ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 7, October 2014

Implementation and Evaluation of Steganography using PN Sequences Based on Wavelet

Dr. Eng. Saad M. Khaleefah Al-Janabi
Ass. .Prof
AL-Turath College University
Iraq-Baghdad

Abstract:

Steganography means the use of a cover image to hide a bits of information or images in away that it is imperceptible to an observer . We use the Wavelet transforms because it gives perfect reconstruction of the original image. we proposed an algorithms that embeds the message bits stream in the LSB s of the wavelet coefficients of a color image reach up to half cover image. The algorithm used the PN sequence as a key for embedded and extracting in order to recover the embedded message without lose of quality of image. We use the MATLAB to implement the two Algorithms one for implements the embedding procedure the another for implements the Extracting procedure . The results showed the high invisibility of the proposed model even with large message size were embedded .

1. Introduction

This method based on hiding bits of image or message in the coefficients of wavelet transformation. The bits of information reach to four bits as the capacity of information increase the degradation of image increase but in our method there is no degradation happen depends on the chosen the cover image [1].

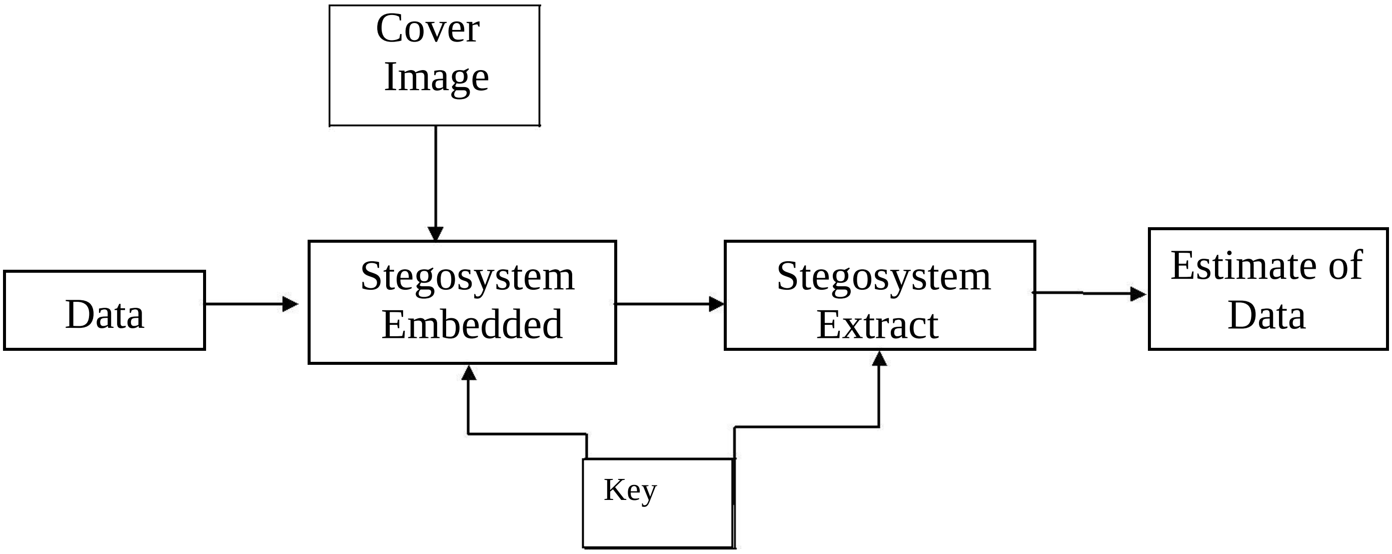

Figure (1) Steganographic system

The image covers taken the Haar transform and then made threshold which is flux able and put the binary representation of the image or text. Instead of bits of threshold and then take the inverse Haar transform, hence we get the stego-image which contain the cover image with the secret information.

At the extraction first we take the Haar transform for the modified image, and then make threshold and extracted the bits instead of threshold and combine these bits to obtain the original image or text.

The cover image is color, each color give us a four bits of information. The PN sequences generated at receiver and transmitter of the system are the same. The steganogrphic system shown in Fig. (1).

2. Wavelet Transforms

The wavelet domain is growing up very quickly. A lot of mathematical papers are published every month. Wavelets have been effectively utilized as a powerful tool in many fields signal processing, physics, astronomy, and image processing [2]. The input is convolved with a high pass filter and a low pass filter. The result of the latter convolution is a smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the syntheses filters and the results of these convolutions are added. In two dimensions, we first apply one step of the one dimensional transform to all rows. Then, we repeat the same for all columns. In the next step, we proceed with the coefficients that result from a convolution in both directions. As shown in figure (2), these steps result in four classes of coefficients: the (*HH*) coefficients represent *diagonal* features of the image, whereas (*HG* and *GH*) reflect *vertical* and *horizontal* information.

