# Color Images Hiding Based on Wavelet Based Fusion

Saddam Kamil Alwane

Received on: 9/5/2011
Accepted on: 6/10/2011

.

## Abstract

At present, information is being communicated and proceeds automatically on a large scale. Hence, the required measures for secure storage and transporting of the information are increased. The protection of the information is necessary to guard economic interests, to prevent fraud, to guarantee the privacy of the citizen, etc.

In this paper, a new steganographic system with high capacity is proposed.

The proposed algorithm chooses wavelet transform techniques for embedding to achieve a robust system. The main idea of the proposed system is called the wavelet based fusion. In this method, the wavelet decomposition of the cover image and the secret image are merged into a single result called stego-image.

**Keywords:** Steganography, Wavelet Fusion, Security, Embedding parameters,Imperceptibility

.

## اخفاء الصور الملونة بالاعتماد على انصهار المويجات

### الخلاصة

في الوقت الحاضر, تطورت الاتصالات و نمت بشكل هائل جداً. فقد أصبحت المعلومات تتناقـــل بانسيابية عالية و على نطاق واسع. لذلك تطلّب مقاييس إضافة للخزن والنّقـــل الآمـــن للمعلومـــات. فحماية المعلومات  يحتمل أن تكون ضرورية في حراسة اهتمامات اقتصادية،آو أن تمنع احتيالاً ،آو أن تضمن خصوصية المواطن، الخ.

في هذا البحث تم اقتراح نظام جديد لإخفاء الصور، ذي سعة عالية. فللنظام المبتكـــرتم اختيـــار تقنية حيز التحويل لغرض الاخفاء من اجل الحصول على نظام متين.   الفكرة من النظـــام المبتكـــر تسمى المويجة معتمدة الاندماج(wavelet based fusion ). في هذه الطريقـــة, تحليـــل المويجـــة للصورة الغطاء والصورة السرية يتم مزجه لتكوين الصورة المضمنة(stego-image)  .

## 1. Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means "covered writing." It includes a vast array of secret communication methods that conceal the message's very existence. Though steganography is an ancient craft, the onset of computer technology has given it new life. Computer-based steganographic techniques introduce changes to digital covers to embed information foreign to the native covers [1].

The main problem of image hiding in another host image is the large amount of data that requires a special data embedding method with high capacity as well as transparency and robustness.

In this paper, the system has been proposed to embed a color image into a color cover image choose a transform domain technique for embedding to achieve a robust system, the main idea of the proposed system is called the wavelet based fusion. In

* Computer Engineering & Information Technology Department, University of Technology/Baghdad

https://doi.org/10.30684/etj.29.15.10
2412-0758/University of Technology-Iraq, Baghdad, Iraq

this method, the wavelet decomposition of the cover image and the secret image are merged into a single image result.

### 1.1 Related Work

Raja et al (2006), [14], proposed a system to hide message in image by using DWT for the cover image. The secret message is first scrambled then embedded in cover coefficients by using PN sequence. The quality of the stego image of the proposed method is very close to that of the original one. Yuan-Yu Tsai and Chung-Ming Wang (2007), [15], has proposed a novel data hiding scheme for color images using a BSP tree. This method shows high capacity with little visual distortion. Furthermore, there is an advantage of the tree data properties to improve the security of embedding process, making it difficult to extract the secret message without the secret key provided. L.Y. Por et al. (2008), [16], proposed a combination of three different LSB insertion algorithms on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden from intercepting the transmission of the covert data during a communication because the stegokey is only known by the sender and the receiver. Chin-Chen Chang et al (2009), [12], proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on wet paper coding. H S Manjunatha Reddy& K B Raja (2010), [17], proposed High Capacity and Security Steganography using discrete wavelet transform (HCSSD), The wavelet coefficients of both the cover and payload are fused into single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to reduce the

pixel range to ensure the payload is recovered accurately at the destination. Note that the Cover and payload images are grayscale uncompressed images, i.e., color images are converted into grayscale images.

## 2. The Basic Model of Steganographic System

The following terms are used along the embedding and extraction process:

- Cover-object,C: the original object where the message has to be embedded. Cover-text, cover-image.
- Message, M: the message that has to be embedded in the cover-object. It is also called stego-message or in the watermarking context mark or watermark.
- Stego-object, S: The cover object, once the message has been embedded.
- Stego-key, K: The secret shared between A and B to embed and retrieve the message [2].

