

Design and Implementation proposed encryption and Hiding Secure Image In an Image

Asst. Prof. Dr. Baheja k.Shukur, Alaaldeen Abbas Abdulhassan, Mohammed Hussein Jawad

Computer Technology /network department, Babylon University, Iraq

Abstract

Steganography and cryptography are two general methods of transfer vital information in a top-secret method. When we hide the secure image the malicious want to distort this secure image itself. Therefore, the cryptography techniques used must be one of the most powerful techniques. Also cryptography and Steganography are the two major techniques for secret communication. The contents of secret message are scrambled in cryptography, where as in steganography the secret message is embedded into the cover medium. This paper presents hybrid method of cryptography which combined two nonlinear feedbacks register in one non-linear function to produce a strong cryptography technique. The cryptography method is working on the image resulted from the DWT which, used the orthogonal filter. In steganography part we have used most significant method to hide the secret true image into true image. To evaluate our system number of measurements used such as Mean Square Error, Normalized Cross Correlation, Average Difference, Structural Content, peak signal to noise ratio (PSNR) have been computed between the cover and stego image. Finally histogram plot of cover image, stego image, secret ciphered images have been plotted.

Keyword: steganography, cryptography, orthogonal filter, cipher, decipher.

I. Introduction

The science of hiding data by embedding information into cover means is called a Steganography, which is supplement cryptography not replace it in security. To provide another layer of protection the hidden message is encrypted, which it must be decrypted if discovered. The science that studies mathematical techniques for keeping message secure and free from attacks called the cryptography [1], [2]. Whereas the science for hiding communication called a steganography [3]. Which, involves hiding information that appears no information is hidden in it at all.

Cryptography and Steganography achieve the same goal via different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography, in contrast attempts to prevent an unintended recipient from suspecting that the data is there. [4]. Combining encryption with steganography allows for a better private communication. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message.

There are number of methods in steganographic systems, which can be classify according to the type of covers used for secret communication. Which they: The systems which

substitute redundant parts of a cover with a secret message is called Substitution systems; but embedding the secret information in a transform space of the signal (e.g., in the frequency domain) is called transform methods; and in spread spectrum method implemented the concepts of spread spectrum communication; By exploiting several statistical properties of a cover and use hypothesis testing in the extraction process the statistical methods encode data invented; also in the distortion methods the data storing by signal distortion and the deviation from the original cover measured in the decoding step; finally the cover generation methods ,which created the encode of the data in the cover for secret communication .

In this study we apply the discrete wavelet transform on the secret first then embedding the LL level resulted from this stage in the cover image.

Similar to cryptanalysis which applied in the cryptography, the steganography deals with hiding the data in some cover source. Whereas the steganalysis is the science of detecting messages hidden using steganography, which identify suspected packages, to determine whether or not they have a payload encoded into them, and, if possible, recover that payload. [5]

