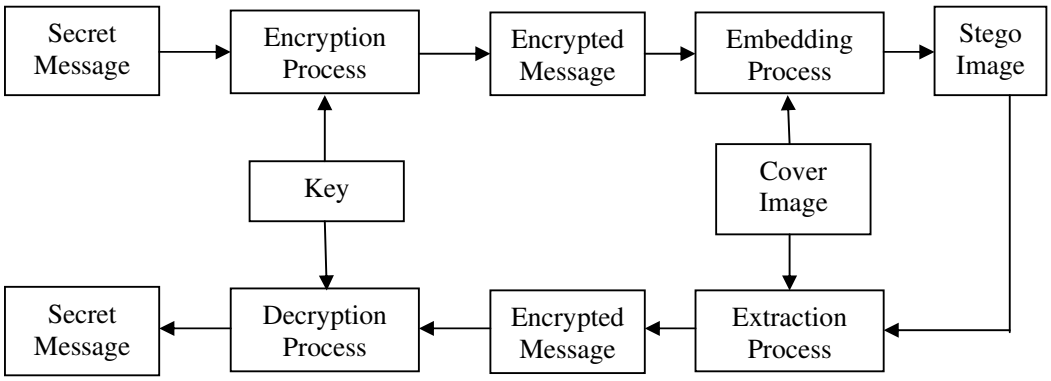

Figure 1. Block Diagram of the proposed system.

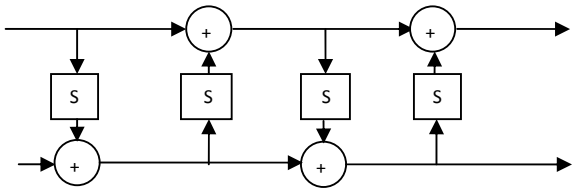

Figure 2. Lifting scheme.

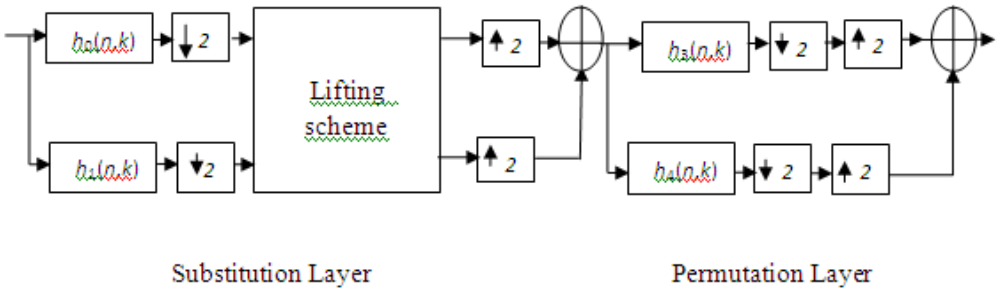

Figure 3. One Round Filter Bank Encryption cipher.

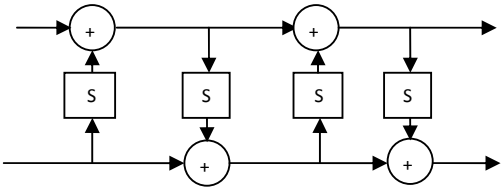

Figure 4. Perfect reconstruction lifting scheme.

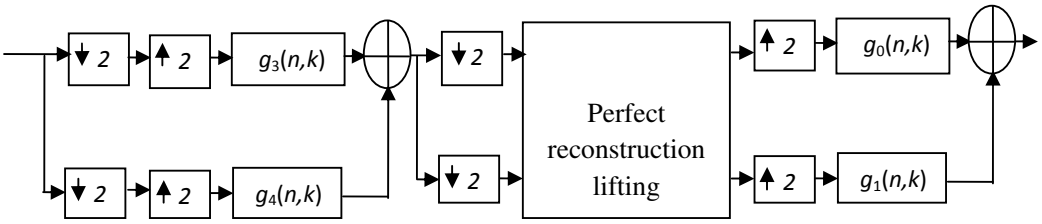

Figure 5. One Round filter bank cipher decryption System.