The embedding function E is a function that maps the tripled cover-object C, message M and stego-key K to a stego-object [3]

$$E(C, M, K) = S \ldots\ldots\ldots\ldots\ldots (1)$$

## 3. Steganalysis

Steganalysis is the comparison between the carrier (cover), stego-image and the hidden message. In other meaning steganalysis is an attempt to detect the existence of hidden information [4]. The various methods used to analyze stego-message are termed attacks and include:

- Stego-only attack: Only the stego-object is available for analysis.

- Known cover attack: The “original” cover object and stego-object are both available.
- Known message attack: At some points, the attacker may know the hidden message. Analyzing the stego-object for patterns that correspond to the hidden message may be beneficial for future attacks against that system. Even with the message, this may be very difficult and may even be considered equivalent to the stego-only attack.
- Chosen stego attack: The steganalyst generates a stego-object from steganography tool or algorithm from a chosen message. The goal in this attack is to determine corresponding patterns in the stego-object that may point to the use of specific steganography tools or algorithms.
- Known stego attack: The steganography algorithm (tool) is known and both the original and stego-objects are available.

## 4. Image Analysis

- **Image Resizing**

It means the change of image size to reduce or to enlarge an image. When one reduces the size of the image, either bilinear or bicubic interpolation can be used. Interpolation is the process used to estimate image values at a location in between image pixels. There are three interpolation methods: Nearest-neighbor interpolation, Bilinear interpolation and Bicubic interpolation [5].

- **Image Histogram**

An image histogram is a chart that shows the distribution of intensities in an image. The image histogram function procedure creates this plot by marking $n_k$ equally spaced bins (frequency of occurrence), each representing a range of data values .It then calculates the number of pixels within each range [6].

- **Image Fusion**

The fusion of images is the process of combining two or more images into a single image retaining important features from each. The most common form of transform image fusion is wavelet transform fusion. In common with all transform domain fusion techniques, the transformed images are combined in the transform domain using a defined fusion rule then transformed back to the spatial domain to give the resulting fused image. Wavelet transform fusion is more formally defined by considering the wavelet transforms $\boldsymbol{\omega}$ of the two registered input images $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ together with the fusion rule (Ø). Then, the inverse wavelet transform $\boldsymbol{\omega^{-1}}$ is computed, and the fused $\boldsymbol{I}$ is reconstructed [8].

$$I = w^{-1}(f(w(I_1),w(I_2))) \ldots \quad (2)$$

where, $\boldsymbol{\omega}$ is the wavelet transform, $\boldsymbol{\omega^{-1}}$ is the inverse wavelet transform., $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ are the input images, $\boldsymbol{I}$ is the fused image.

This process is depicted in Figure (1)

## 5. Wavelet Transform

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients[7]. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Horizontal band (LH), Vertical Band (HL), and diagonal detail band (HH)[17].

Each subband provides different information about the image. The LL subband is a coarse approximation of the image and removes all high frequency information. The LH subband removes high frequency information along rows and emphasizes high frequency information along the columns, thus capturing the horizontal edges. The HL subband emphasizes vertical edges, and the HH subband emphasizes diagonal edges. To compute the DWT of the image at the next scale, the process is applied again to the LL sub band [10]. Further, N-level of decomposition is applied over the low- low (LL) subband, as shown in Figure (3).

## 6. Pseudorandom Sequences Generation

Random sequence is a series of numbers which when observed for a sufficient time interval, exhibits independence of any previous or future time intervals. The sequences generated by shift register are not truly random, being finite in length. The length of the sequence varies with the length of the shift register. The sequence repeats itself periodically; hence the name pseudorandom sequence. Even so, there are certain properties associated with *PN* codes that agree with the concept of randomness. The sequence generated by shift register is a series of binary bits (1's or 0's) [11].

The proposed *PN* here must be compatible with number of pixels in cover image [12]. The purpose of using the *PN* is to distribute the secret image bits over very wide range of cover pixels which may increase the imperceptibility of the stego- image as well as to increase the robustness**,** which is the main important property of the steganographic systems, against attacks which try to remove the secret image.

## 7. The proposed system

In the proposed steganographic algorithm will be used three PN are :

- ***PN1****:* this PN is used to select random host pixels from the decomposed image.
- ***PN2***: this PN is used to select the position within the host pixels bits to insert the secret image coefficients.
- ***PNe*** : to increase the robustness of their proposed algorithm, PNe is used

to cipher the secret image by transposition of the pixels. This PN must be compatible with the number of secret image pixels.