II. The structure of the suggested system:

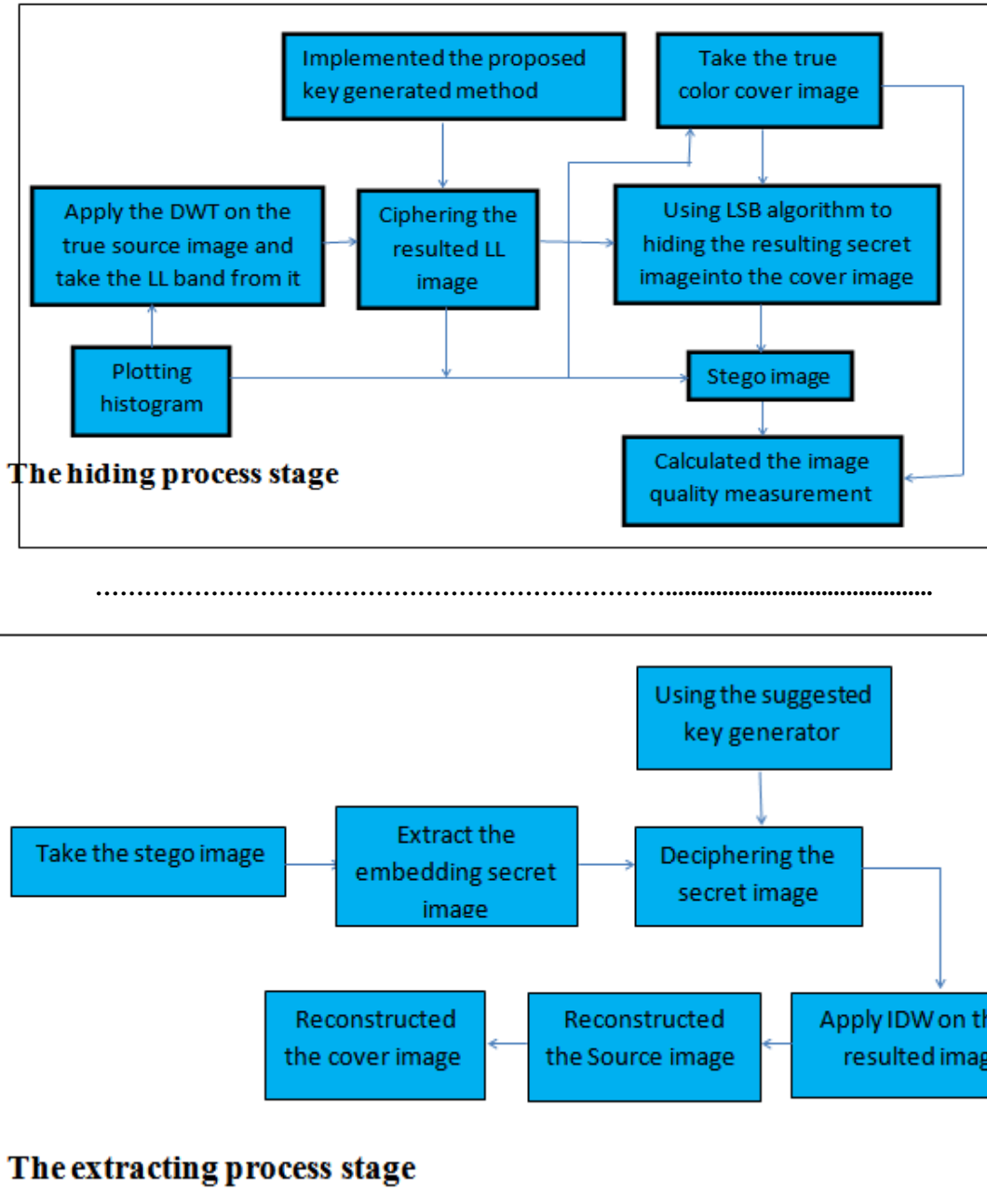


Figure (1) the design of the suggested system

Steps for hiding the encoding image are,

1. Use Discrete Wavelet Transform.
2. Apply proposed encryption algorithm on the LL band resulted from step 1 by making xor operation between it with the bytes of the LL band.
3. Use LSB replacement to hidden the resulting secret encryption image.
4. Store the stego resulting image which contains the encryption secret information.

5. to evaluate the result number of performance measurements used .

Steps for extracting and decoding of hidden image are,

1. Extract the embedding secret encryption image using the extracting LSB algorithm.
2. Apply the decryption proposed algorithm to extract the origin secure image by making xor operation between the key and encryption image.

3. Take the Inverse Discrete Transform to the resulted image from step 2.
4. Then extract secret image and cover image.

2.1 Discrete Wavelet Transform (DWT)

The DWT is a system, which involved two filters, one is the “wavelet filter”, and the other is the “scaling filter”. The wavelet filter is a high pass filter, while the scaling filter is a low pass filter. DWT includes many kinds of transforms, such as Haar wavelet, Daubechies wavelet, and others. Our study utilizes the orthogonal wavelet.

After applying a 1- level DWT on an image, we get the approximation subband LL, the horizontal subband LH, the vertical subband HL, and the diagonal subband HH. .

An advantage of DWT over other transforms is it allows good localization both in time and spatial frequency domain. Because of their inherent multi-resolution nature, wavelet coding schemes are especially suitable for applications where scalability and tolerable degradation are important. Applying IDWT to LL, HL, LH, and HH, we can get four different frequency's images that are low frequency image, middle-low frequency image, middle-high frequency image, high frequency image separately [6].

The main steps of DWT are: First, the row and column convolution with scaling filters (Low-Pass Filters) and wavelet filters (High-Pass Filters)

1. Convolve the lowpass filters with rows of image file and save the result.
2. Convolve the lowpass filters with the columns (of the result from step 1) to obtain the Low pass-Lowpass (LL) subimage.
3. Convolve the result from step 1 (the lowpass filtered rows) with the highpass filter on the column, to produce the Low pass-High pass (LH) Subimage.
4. Convolve the original image with the Highpass filters on the rows and save the result.
5. Convolve the result from step 4 with the lowpass filtered on the columns to yield the Highpass_Lowpass (HL) Subimage.
6. To obtain the Highpass_Highpass (HH) subimage, convolve the columns of the result from step 4 with Highpass filter.

