A Novel Security Scheme based on Twofish and Discrete Wavelet Transform

Mohammad S. Saraireh
Department of Computer Engineering
Mutah University, Karak, Jordan

***Abstract*—Nowadays, there is a huge amount of data exchanged between different users; the security of the exchanged data has become a significant problem due to the existing of several security attacks. So, to increase the confidence of users several security techniques can be used together to enhance the level of security. In this research paper a new secure system is proposed. The proposed system employs cryptography and steganography together. The combination between cryptography and steganography contributes in increasing the security level to provide a robust system that can resist the security attacks. In this paper, the Twofish block cipher based cryptography is employed to encrypt the data. The Twofish permits trade-offs between speed, key setup time, software size, memory, and security level. The steganographic algorithm employed to hide the encrypted data into an image is the discrete wavelet transforms (DWT) algorithm. Different security tests are used to evaluate the security and functionality of the suggested algorithm, such as, the peak signal to noise ratio (PSNR) analysis and histogram analysis. The results reveal that, the algorithm proposed in this paper is secure.**

Keywords—Cryptography; Twofish; DWT; Histogram; PSTN; Steganography

I. Introduction

The rapid progress in computer networks allows a large amount of data to be transmitted over different kinds of computer networks. Usually, people send personal data and sensitive document over these networks, moreover, military application, e – commerce, video conferencing and money transfer. All these applications are made over a non-secured channel. Therefore, it is necessary to have strong security algorithms to protect these applications from attackers and to satisfy authentication, confidentiality and data integrity. So, various security techniques can be used, such as cryptography and steganography, these techniques increase the confidence of users to use such computer networks.

Cryptography is defined as the art of protecting the data by the encryption process [1]. The encryption process transforms the original information (plaintext) into an unreadable data called ciphertext. In this case, only the person who has the secret key can recover the original information. The steganography is the art of embedding data within an image or an audio. Usually the encryption process and hiding process are prepared in the transmitter while the decryption process and extraction process is done in the receiver.

The cryptographic algorithms rely on using a key to making the encryption and decryption process, while the steganographic algorithms do not need a key to make the embedding and extracting process. Usually, there are two cryptographic algorithms, namely, symmetric key, and asymmetric key algorithms. For symmetric algorithm the encryption and decryption processes of the data are executed using the same key, one the other hand; asymmetric algorithm employs different key for encryption and decryption of the data. Steganographic systems can embed the data using, the spatial domain steganographic, or the transform domain based steganography. Cryptography algorithm and steganography algorithm are coupled to design strong security systems.

Steganographic algorithms should satisfy the following conditions to be useful [2]:

a) Invisibility: it means that nobody could notice the difference between the images before and after applying the steganographic system (cover and stego images).

b) Security: To evaluate the security of steganographic algorithms, PSNR can be used to measure the difference between the images before and after applying the steganographic system (cover and stego images). PSNR can be calculated using:

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

L: the maximum samples value.

MES: mean error square.

This research paper is introduced as follows. The previous study and related researches are presented in Section 2. The suggested system is discussed in Section 3. In Section 4, the simulation and the experimental results are discussed. The conclusion is presented in Section 5.

II. Literature Review

Several security techniques are used to ensure data security. Many techniques based on a combination of different security algorithms to improve the security of the data exchange. In [3] the filter bank block cipher based cryptography is combined with a discrete wavelet transform based steganography, so in addition to the encryption process, the encrypted message is hidden using the particular cover image to generate stego image. In [4] a hybrid image security framework was proposed by combining various security techniques together, which are cryptography, steganography and image compression. In [5], an image steganography algorithm was designed using least significant bit (LSB) insertion; also, the authors employed the

RSA algorithm to execute the encryption process to generate a strong security system. In [6], the advanced encryption algorithm (AES) based cryptography was used to encrypt secrete data, after that, pixel value differencing (PVD) with K-bit LSB substitution was employed to embed the encrypted secrete data into a true colour RGB image. In [7], cryptography, steganography and digital watermarking were combined together to produce a robust security system, where visual cryptography scheme was used to encrypt a secret image, after that, Zig – Zag scanning pattern based steganography was used to hide the information, then, the secret shares were watermarked into an image using digital watermarking. In [8], a secure and fast algorithm was proposed; it performs cryptography and steganography for the speech signal. In [9], a novel steganography and authenticated image sharing (SAIS) algorithm were introduced without a need for parity bits. By using this algorithm, the user can share a secret image into n stego-images and can reconstruct it with any k or more than k stego-images but not less than k stego-images. A novel approach was proposed in [10], in this approach, the secret image was divided into n shares to be hidden in stego images, and then image watermarking algorithm was used to embed fragile watermark signals into the stego images by the use of parity-bit checking to provide authentication. In [11], vigenere cipher based cryptography was combined with least significant bit based steganography; this combination was employed to scramble the secret data firstly, then embedding it to provide confidentiality of the information. In [12], the encoded process consists of encryption and hiding, where AES was used for encryption and bit substitution-based steganography was employed for hiding.