3.2 Embedding and Extraction Process

DWT based steganography is used to hide the message using Haar wavelet. Wavelet transform converts a spatial domain into frequency domain. In this case the cover image is decomposed into four sub-images, namely, approximation coefficients, horizontal detail coefficients, vertical detail coefficients and diagonal detail coefficients. The embedding process is achieved at the transmitter to hide the message. In this paper the embedding process based on the following algorithm.

Algorithm

Input: Cover image and encrypted message.
Output: Stego image.

Begin
1. Normalized the encrypted message.
2. Transform the cover image using Haar wavelet transform
3. Embedding the normalized encrypted image in vertical detail coefficients and diagonal detail coefficients.
4. Inverse DWT of all the subbands.
5. Denomoralize.
6. Stego image is generated.

End

The extraction process is used to retrieve the original message at the receiver. It processes the stego image to extract the original message. In this paper the extraction process based on the following algorithm.

Algorithm

Input: Stego Image.
Output: Encrypted message.

Begin
1. Transform the stego image using Haar wavelet transform.
2. Extracting the normalized encrypted image from the vertical detail coefficients and diagonal detail coefficients.
3. Normalization.
4. The encrypted message is generated.

End

Note that, the encryption and embedding processes are achieved in the transmitter to generate the stego image, while the extraction and decryption processes are achieved in the receiver to recover the original message.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

To evaluate the performance of the proposed system in this paper, five cover images (Cameraman, Lenna, Peppers, House, Baboon and each of size 256×256) were employed to embed a text encrypted message. In this paper, the message is firstly encrypted, after that it is hidden to be sent. At the receiver, the hidden message is extracted and then decrypted. This represents a hybrid system that combines cryptographic and steganographic algorithms together to improve the security of the information. This combination is tested using PSNR and histogram analysis.

PSNR is used to compare between the cover image and the stego image. It is measured in decibels (dB). It is used to assess the quality of the stego image. If PSNR of gray scale image larger than 36 dB then the human cannot distinguish between the cover image and the stego image [17]. The PSNR of the proposed system using different images were calculated using equation (1), and the results are summarized in Table 1. The results indicate that, the PSNR values are much greater than 36 dB; this proves the suitability of the proposed system.

Table 1. PSNR Results

Cover Image	**PSNR**
Cameraman	68.8120
Lenna	62.1071
Peppers	53.1336
House	68.6596
Baboon	59.9863

The histogram analysis can be used to evaluate the efficiency of the embedded algorithm. If the histogram remains the same after the embedding, then the embedded algorithm is efficient. The histograms of the cover images before and after the embedding process were plotted as shown in the Figures 6, 7, 8, 9 and 10. Note that the histograms of the cover images and the stego images do not have any significant change. The stability of the stego images histograms means that the proposed system can resist the attacks and statistical changes.

The processing time for embedding and extraction processes using different cover images are summarized in Table 3 and Table 4 respectively. Basically, the processing time depends on the specifications of the computer that used to run the program, and the speed of the compiler of the used programming language which is the Matlab in this paper. Usually the Matlab compiler is very slow when it compares with the compilers of other programming languages. Even though, the processing times for embedding and extraction are acceptable.

Table 2. Embedding Process Time

Cover Image	**Embedding Time (Second)**
Cameraman	1.0462
Lenna	0.9986
Peppers	1.1033
House	1.0651
Baboon	0.9965

Table 3. Extraction Process time

Cover Image	**Extraction Time (Second)**
Cameraman	1.1322
Lenna	1.0192
Peppers	1.1321
House	1.1151
Baboon	1.0795