Secondly, the (Down Sampler) are implemented by choosing only the odd or even locations of the sub-bands.

2.2 Inverse Discrete Wavelet Transform

The inverse wavelet transform performed by enlarging the wavelet transform data to its original size. Insert zeros between each two values horizontally and vertically, then convolve the corresponding (lowpass and highpass) inverse filters to each of the four sub

images, and sum the results to obtain the original image [7].

1. Upsample the rows for each Sub-band (LL, LH, HL, and HH) by inserting zero between every two samples.
2. Convolve the rows result from step1 with low and high pass filter, where the sub-bands (LL, LH) with low pass filter and (HL, HH) with the high pass filter.
3. Upsample the columns for the result from step2 by inserting zero between every two samples.
4. Convolve the result from step 3 with low pass and high pass filters, where the sub-bands (LL, HL) with the low pass filter and (LH, HH) with high pass filters.
5. Add the results from step 3 with the result from step 4 and save the result.

2.3 Least Significant Bit (LSB)

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit of some of all of the bits inside an image is changed to a bit of a secret message. When using 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a bit So it is possible to embed three bits in each pixel [8].

Algorithm of LSB Based Steganography:

Algorithm to embed secret image in cover image

Step 1: Read the cover image & secret encryption image, which is to be hidden in the cover image.

Step 2: Convert secret image into binary.

Step 3: Calculate LSB of each pixel of cover image.

Step 4: Replace LSB of cover image with each bit of secret encryption image one by one.

Step 5: Write stego image.

Algorithm to retrieve secret message using cover image

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixel of stego image.

Step 3: Retrieve bits & convert each 8 bit into byte of secret encryption image for each band (Red, Green, and Blue).

Step 4: Reconstruct the cover image.

2.4 Encryption method:

The first method:

. A combination of three LFSRs:

. If a_1 , a_2 and a_3 are the outputs of three LFSRs, the output of the generator can be calculated by the following equation:

$$b_1 = (a_1 \wedge a_2) \oplus (\neg a_1) \wedge a_3$$

If the LFSRs have lengths n_1 , n_2 and n_3 respectively then the linear complexity of the generator is:

(n1+1) n2+n1n3

The second method:

Consist of three LFSRs:

- .19 bits
- .x19+x5+x2+x+1
- .clock bit 8.
- .tapped bits: 13,16,17,18
- .22 bits
- . X22+x+1
- .Clock bit 10.
- .tapped bits 20, 21.
- .23 bits
- .x23+x15+x2+x+1
- .clock bit 10.
- .tapped bits 7,20,21,22

In this study we combined the result of two methods in one in nonlinear function to produce more robust method.

III. Performance Metrics

For data hiding, the main objectives are that the embedded data must be invisible to the observer, and it should have maximum load possible. It is difficult to quantify how invisible embedded data, for this reason number of statistical metrics have been used to show the difference between the cover and stego image such as Average Distance (AD) , Structure Content (SC),Normalized Cross-Correlation (NK) and Normal Mean Square Error (MSE),peak signal to noise ratio (PSNR).

Let the cover's pixels be represented as C(i,j) and the stego image pixels as S(i ,j) for fixed image size of M x N. Then the following equations can be represented as follow:

$$AD = \frac{1}{M * N} \sum_{i=1}^M \sum_{j=1}^N ([S(i, j) - C(i, j)])$$

$$SC = \frac{\sum_{i=1}^M \sum_{j=1}^N ([C(i, j)])^2}{\sum_{i=1}^M \sum_{j=1}^N ([S(i, j)])^2}$$

$$NK = \frac{\sum_{i=1}^M \sum_{j=1}^N ([C(i, j)]. [S(i, j)])}{\sum_{i=1}^M \sum_{j=1}^N ([S(i, j)])^2}$$

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

$$PSNR = ((M*N)*10*LOG (255^2))/MSE$$

IV. The implementation of the suggested system

In the suggested system

- We used orthogonal DWT transform on the true color image first to reduce the size of the secret image, which we needed to transfer it over the communication channel.
- Scrambled the resulted above image using suggested encryption method by making xor operation between the byte of the LL secret image and the bits resulted from this method..
- Preparing the cover image, which used for hiding the resulted scrambled secret image then the stegoimage resulted.