III. Proposed Algorithm

The aim of this paper is the design of a secure algorithm using different security techniques. The design based on the combination of two powerful security techniques, these techniques are cryptography and steganography. So, the data to be sent, it should firstly be encrypted, after that it should be hidden using a particular cover image, then it can be sent to the other user. In this paper, the Twofish block cipher is employed to make the encryption process, and the DWT steganographic algorithm is used to make the embedding process. The block diagram of the proposed system is shown in Figure 1. Note that the proposed system consists of four processes which are encryption process, embedding process, extraction process and decryption process. These processes are described as in the following algorithm.

Algorithm

Input: Data to be sent.

Output: Original data is encrypted and embedded in an image and recovered properly.

Start

1. Original data.
2. Encryption of original data.
3. Implementation of DWT based steganography using Haar wavelet.
4. Embedding the encrypted data.
5. Generation of stego image.
6. Extraction of embedded encrypted data.
7. Encrypted message generation.
8. Decryption.
9. Original data.

Finish

A. *Encryption and Decryption Processes*

The encryption and decryption processes based on the Twofish block cipher as shown in Figure 2 [12]. Twofish is a symmetric cryptographic encryption algorithm. It employs 16 rounds Feistel structure with additional whitening of the input and output. In this algorithm plaintext is split into four 32-bit words which are Xored with four key words that are called the whitening process. This process is followed by sixteen rounds and in each round the same process is repeated [12]. Note that,

$\oplus$: Bitwise xoring.

$\boxed{+}$: 32-bit word-wise addition.