The general model of the proposed system includes two parts:

- Sender part.
- Recipient part.

### 8.1 Sender part

Several stages are proposed in the sending process to achieve the goal of information hiding. Figure (4) shows the sender process.

### 8.1.1 Stages of the sending process

**Stage 1 Wavelet Decomposition:**

The aim of decomposition is to separate the low frequency component, which has the most energy of the image, from the high frequency component.

For wavelet transform, the cover image is decomposed up to 4 levels using Haar wavelet transform. Figure (5) show the 4-levels decomposition on a Lena covered image.

After wavelet decomposition, the result converted into a vector form (V) in which the wavelet coefficients using bit form for each coefficient. So, three vectors will be generated (V-red,V-green,V-blue)).

**Stage 2 Ciphering Process**

A transposition ciphering, which is based on changing the position of the pixels of the secret image, has been carried out. The transposition ciphers rearrange pixels according to some pre-defined scheme. In the case of image, there are many algorithms that could be used to rearrange the original image data. One of these algorithms, which are selected in this paper, is the use of PN-sequence (PNe) to get scrambled image.

The selected color secret image and its ciphering are shown in Figure (6).

**Stage 3 Wavelet Decomposition of Secret Image**

The ciphered secret image is transformed to one level DWT using Haar wavelet transform. The coefficients are converted to a binary form.

**Stage 4 Embedding Process**

Embedding process has been achieved by embedding the 1-level decomposition for the ciphered secret image into the 4-level decomposition of the cover image. The coefficients obtained in the wavelet decomposition are randomly selected from the vectors V according to a pseudorandom sequence, which is named PN1.

The embedding process will place the bits of ciphered secret image instead of selected bits from the coefficient of the cover image. The selection of which bits will be taken as a host depends on another pseudorandom sequence named PN2. This process is repeated until all the bits of ciphered secret image are completely embedded in the coefficients.

**Stage 5 Wavelet Reconstruction**

After all bits of the ciphered image are successfully embedded in the coefficients, new vectors of coefficients will be obtained. For wavelet coefficients (vectors V), taking inverse wavelet transform and using the same filters according to the filter and levels used in decomposition process and concatenation between the three layers (R,G,B), will reconstruct the original image. This image is called Stego-image. As a result, the stego-image is completely similar to the original cover, as shown in Figure (8).

The proposed system is embedding a color secret image into a color cover image. The 2D DWT is applied for each color plane (Red, Green, Blue) of both images separately. Four level DWT is applied for the cover image, while the secret image is ciphered by using the PN-sequence PNe to get scrambled image and then converted into one level DWT. For the two images, Haar wavelet transform is used as a wavelet filter.

The embedding process depends on two PN-sequences, PN1 for choosing the suitable coefficient for embedding and PN2 to select the bits in the cover image coefficients to replace them with the secret image coefficients. Each color plane in the secret image is embedded in the corresponding color plane from the cover image. This process is illustrated in Figure (9).

### 8.1.2 The Histogram of Test

The test can be implemented with these chosen images:

- The secret image (Helicopter (128*128)) color image.
- The cover image (Lena (256*256)) color image.

The histogram of the cover image Shown in the Figure (10) and the histogram of the stego-image shown in the Figure (11)

As shown from Figure (10) and Figure (11), the histogram of the cover image does not differ from the histogram of the stego-image.

To prove this similarity, the histogram result for subtraction of the cover image from the stego image will be as shown in Figure (12).

### 8.2 Recipient part

The recipient will certainly get the stego-image, but he could not extract the secret information out of the cover without the knowledge of which keys (PN1, PN2 and PNe) have been used in the embedding process. The block diagram of this part is shown in Figure (13). The extracting process will be started. This can be done by handling the stego-object by 4-level wavelet decomposition using the same filters used in the sender stage, the coefficients results are rearranged in a manner similar to that in the sender. The secret image will be extracted by using the same PN1 and PN2 used in the sender to select the coefficients where the data has been embedded and the same PNe for deciphering process. By taking the inverse of the ways used in embedding process, the secret image is perfectly reconstructed.

The recipient will certainly get the stego-image. The extraction of secret image cannot be done without previous knowledge of which keys PN1, PN2 and PNe have been used in the embedding process. This process is shown in Figure (14).