In the extracted stage:

















- Take the stego image and reconstructed the hidden scrambled secret image.
- Deciphering the hidden secret image by making xor operation between the byte of scrambled secret image and the bits of suggested encryption method.
- Apply the IDWT on the resulted secret image to reconstructed it to the original size of the secure image..
- Extract the cover image and the secret image.

All of the above stage can be seen briefly in the tables from (1) to (5) ,where the first table explain the implementation of the DWT on the secure true image then apply the suggested encryption algorithm for ciphering and deciphering, whereas the second table

show the affected of the encryption process on the image as show in the histogram, while the third table show the application of the steganography algorithm on the cover and cipher true image and the reconstruction

process, in table (4) show the histogram of the cover and stego image, finally in table (5) described the implementation of the performance metrics on the cover and stego image :

Table (1) explain the implementation of the DWT on the secure true image then apply the suggested encryption algorithm for ciphering and deciphering

The secure image	Apply DWT	Cipher image	Decipher image
			
			
			
			

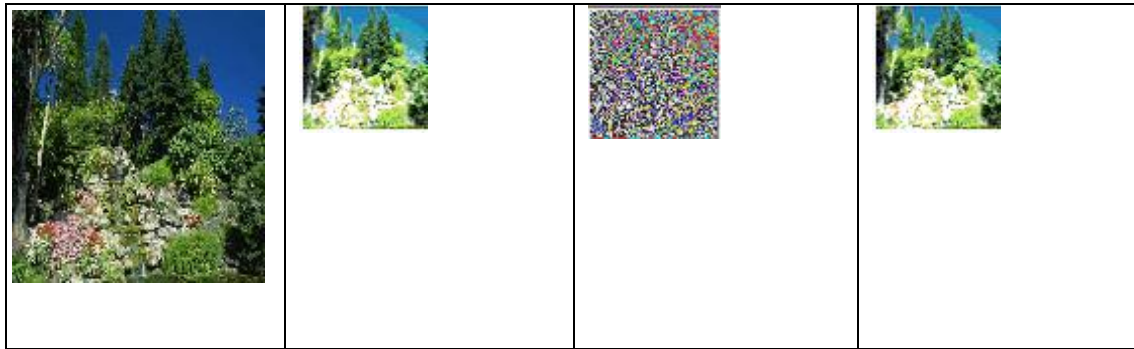

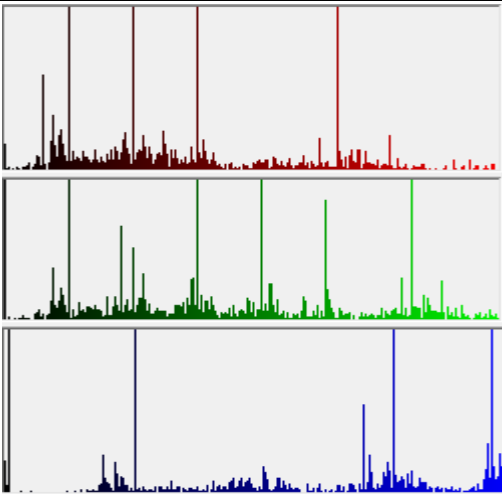
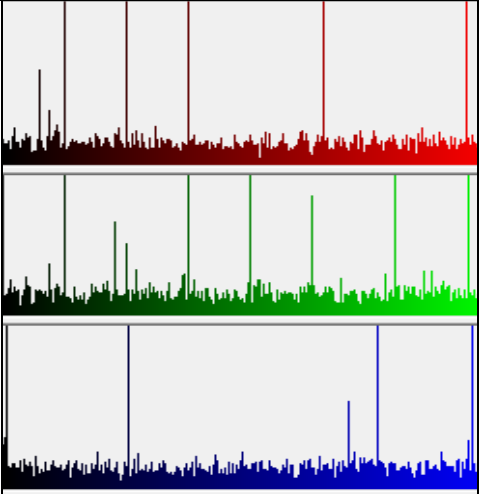