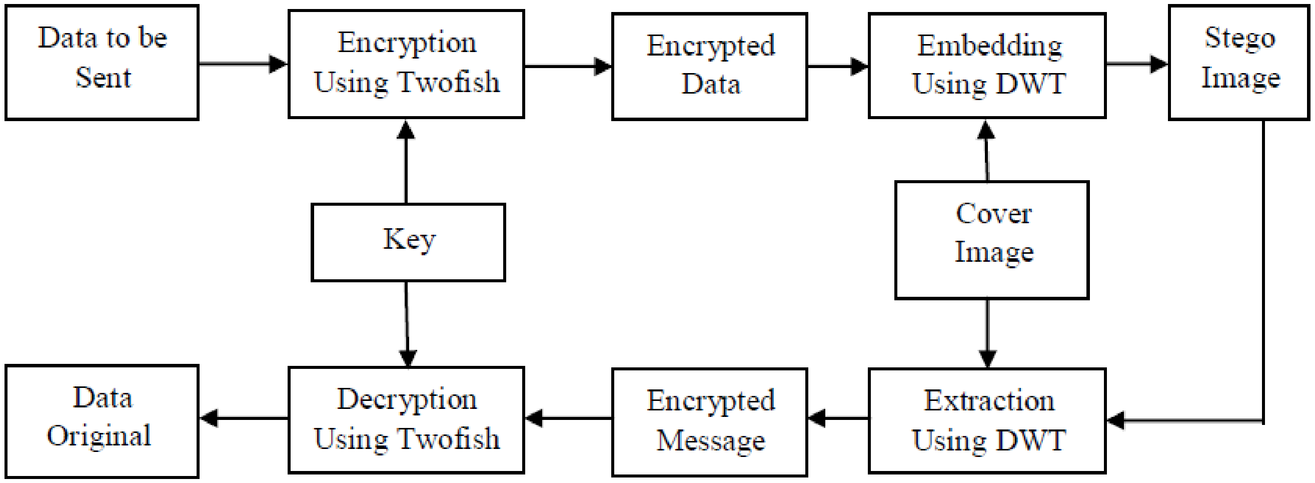


Fig. 1. Block Diagram of the Proposed Algorithm

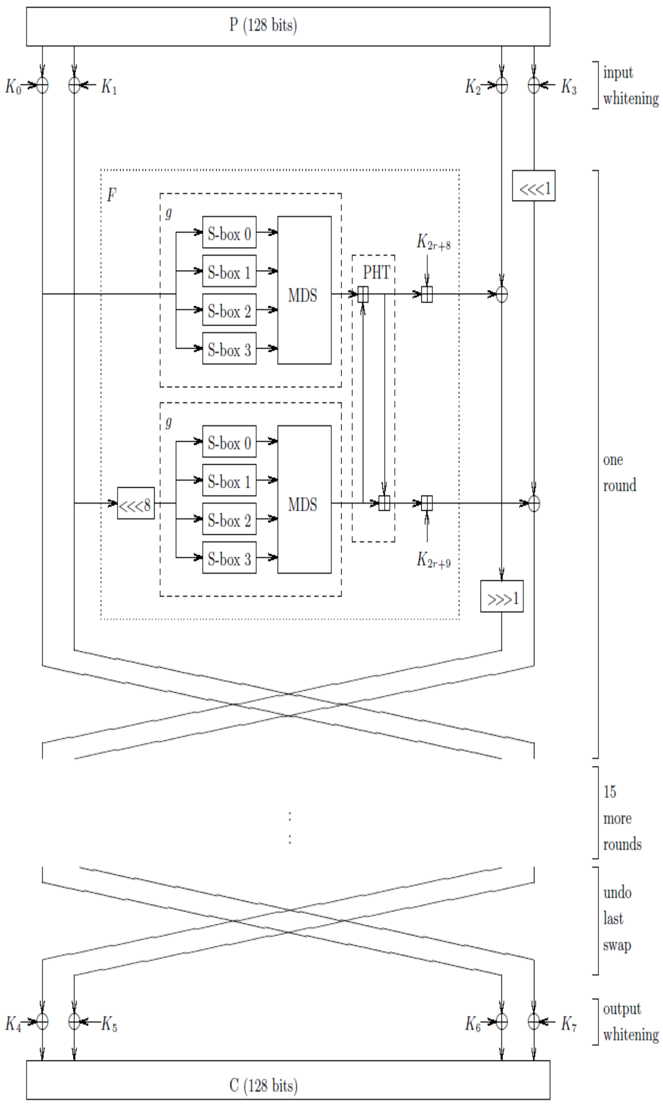


Fig. 2. Twofish Block Cipher.

B. Embedding and Extraction Processes

DWT is used to execute the embedding and extracting process. Haar wavelet is employed to decompose the cove image into four coefficients or sub – images which are called approximation, horizontal detail, vertical detail and diagonal detail coefficients. The data is hidden in the vertical and diagonal detail coefficients to generate the stego image. So the embedding technique replaces the data in a given pixel with data in the cover image using the following algorithm.

Embedding Process Algorithm

Input: Encrypted information and the cover image.

Output: The stego image.

Start
1. Normalisation of the encrypted information.
2. The cover image is transformed into sub images by the Haar wavelet transform.
3. Hiding the normalised data into vertical and diagonal detail coefficients.
4. Applying the inverse DWT all sub bands.
5. Denomoralisation.
6. Stego image produced.

Finish

The extraction is the process of recovering the original data from the stego image. In this paper the extraction is done using the following algorithm.

Extraction Process Algorithm

Input: The stego Image.

Output: The encrypted information.

Start
1. Transformation of the stego image by applying the Haar wavelet transforms.
2. The normalised sub images are extracted from the vertical and diagonal detail coefficients.
3. Normalisation.
4. Production of the encrypted message.

Finish

IV. Results Analysis and Discussion

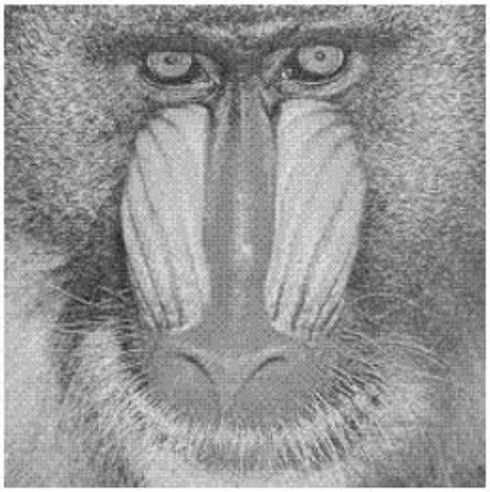
To evaluate and examine the performance of the proposed algorithm different cover images are used, which are Cameraman, Lenna, Peppers, House and Baboon where the size of the images is 256×256 bits. The cover images are employed to hide the encrypted data. The encrypted data is generated using the Twofish block cipher algorithm, then, the Haar wavelet transform is applied to produce the stego image to be exchanged over a non-secure communication channel. To recover the original data, the hidden encrypted data is retrieved to be decrypted to obtain the original message. PSNR and histogram analysis are employed in this research to examine the security of the proposed algorithm.