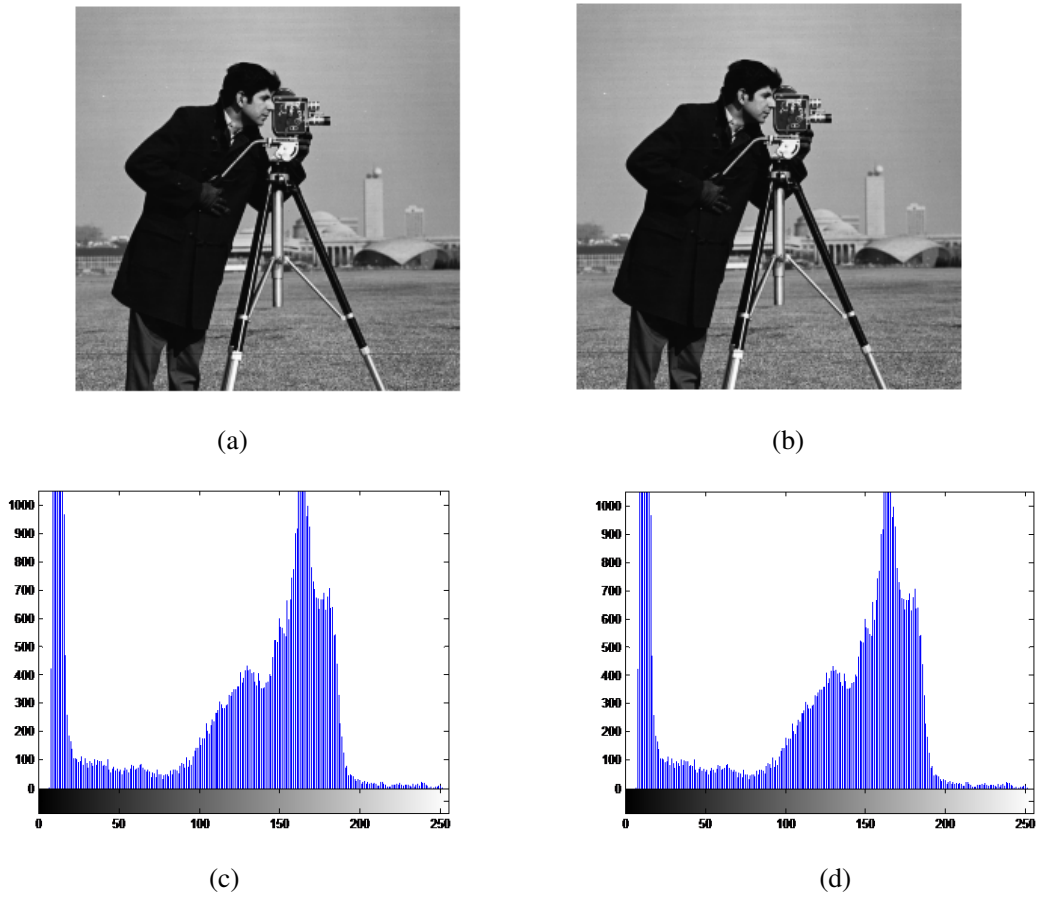

Figure 6. a) Cameraman cover image. b) Stego image. c) Histogram of Camerman image. d) Histogram of stego image.