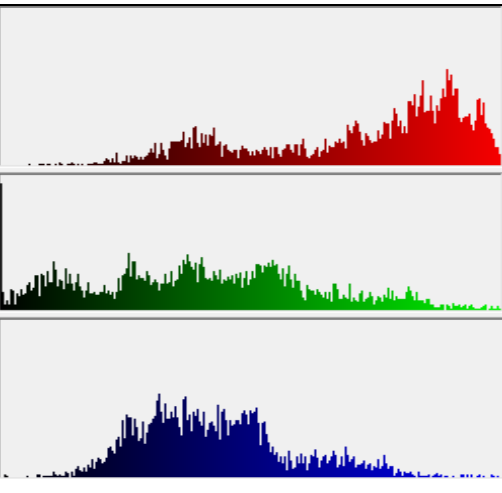
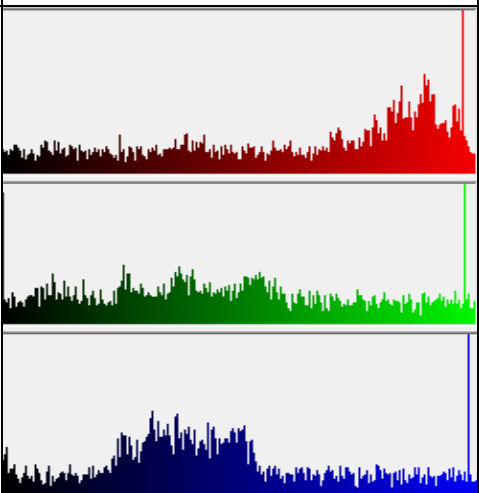
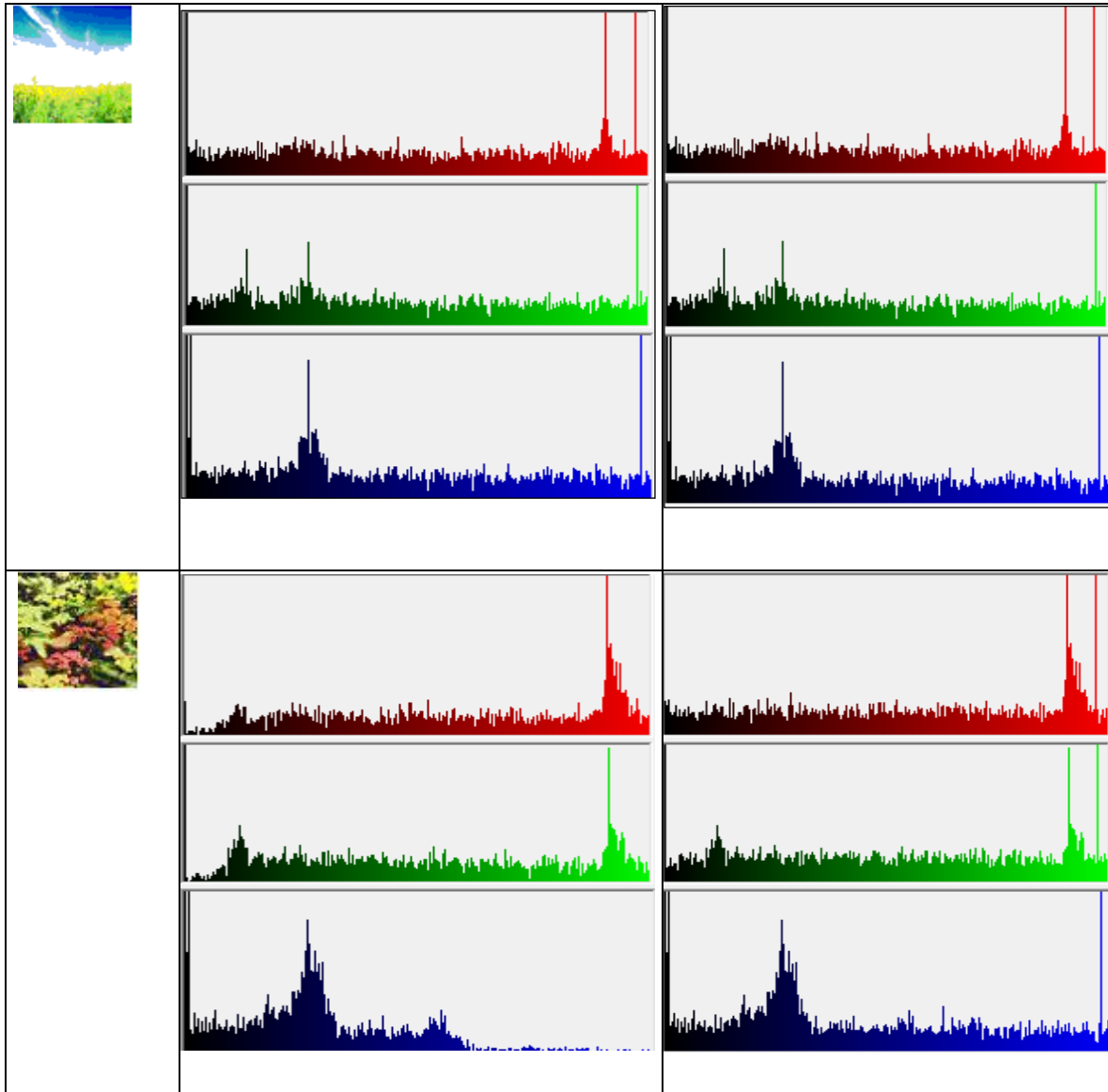