Usually, PSNR is used to measure the difference between the cover and stego images; it is measured in decibels (dB). PSNR is also used to evaluate the quality of the steganographic algorithm. If the PSNR of gray scale of the image larger than 36 dB, then, nobody could notice the difference between the cover image and the stego image, while, if the PSNR smaller than 36 dB, then the human can distinguish the difference between the cover and stego images [13]. The value of PSNR is calculated using equation (1). Table 1 shows the values of PSNR for different cover images. As shown in Table 1, the values of PSNR are greater than 36 dB; so, the proposed algorithm is secure.

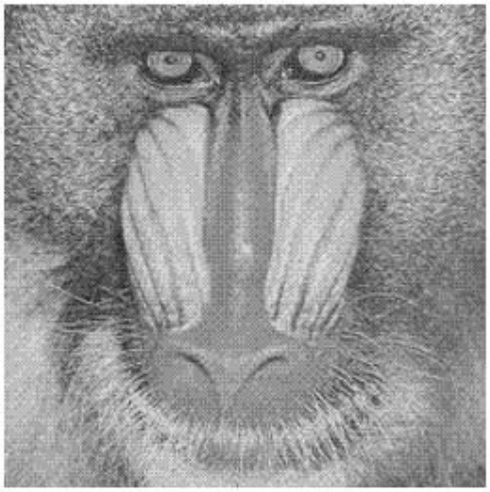
TABLE I. Peak Signal To Noise Ratio Results

Cover Image	PSNR
Peppers	54.3421
Baboon	60.3425
Cameraman	68.5643
House	68.0823
Lenna	61.7436

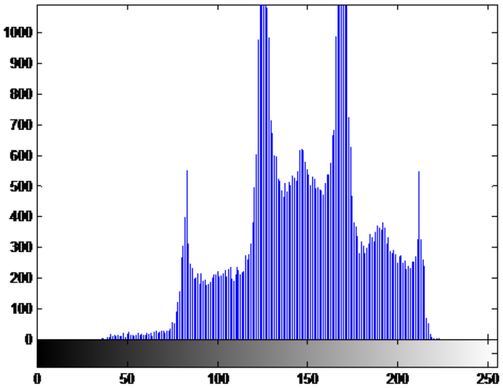
There is another method used to evaluate the security and efficiency of the proposed algorithm. This method is called the histogram analysis. In this case, it is essential to generate the histogram of the cover image and stego image, and then notice the difference of the histogram before and after the embedding process. If they are the same, then the embedding algorithm is secure, otherwise it is non-secure. In this research different images are analysed, so the histograms for different cover images are generated and compared with the histogram of their corresponding stego images. Figures 3, 4, 5, 6 and 7 show the histograms of the cover images and the stego images. Note that, the histogram of cover images and stego images are the same and do not have any significant change. So, the proposed system is secure and can resist the attacks and statistical changes.



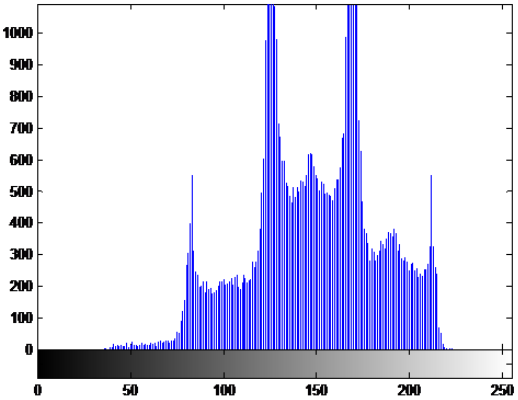
(3.1)



(3.2)