Several tests have been applied to several images shown Figure (15), and the results were as in the table (1), the results were compared with the results of the reference [17].

### 9.Conclusions

- The proposed system hides the secret image in the cover image based on wavelet based fusion method, this lead to increase the imperceptibility of the system.
- The combination of the steganography with the cryptography techniques is used in this work to increase the level of security. Even if the attacker knows the embedded image, it is difficult for him to known the original image, since it is scrambled before embedded.
- The histogram test proved that the histogram of the stego-image is similar to the histogram of the cover image. That means the attacker cannot

distinguish between the statistics of stego-image and cover image.

- The results that were obtained from a variety of tests as in Table 1 that the system is aimed at security, since the correlation value approaches one and high PSNR value (PSNR equals up to 44.9752dB). Also if the capacity of embedded images increases then the PSNR and Correlation will be decreased.

## References

[1] Petitcolas F.A.P., Anderson R.J., and Kuhn, M.G., **"Information Hiding-a Survey"** Proceedings of the IEEE, (2006).

[2] Johuson, Neil F., Duric, Zoron, Jajodia (Information Hiding: Steganography and watermarking Attacks and Countermeasures) Kluwer Academic Publishers, 2008.

[3] D.Sellars**, "An Introduction to Steganography**". **URL**:http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/ds.../stego.htm .

[4]Gaetan Le Guelvouit, **"Trellis-Coded Quantization for Public-Key Steganography,"** IEEE International conference on Acostics, Speech and Signal Processing, pp.108-116, 2008.

[5]Shilpa P. Hivrale, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar **"Statistical Method for Hiding Detection in LSB of Digital Images: An Overview"** World Academy of Science, Engineering and Technology, vol. 32, pp. 658-661, 2008.

[6]Babita Ahuja and, Manpreet Kaur, **"High Capacity Filter Based Steganography,"** International Journal of Recent Trends in Engineering, vol. 1, no. 1, pp.672-674, May 2009.

[7]Debnath Bhattacharyya, Poulami Das, Samir kumar Bandyopadhyay and Tai-hoon Kim**, "Text Steganography: A Novel Approach,"** International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.

[8] Paul Hill, Nishan Canagarajah and Dave Bull" **Image Fusion using Complex Wavelets**",Dept. of Electrical and Electronic Engineering. The University of Bristol -Bristol, BS5 1UB, UK-2007.

[9]Jan Kodovsky, Jessica Fridrich **"Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain"** Proceedings of SPIE, the International Society for Optical Engineering, vol. 6819, pp. 681902.1-681902.13, 2008.

[10] Rafael C. Gonzalez, "**Digital Image Processing**", Second Edition University of Tennessee Richard E. Woods MedData Interactive Prentice Hall (2007).

[11] Jain A.K. "**Fundamentals of Digital Image Processing**" Prentoce-Hall, 2004.

[12]Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, " **steganography scheme based on wet paper codes suitable for uniformly distributed wet pixels,"** IEEE International Symposium on circuits and Systems, pp. 501-504, 2009.

[13] G. Voyatzis et al**,"Digital Watermarking:An Overview"**, euspico, vol. 1, pp.9-12, 2006.

[14] K B Raja, Venugopal K R , L M Patnaik ***(High Capacity Lossless Secure Image Steganography using Wavelet)*** Proce. IEEE 2006.

[15] Yuan-Yu Tsai, Chung-Ming Wang ***"A novel data hiding scheme***

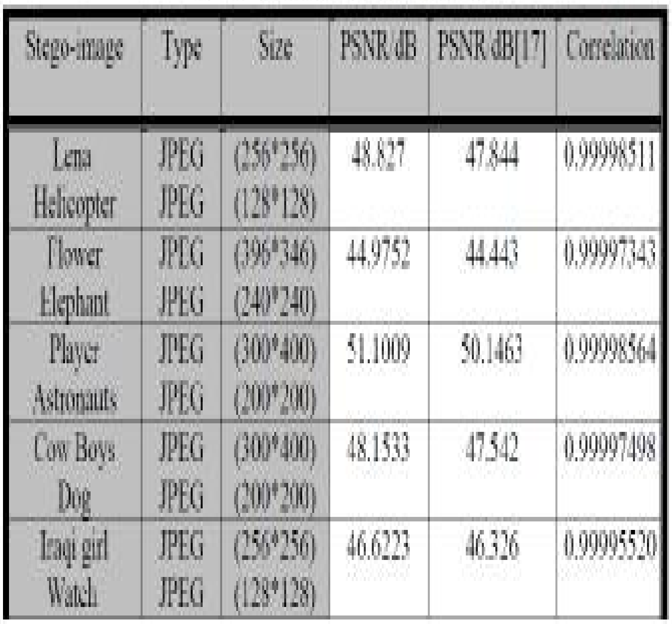
***for color images using a BSP tree”*** Journal of systems and software, vol.80, pp. 429-437, 2007.