Table (2) show the affected of the encryption process on the secure image as show in the histogram

The DWT secure image	The histogram of DWT secure image	The histogram of the cipher DWT secure image
		
		



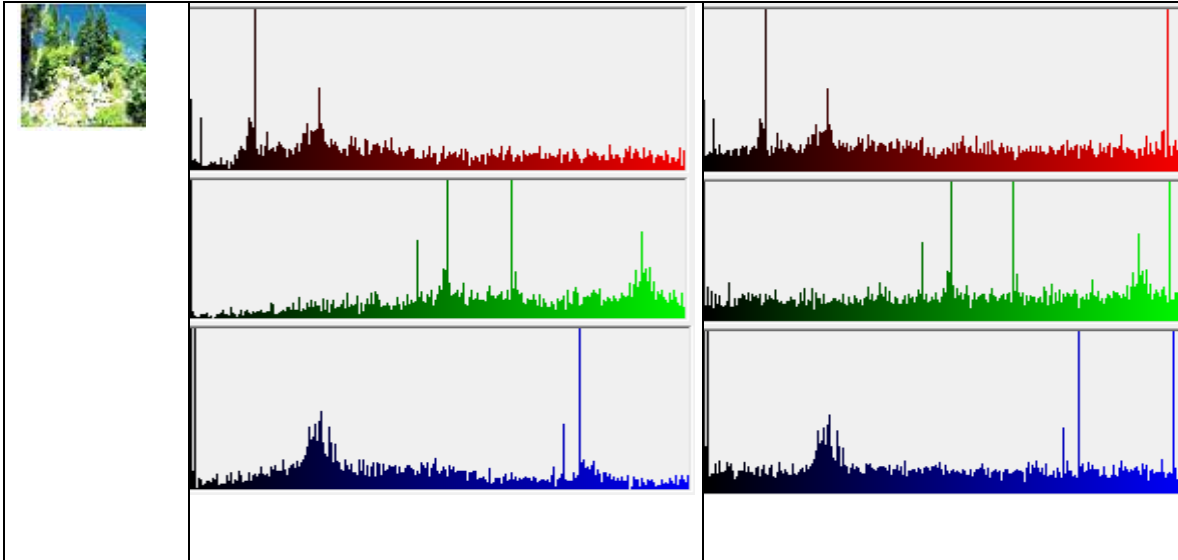


Table (3) show the application of the steganography algorithm on the cover and cipher true image and the reconstruction process

The cover image	The DWT secure image	Encryption of DET	Stego image	Extracted secret image