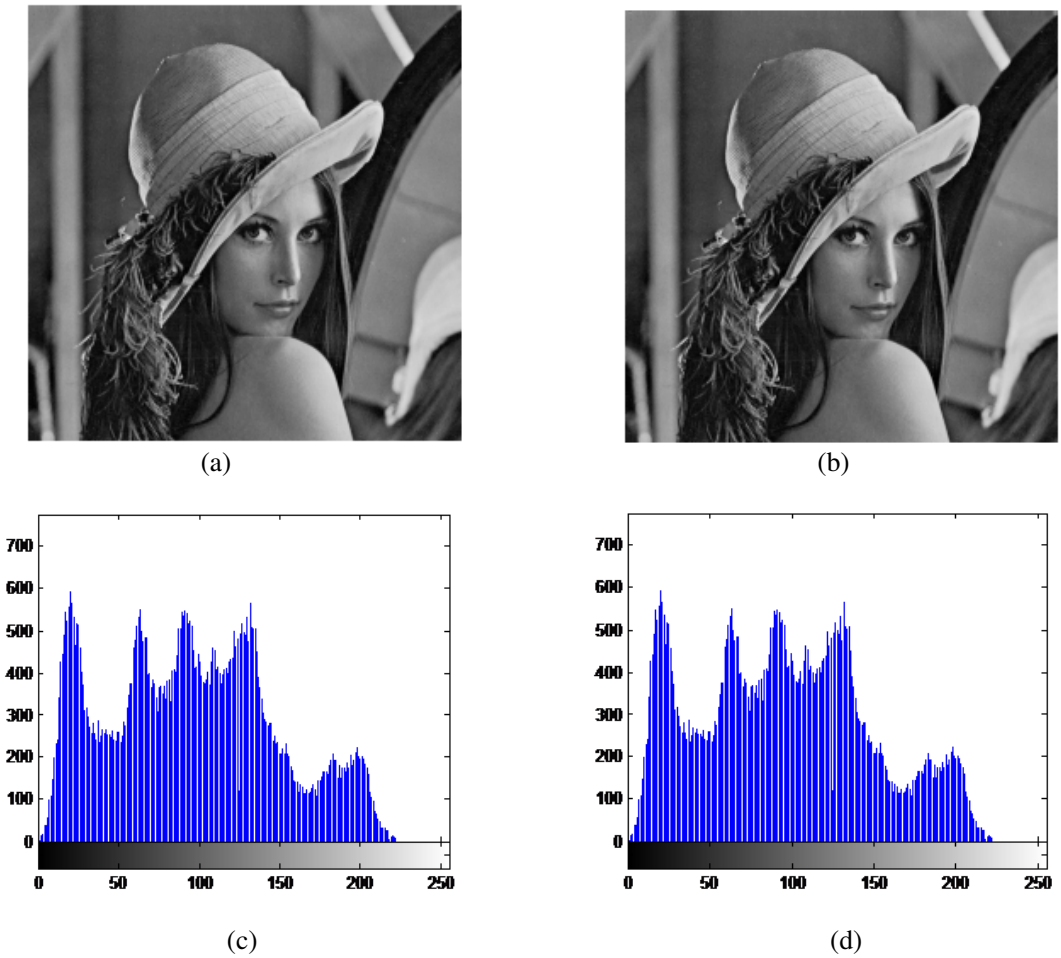

Figure 7. a) Lenna cover image. b) Stego image. c) Histogram of Lenna image. d) Histogram of stego image.