[16] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, B. Delina,

**“StegCure: A Comprehensive Steganographic Tool using Enhanced LSB Scheme,”** Journal of WSEAS Transctions on Computers, vol. 8, pp. 1309-1318, 2008.

[17] H S Manjunatha Reddy& K B Raja **"High Capacity and Security Steganography using Discrete wavelet transform"** Dept. of Electronics and Communication Global Academy of Technology, Bangalore, India, 2010.

Table (1) PSNR and Correlation of Testes



| Stego-image | Type | Size | PSNR dB | PSNR dB[17] | Correlation |
|---|---|---|---|---|---|
| Lena<br>Helicopter | JPEG<br>JPEG | (256*256)<br>(128*128) | 48.827 | 47.844 | 0.99998511 |
| Flower<br>Elephant | JPEG<br>JPEG | (396*346)<br>(240*240) | 44.9752 | 44.443 | 0.99997343 |
| Player<br>Astronauts | JPEG<br>JPEG | (300*400)<br>(200*200) | 51.1009 | 50.1463 | 0.99998564 |
| Cow Boys<br>Dog | JPEG<br>JPEG | (300*400)<br>(200*200) | 48.1533 | 47.542 | 0.99997498 |
| Iraqi girl<br>Watch | JPEG<br>JPEG | (256*256)<br>(128*128) | 46.6223 | 46.326 | 0.99995520 |

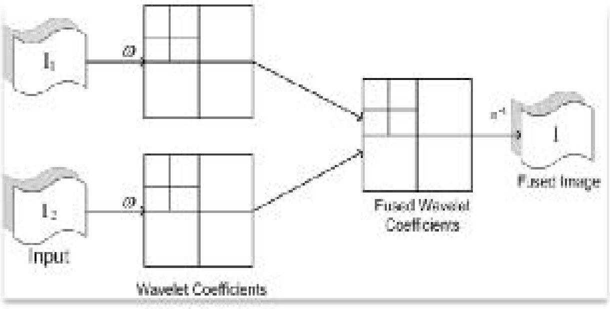


Figure (1) Fusion of the wavelet transforms of two images

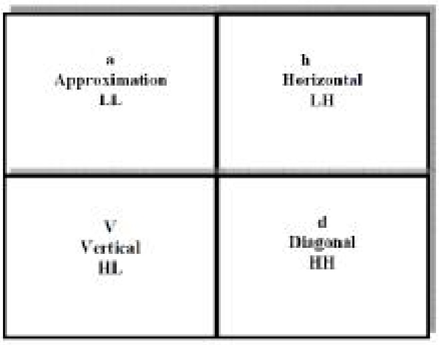


Figure (2) 1-level 2D- DWT representation of an image.

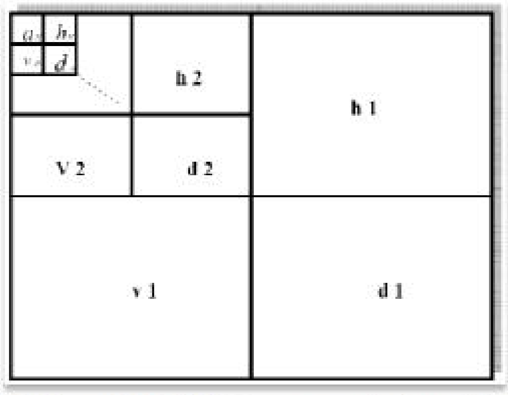


Figure (3) N-Level-2D-DWT representation of an image.