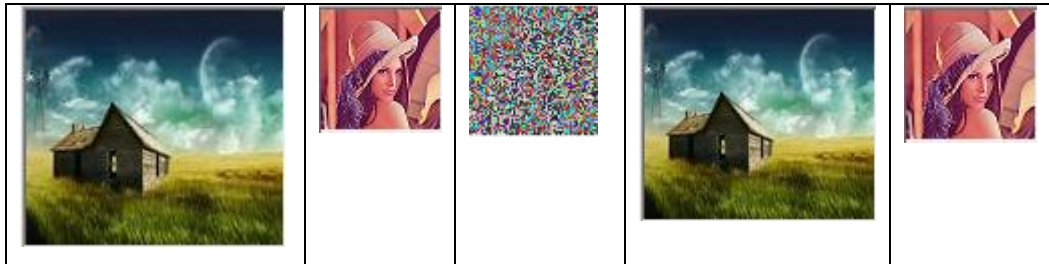

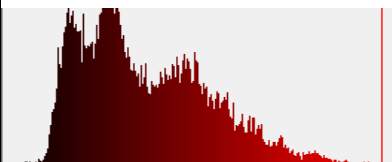
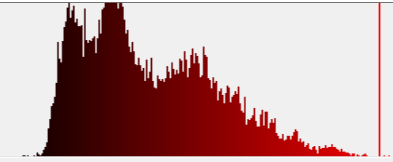
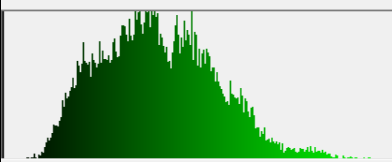
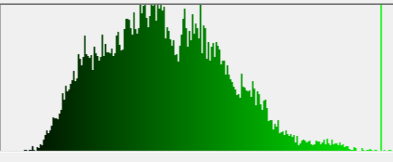
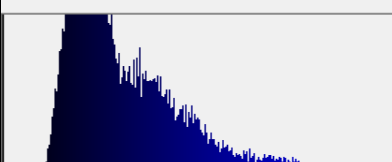
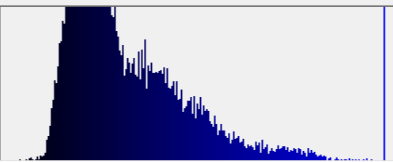

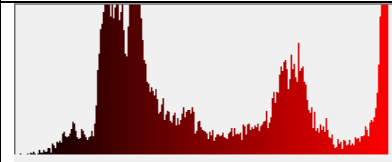
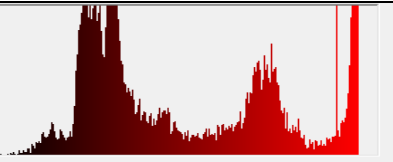
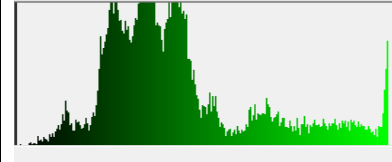
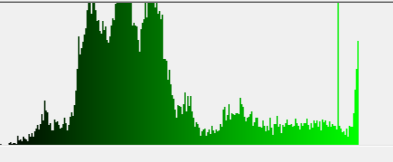
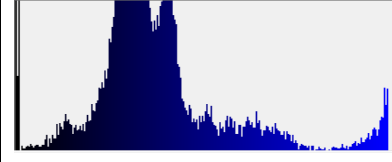
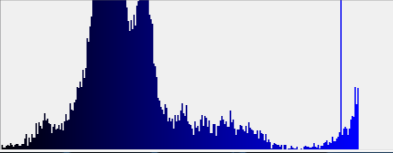


Table (4) show the histogram of the cover and stego image

The cover image	The histogram of cover image	The histogram of the stego image
		
		
		
		
		
		