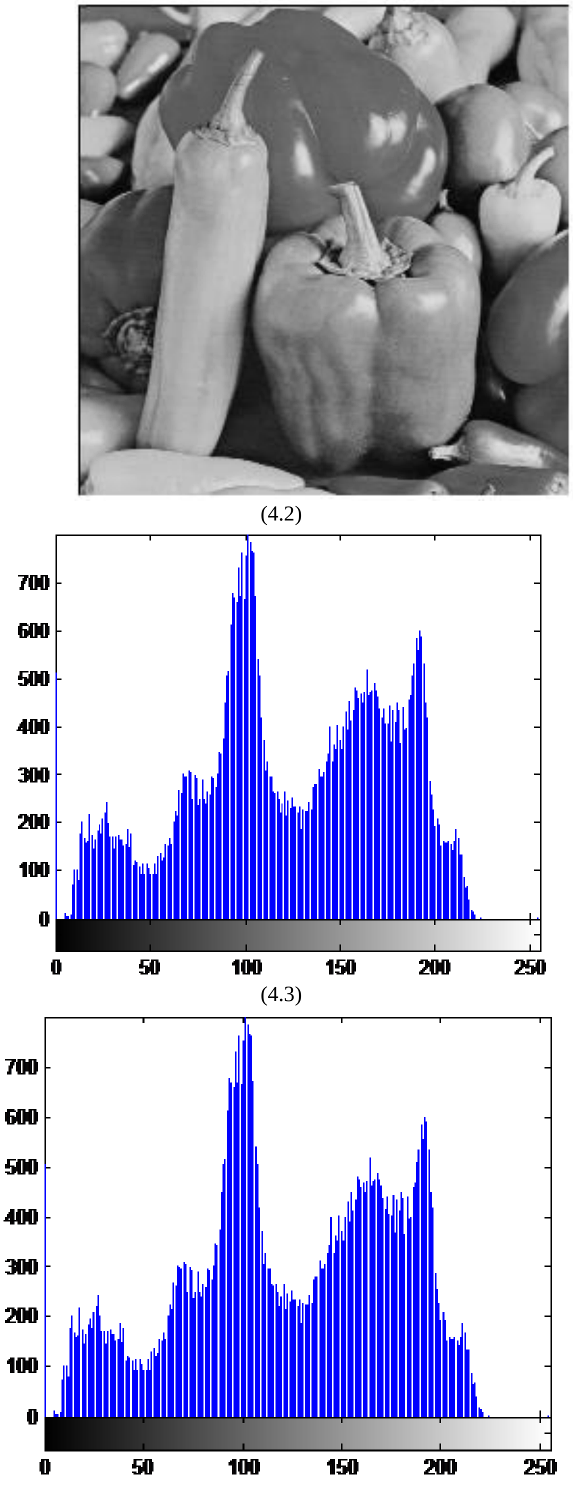
(3.3)



(3.4)

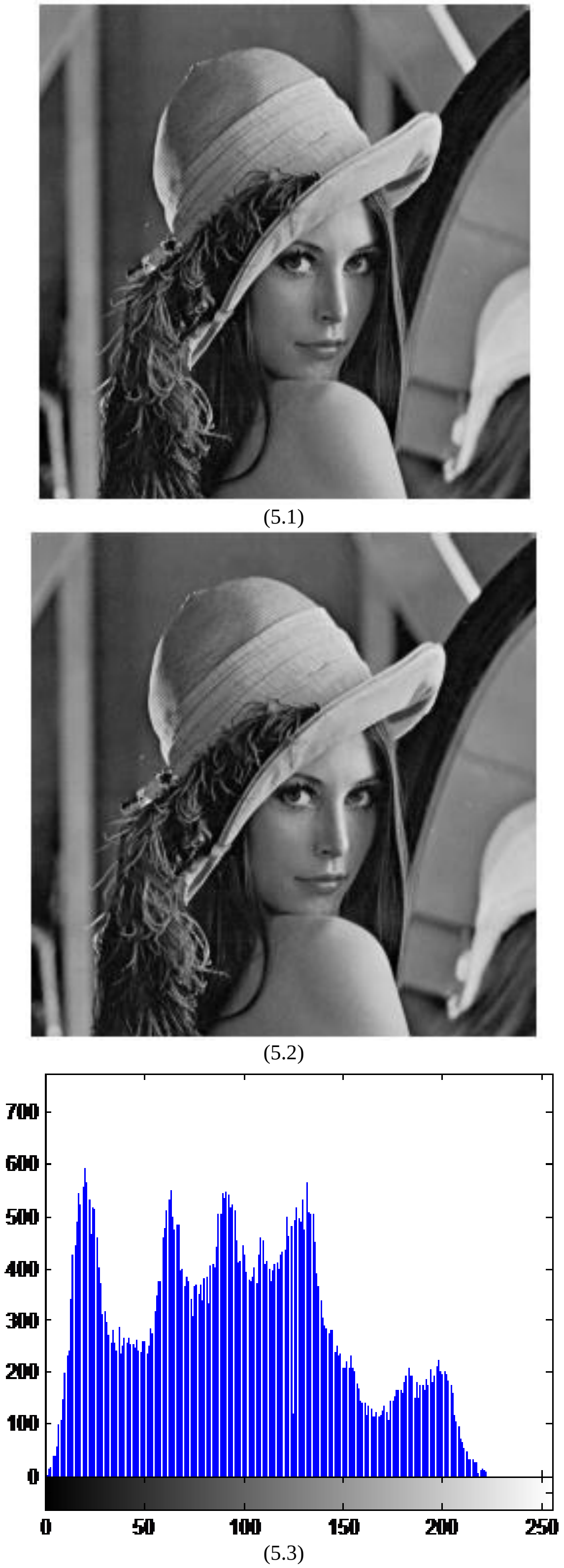
Fig. 3. (3.1) Cover image. (3.2) Stego image. (3.3) Histogram of cover image. (3.4) Histogram of stego image.