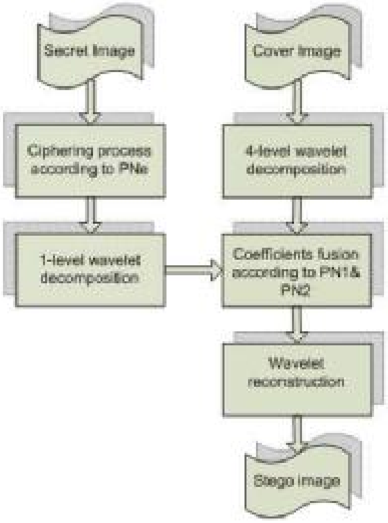
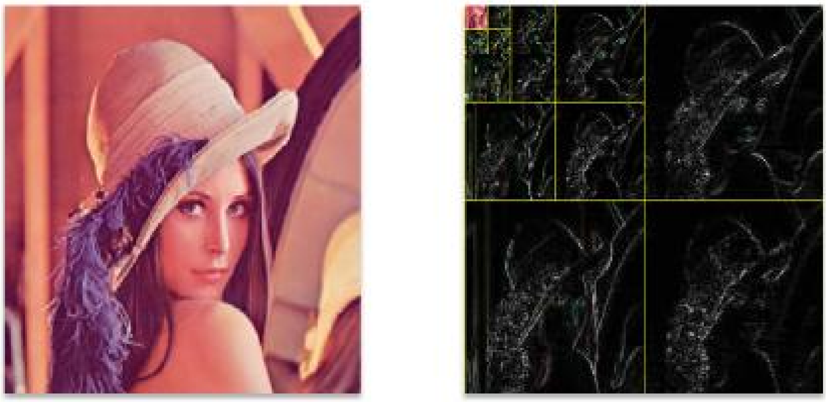

Secret Image
Cover Image
Ciphering process according to PNs
4-level wavelet decomposition
1-level wavelet decomposition
Coefficients fusion according to PN1& PN2
Wavelet reconstruction
Stego image

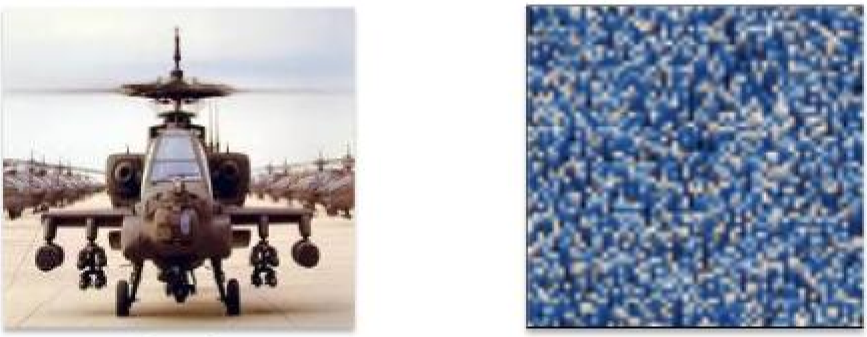
Figure (4) The main algorithm of sender process



a. The Cover Image

b. The 4-level DWT

Figure (5) DWT of the cover image



a. Secret Image

b. Ciphered Image

Figure (6) The Color Secret Image

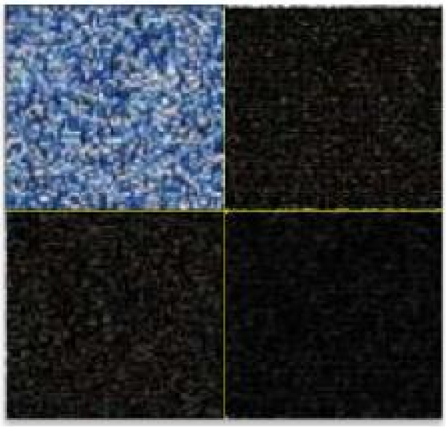


Figure (7) 1-level decomposition for ciphered secret image.

a. Cover Image

b.Stego-Image

Figure (8) The similarity between cover image and stego-image.