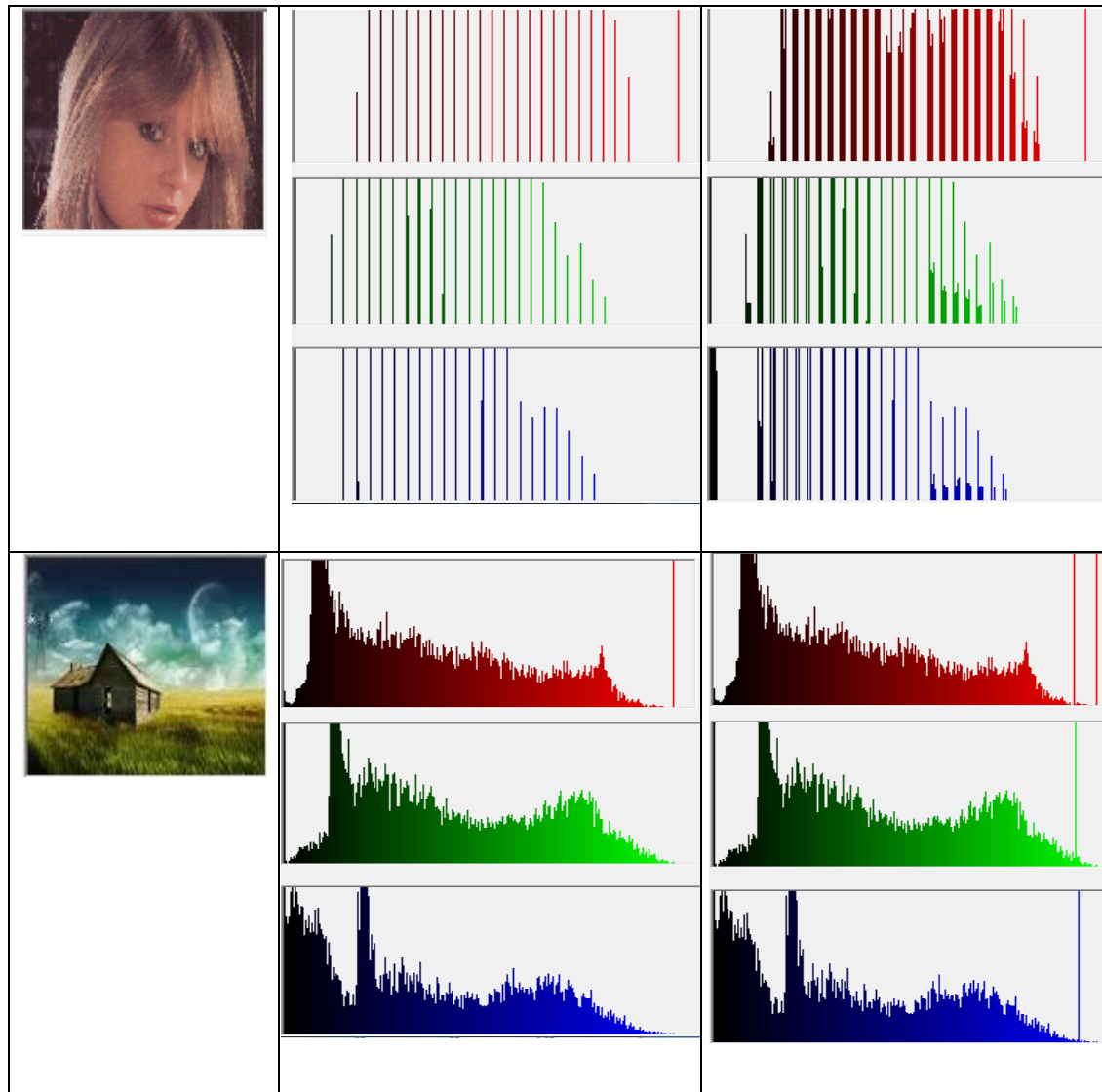





Table (5) described the implementation of the performance metrics on the cover and stego image

The image	AD	MSE	SC	NK	PSNR
	0.0125732421875	0.583984375	0.9997844273390 23	0.99981617034 182	154.58896346936

	-0.05322265625	0.57745361328125	1.0009730282621	1.00044494761	158.112742442548
	0.14666748046875	0.53581237792968	0.9967093283069	0.99830661597	168.482488871287
	0.023681640525	0.58511352539062	0.9995004219713	0.99967682783	154.290546515341

V. Conclusions

1. The using of DWT and suggested encryption method, which could be proven a highly secured and efficiency method for data communication.
2. This study presented a system that combined Steganography, with cryptography, which is a powerful tool that enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place.
3. The proposed method provides acceptable image quality with very little distortion in the image.
4. The main advantage of this Crypto/Stegno System is that the method used for encryption, proposed encryption method, is very secure and the DWT transformation ,LSB steganography techniques are very hard to detect.
5. The using of DWT allow to hiding secure image in cover image with the same size or larger than it.
6. The LSB steganography method added another level of security to the secret image.

References:

- [1] Menezes, Alfred , Paul C van Oorschot ,Scott A. Vanstone, — Handbook of Applied

Cryptography. CRC Press□ , October 1996 , ISBN 0-8493-8523-7.

- [2] William Stallings, —Cryptography and Network Security: Principles and practices□ , Pearson education, Third Edition, ISBN 81-7808-902-5.
- [3] N. Provos and P. Honeyman, —Hide and seek: An introduction to steganography,□ IEEE Security and Privacy Mag.□ , 2003, vol. 1, no. 3, pp. 32–44,.
- [4] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science, Springer, 1998. Pp. 32-47.
- [5] Ms. G. S. Sravanthi, Mrs. B. Sunitha Devi, S. M. Riyazoddin & M. Janga Reddy, "A Spatial Domain Image Steganography Technique Based onPlane Bit Substitution Method",Global Journals Inc. (USA),Volume 12 Issue 15 Version 1.0 Year 2012.
- [6] P.Saxena, S.Garg and A.Srivastava,"DWT-SVD Semi-Blind Image WatermarkingUsing High Frequency Band", (ICCSIT'2012) Singapore April 28-29, 2012.

- [7] Panrong X., "Image Compression by Wavelet Transform", East State University, Master Thesis, 2006.
- [8] P. Rajkumar ,R. Kar,A. K. , H. Dharmasa,"A Comparative Analysis of Stegano graphic Data Hiding within Digital Images",International Journal of Computer Applications (0975 – 8887) Volume 53– No.1, September 2012.