(4.1)

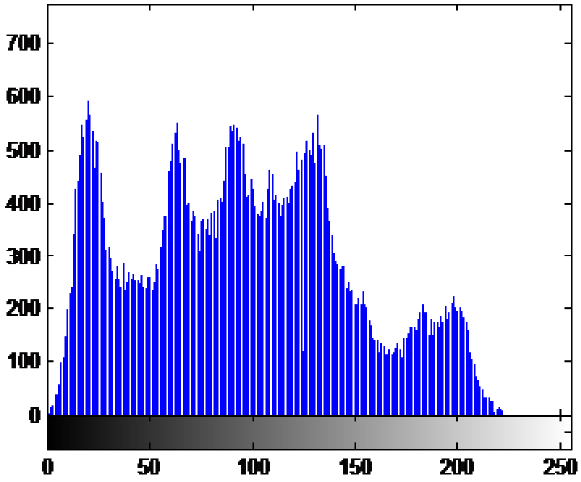


(4.4)

Fig. 4. (4.1) Cover image. (4.2) Stego image. (4.3) Histogram of cover image. (4.4) Histogram of stego image.

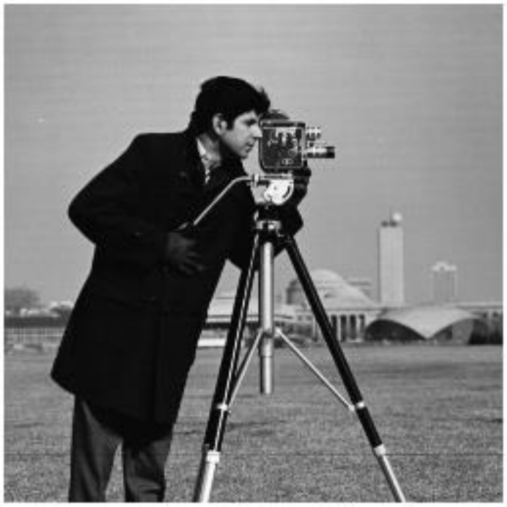


(5.3)

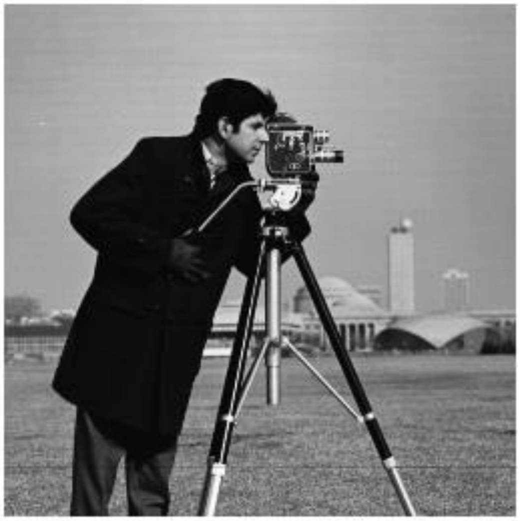


(5.4)

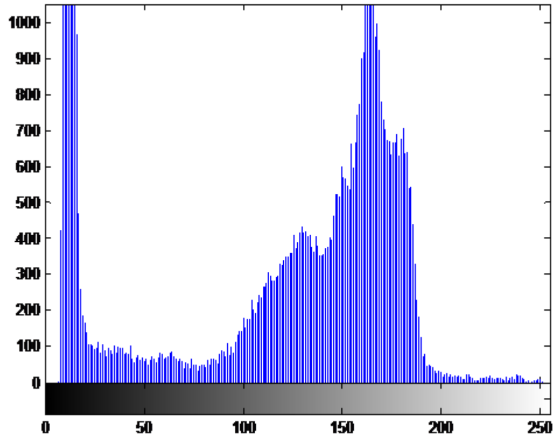
Fig. 5. (5.1) Cover image. (5.2) Stego image. (5.3) Histogram of the cover image. (5.4) Histogram of stego image.