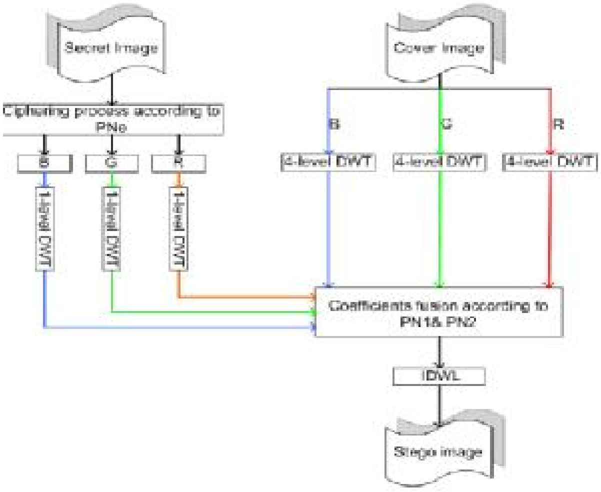


Figure (9) Embedding Process

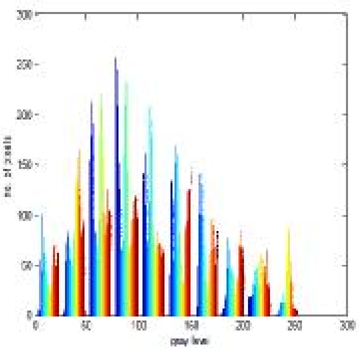


Figure (10)
Histogram for the cover image.

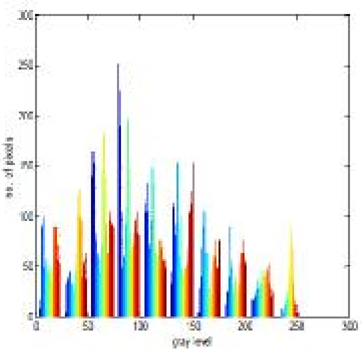


Figure (11)
Histogram for the stego image.

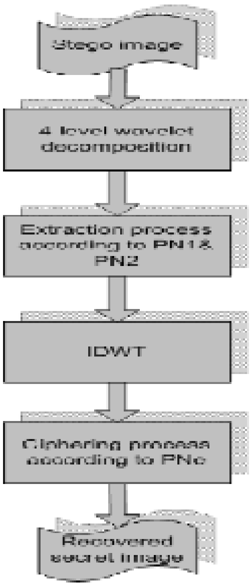

Stego image
4 level wavelet decomposition
Extraction process according to PN1& PN2
IDWT
Ciphering process according to PNe
Recovered secret image