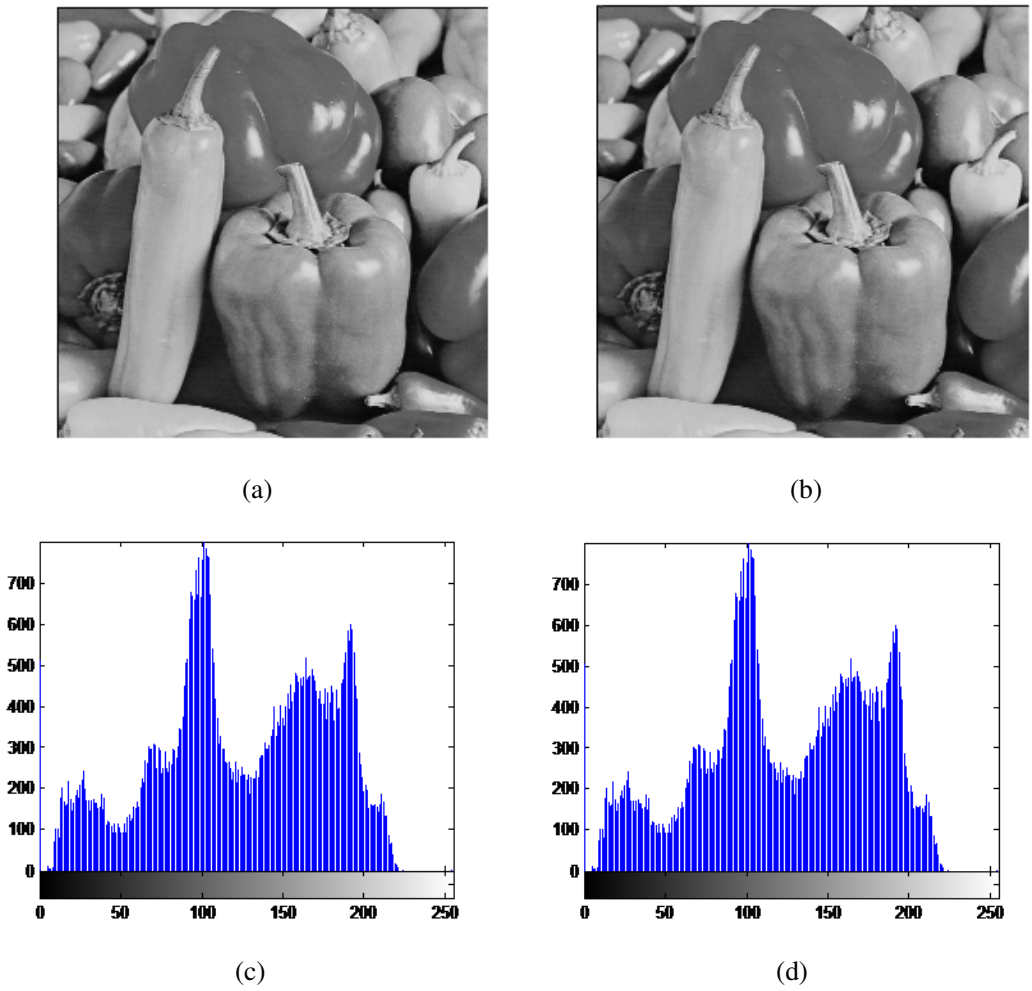

Figure 8. a) Peppers cover image. b) Stego image. c) Histogram of Peppers image. d) Histogram of stego image.