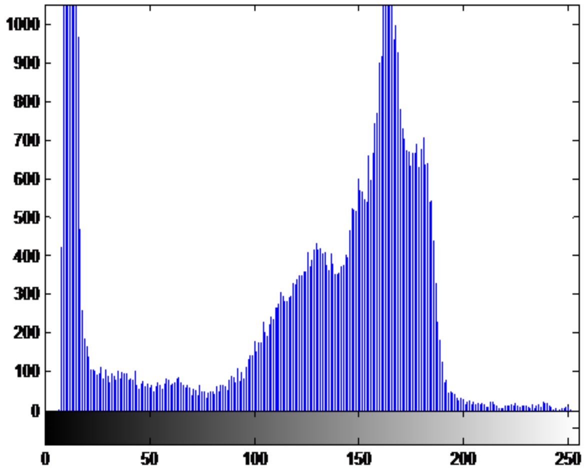
(6.1)



(6.2)

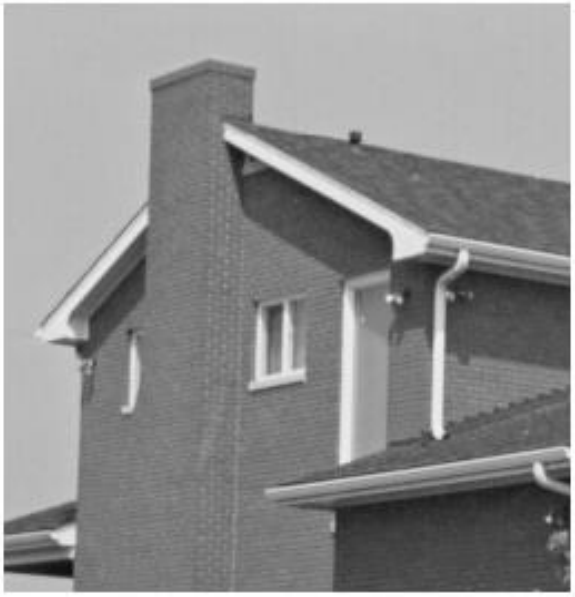


(6.3)