Figure (13) Recipient Process

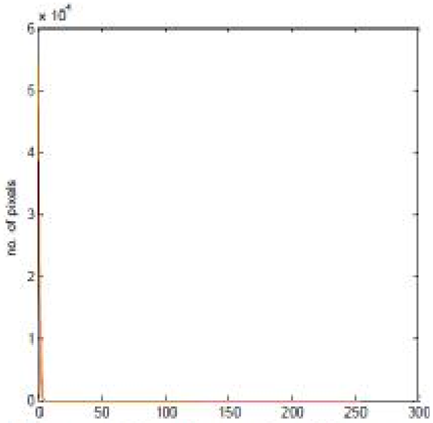


Figure (12) subtraction histogram

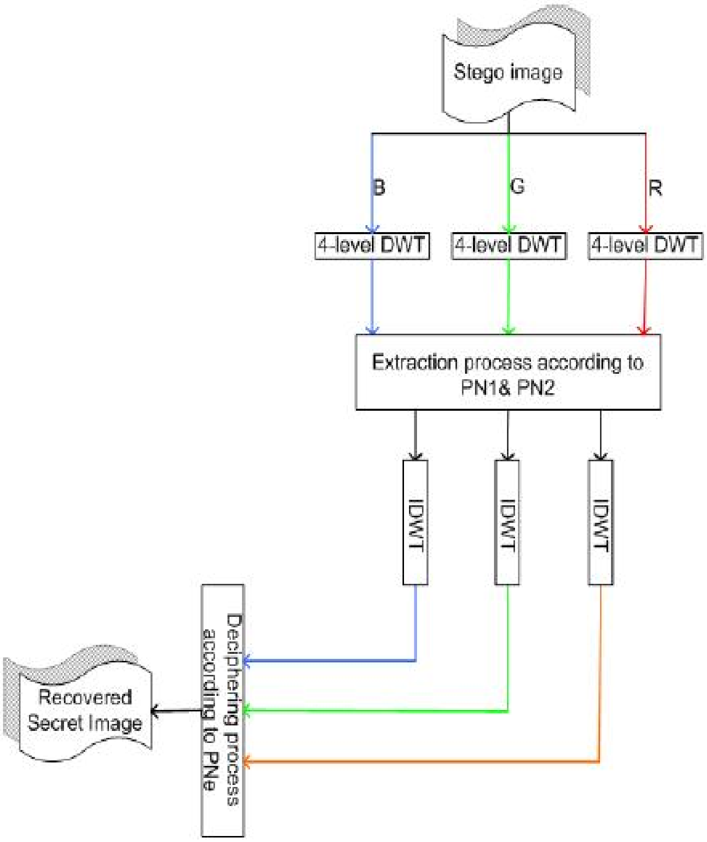
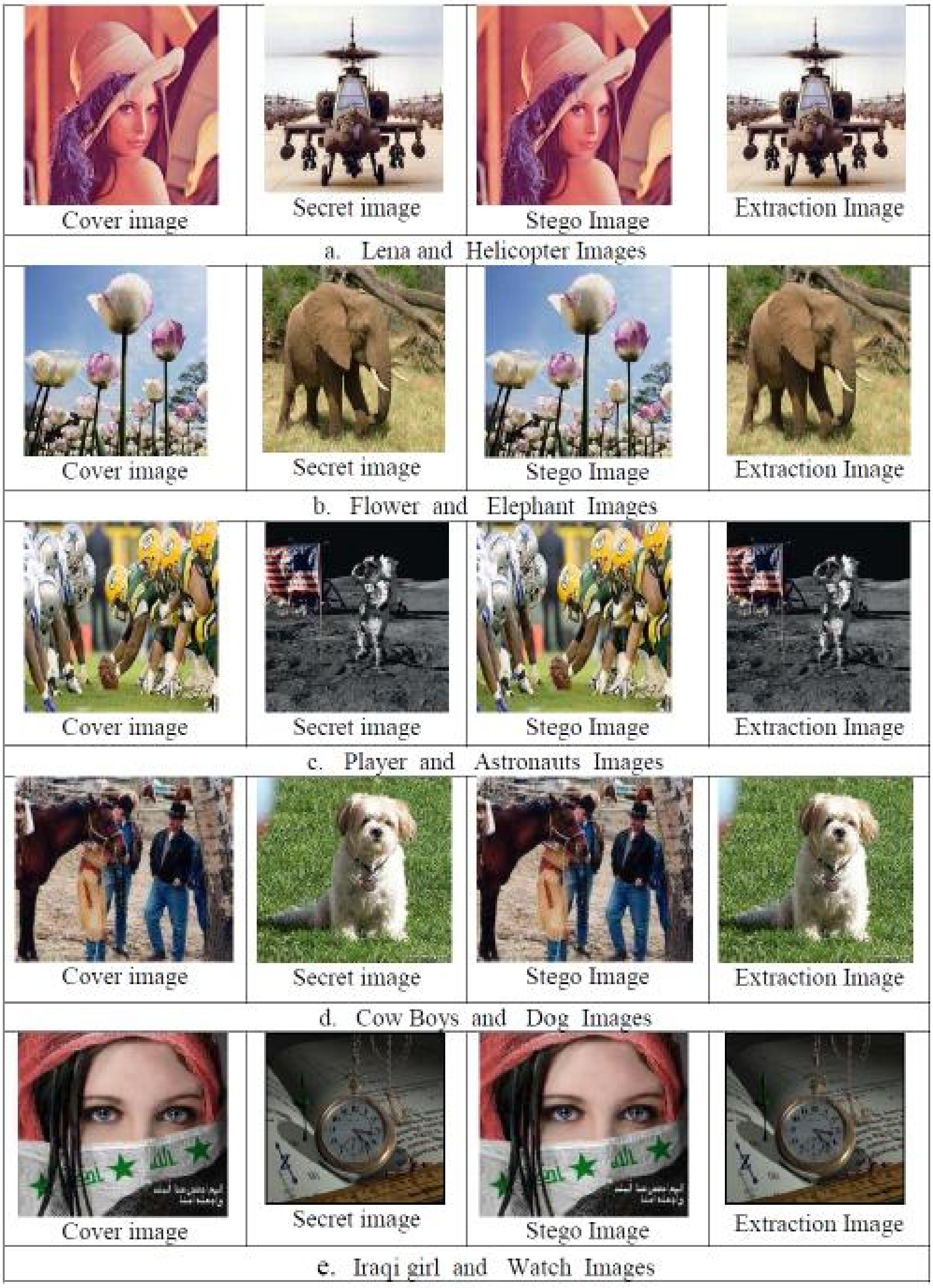


Figure (14) Extraction Process



a. Lena and Helicopter Images

b. Flower and Elephant Images

c. Player and Astronauts Images

d. Cow Boys and Dog Images

e. Iraqi girl and Watch Images

**Figure (15) Several tests of Images**