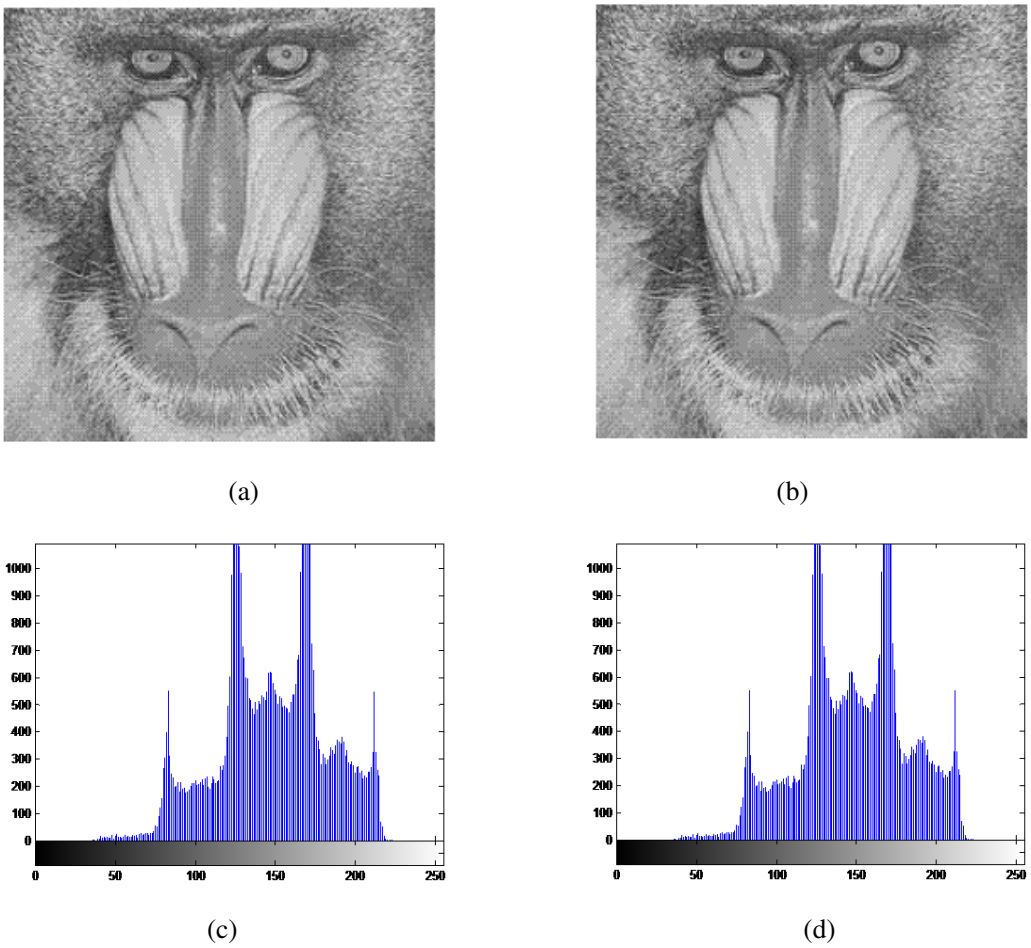

Figure 9. a) Baboon cover image. b) Stego image. c) Histogram of Baboon image. d) Histogram of stego image.