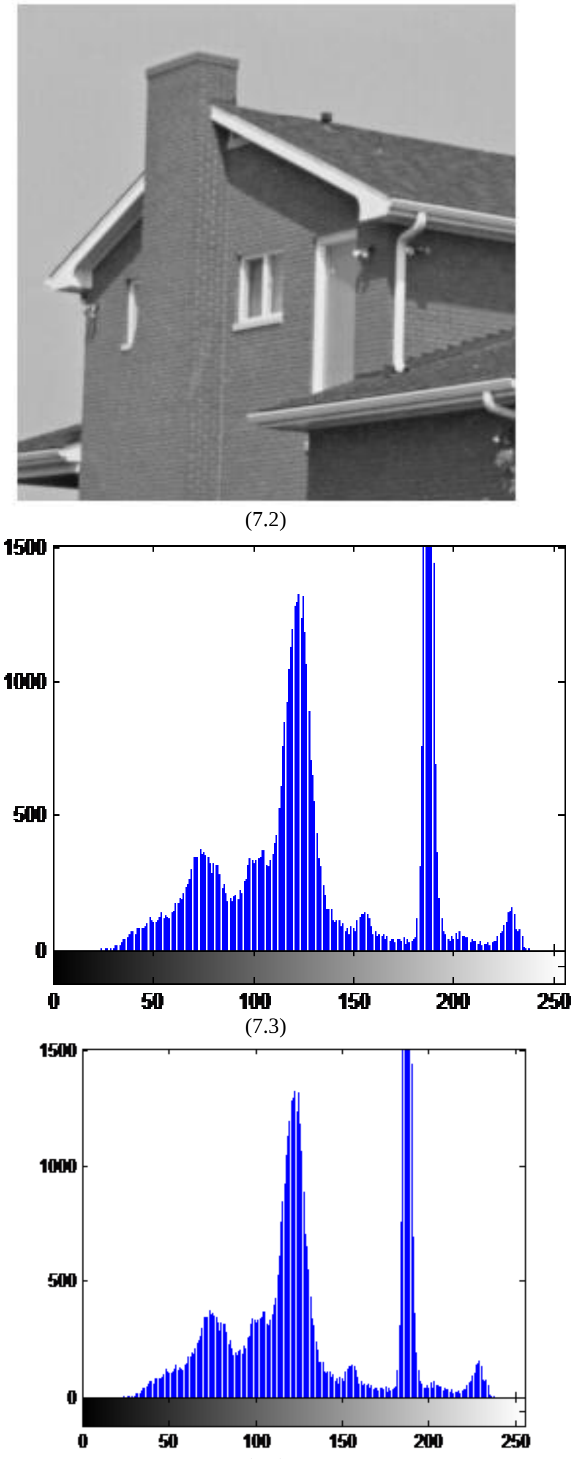


(6.4)

Fig. 6. (6.1) Cover image. (6.2) Stego image. (6.3) Histogram of cover image. (6.4) Histogram of stego image.



(7.1)



(7.2)

(7.3)

(7.4)

Fig. 7. (7.1) Cover image. (7.2) Stego image. (7.3) Histogram of the cover image. (7.4) Histogram of stego image.

V. Conclusion

In this paper, Twofish block cipher and DWT based steganography are combined together to generate a new algorithm which can provide a high security model. Twofish based cryptography is used to make the encryption process to the data, it provides the security and speed of the system. Haar wavelet transform based steganography is used to embed the encrypted data into a cover image to provide the security level. PSNR and histogram analysis were employed to evaluate the security of the suggested system. As shown in the results, all the values of PSNR using various cover images are larger than 36 dB, this means that, the hidden data is invisible. Also the histograms of the cover images and the stego images are similar to each other. This proves the security and efficiency of the suggested algorithm. In conclusion, this research paper can be considered as a base for further research in the field involving authentication, watermarking and keystroke.

References

[1] Saleh Saraireh, Mohammad Saraireh & Yazeed Alsbou, " Secure Image Encryption Using Filter Bank and Addition Modulo 2^8 with Exclusive OR Combination " *International Journal of Computer Science and Security (IJCSS)*, Vol. (7), No. (2), 2013.

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

[3] Saleh Saraireh, "A Secure Data Communication System Using Cryptography and Steganography", *International Journal of Computer Networks & Communications (IJCNC)*, Vol. 5, No. 3, 2013.

[4] Pooja Rani and Apoorva Arora, "Image Security System using Encryption and Steganography", *International Journal of Innovative Research in Science,Engineering and Technology*, Vol. (4), No. (6), June 2015.

[5] Mamta Juneja and Parvinder Singh Sandhu,"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", *2009 International Conference on Advances in Recent Technologies in Communication and Computing*, 27 - 28 Oct 2009, Kottayam Kerala, India.

[6] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R.,"A Novel Security Scheme for Secret Data using Cryptography and Steganography", *J. Computer Network and Information Security*,Vol. 2, pp. 36-42, 2012.

[7] R. Gayathri, and V. Nagarajan" Secure data hiding using steganographic technique with Visual cryptography and watermarking scheme ", *2015 International Conference on Communications and Signal Processing (ICCSP)*, 2-4 April 2015, Melmaruvathur, India.

[8] Divya Sharma and Deepshikha Sharma," Steganography of the keys into an encrypted speech signal using Matlab ", *3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 16-18 March 2016, New Delhi, India

[9] Ching-Nung Yang, Jin-Fwu Ouyang and Lein Harn," Steganography and authentication in image sharing without parity bits " *Optics Communications*, Vol. 285, No. 7, pp 1725–1735, 2012.

[10] Chang-Chou Lin and Wen-Hsiang Tsai," Secret image sharing with steganography and authentication", *Journal of Systems and Software*, Vol. 73, No. 3, pp 405 – 414, 2004.

[11] Cheddad Victor Onomza Waziri), " Cyber Warfare and Terrorism based on Data Transmission through Classical Cryptographic and Steganographic Algorithms", *International Journal of Computer Applications*, Vol, 112. No. 16, 2015.

[12] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall and Niels Ferguson "Twofish: A 128-Bit Block Cipher", 15 June 1998.

[13] B.Veera Jyothi, S.M.Verma, and C.Uma Shanker, "Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification" *International Journal of Computer Applications,* Vol. 5, No. 5, pp 22 - 27, ,2010.

Author Profiles

Mohammad Saraireh is an associate professor at the Faculty of Engineering, Computer Engineering Department, Mutah University, Jordan. His area of expertise is in the quality of service in wireless computer networks and computer Networks, artificial intelligence applied to computer networks, communication systems, security and network security.