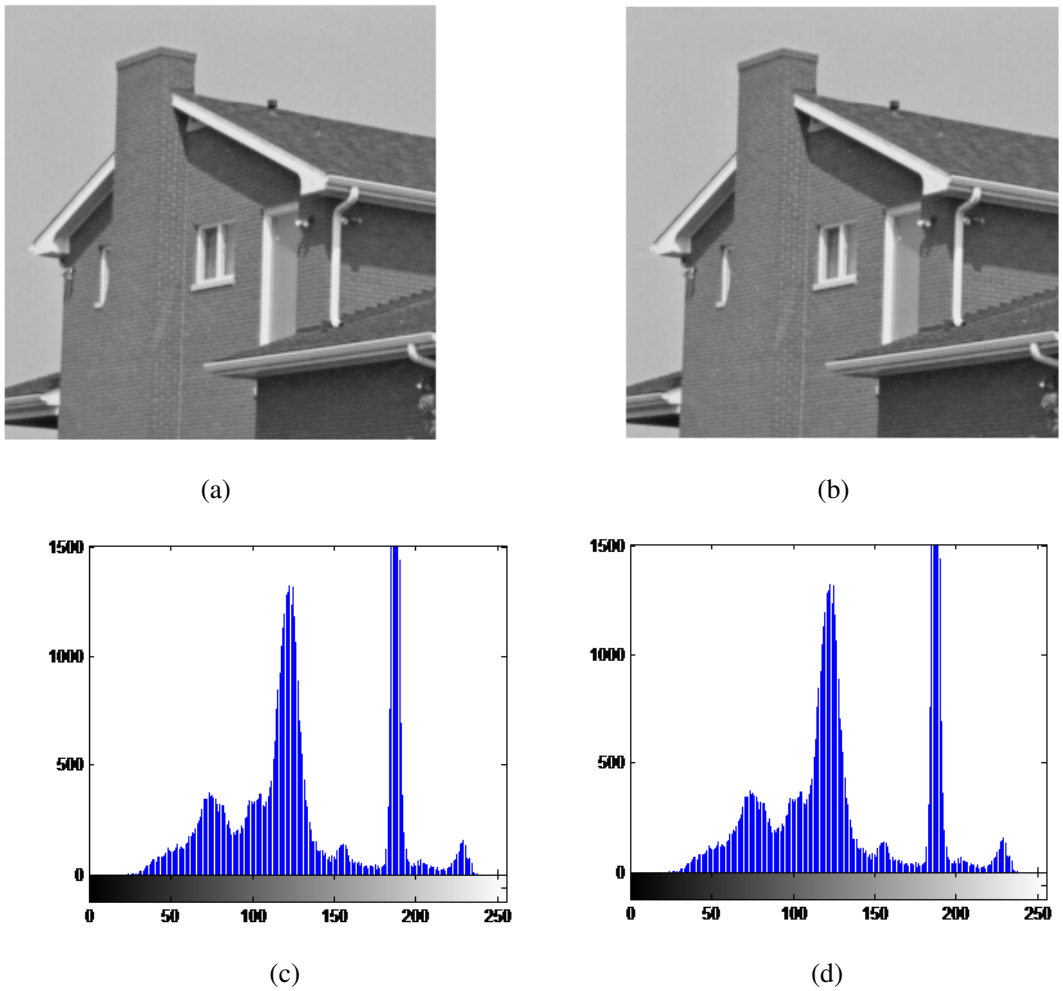

Figure 10. a) House cover image. b) Stego image. c) Histogram of House image. d) Histogram of stego image.

5. CONCLUSION

In this paper a high security model uses both cryptography and Steganography has been developed. Filter bank cipher is used for encryption the data. Filter bank cipher is a symmetric block cipher; it provides high level of security, scalability and speed. The encrypted data is embedded in a cover image using discrete wavelet transform. The performance of the proposed algorithm has been evaluated using PSNR and histogram. The results showed that, the PSNR of the proposed system are high, which ensure the invisibility of the hidden message through the cover image. Also, the histograms of the stego and cover images are very close to each other, which ensure the resistivity of the proposed system against the attacks.

REFERENCES

[1] Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting and Decrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

[2] Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

[3] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.

[4] Jarno Mielikainen, (2006), "LSB Matching Revisited", IEEE signal processing letters, Vol. 13, No. 5.

[5] Piyush Marwaha, Paresh Marwaha, (2010), "Visual Cryptographic Steganography in images", IEEE, 2nd International conference on Computing, Communication and Networking Technologies.

[6] G.Karthigai Seivi, Leon Mariadhasan and K. L. Shunmuganathan, (2012), " Steganography Using Edge Adaptive Image " IEEE, International Conference on Computing, Electronics and Electrical Technologies.

[7] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath, (2012), " A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1.

[8] Tong L.and Zheng-ding, Q, (2002), "DWT-based color Images Steganography Scheme", IEEE International Conference on Signal Processing, 2:1568-1571.

[9] Mandal J.K. and Sengupta M., (2010), "Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC).", Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[10] Septimiu F. M., Mircea Vladutiu and Lucian P., (2011),"Secret data communication system using Steganography, AES and RSA", IEEE 17th International Symposium for Design and Technology in Electronic Packaging.

[11] H. Tian, K. Zhou, Y. Huang, D. Feng, J. Liu, (2008), "A Covert Communication Model Based on Least Significant Bits Steganography in Voice over IP", IEEE The 9th International Conference for Young Computer Scientists, pp. 647-652.

[12] Y. Huang, B. Xiao, H. Xiao, (2008), "Implementation of Covert Communication Based on Steganography", IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1512-1515.

[13] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul,(2008), "Securing Information Content using New Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management.

[14] Rasul E., Saed F. and Hossein S, (2009), " Using the Chaotic Map in Image Steganography", IEEE, International Conference on Signal Processing Systems.

[15] Majunatha R. H. S. and Raja K B, (2010), "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), Vol. 3: Issue (6) pp 462-472.

[16] Saraireh S. and Benaissa M., (2009), "A Scalable Block Cipher Design using Filter Banks and Lifting over Finite Fields" In IEEE International Conference on Communications (ICC), Dresden, Germany.

[17] El Safy, R.O, Zayed. H. H, El Dessouki. A, (2009), "An adaptive steganography technique based on integer wavelet transform," ICNM International Conference on Networking and Media Convergence, pp 111-117.

Author

Saleh Saraireh has been an assistant Professor at Philadelphia university in Jordan – Amman since 2009. I am PhD holder from the university of Sheffield, UK ,in communication engineering. Also I hold a Master degree in Communication Engineering, and a Bachelor degree in electrical engineering from Mutah university, Jordan. My research area related to wireless communication, digital signal processing and cryptography.