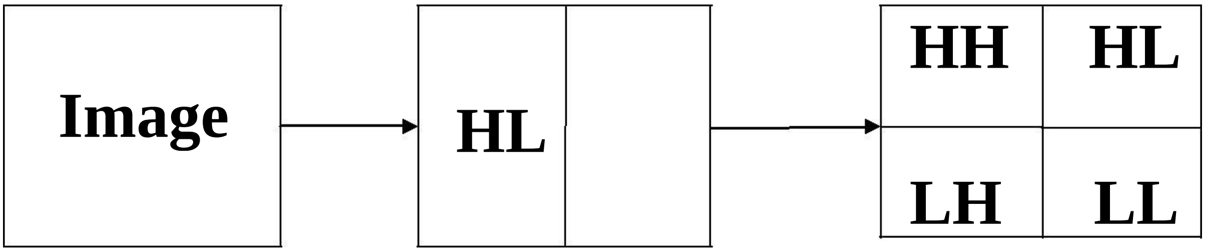

Figure (2) Two dimensional wavelet Transform

Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers we are able to characterize the output completely with integers [4].

The *Transform* is thus reversible and its inverse is given in equations (2a) and (2b).

$$s(n) = \left\lfloor \frac{x(2n) + x(2n+1)}{2} \right\rfloor \qquad (1a)$$

$$d(n) = x(2n) - x(2n+1) \qquad (1b)$$

$$x(2n) = s(n) + \left\lfloor \frac{d(n)+1}{2} \right\rfloor \qquad (2a)$$

$$x(2n+1) = s(n) - \left\lfloor \frac{d(n)}{2} \right\rfloor \qquad (2b)$$

3-Analysis

To find the number of bits imbedded we assumed that the colored image contains *XY* pixels, then every sub-band of its wavelet transform will contain 3*(*XY*/4) coefficients. So, the data payload of the proposed algorithm can be expressed using equations (3,4).

$$\text{Data payload} = 3 * 4(XY/4) * N \quad \text{bits} \qquad)3)$$

$$\text{Payload percentage} = \frac{3 * 4(XY/4) * N/8}{3XY} * 100\% = (N/8 * 100)\% \qquad)4)$$

The question now is: how many bits per coefficient can be embedded while keeping an acceptable visual quality of the stego image? We tried to answer that question by embedding the maximum possible message for each value of *N* (using equation 1) where *N* takes a value between 1 and 8. Judging the visual quality of the resultant stego images in each case showed that the visual quality of the stegoimages is acceptable for embedding up to 4-bits per coefficient of each color. So, substituting in equation (3) with *N*=4 results in an embedding capacity that represents 50% of the cover image.

The embedding process hide (*N)* message or images bits in the least significant bits (LSB) of the (WT) coefficients of the color cover image. Furthermore, we have used the four sub-bands of the image transform for embedding. Of course, after the embedding process ends the stego image is produced by applying the Inverse of the Wavelet Transform (IWT) on the modified coefficients [5].

PN function generator that is computationally feasible and secure. No body can guess the generated random sequence with out knowing the secret key. This ensures that only recipients who know the corresponding secret key will be able to extract the message or image from stego-image [6].

The input for the encoding algorithm is an input image *I* along with the information *that* needs to be embedded into *I*. The output is a modified image *I'* with the same dimensions as *I* [7].

$I' = T^{-1} (T(I)^{+} M)$ *where*
I' *is the modified image*
T^{-1} *is the inverse Haar transform*
T *is the Haar transform*

$\oplus$ *Is the embedding process*

M is the image or text

The embedded means hiding four bits of the secret or text after Haar transform and threshold of the coefficients[8] .

To recover the secrete image or text we used the transformation again of modified image and then extract the bits or image after threshold [9].

$I = T^{-1} (T(I') \ominus \textcircled{M})$

Where

I is the original image

T^{-1} *is the inverse Haar transform*

T is the Haar transform

$\ominus$ *The extracting process*

M image or text

4. The proposed method:

Our implementation is written in matlab

4.1. Embedded algorithm

- Choose color cover images which have a histogram flat this histogram is almost perfect distribution of pixel .which want to hide the secret image or text in it[10]

- Take the Haar transform of the color cover image according to the under equations for each color of the cover image. The Haar is divided the cover color image into four-quarter the upper-left is the cover image but with small scale. The three quarter is the shadow of the cover image and we can hide in these quarters, the secret image or the message. The cover image has dimension of (256 x 256) or (512 x 512) bits or up. The secret image we can hide in these images has dimension (128x128) or (128x72) bits as the dimension not equal we use zero padding to make its dimension equal is the square matrix.

- The secret image is gray scale and the dimension of the image not equal, we can use the Zero Padding to make the dimension equals.

- Determine the threshold level and the threshold level is flexible and remove these bits .As the secret image small enough the threshold is small as the secret image is large enough the threshold is large enough.

- Replace four bits by the bit of the information (image, text) for each color According to PN Sequences .

- We take the inverse wavelet transformation. We gate the modified image now we compare this image with the original image if we get RMES very small we get PSNR very high this is the best situation [11] .

- Store the stego-image or transmit it.The algorithm shown in fig (3)

4.2. Extraction algorithm

- Taking the wavelet transform of the stego-image in the receiver side. Haar is divided the stego-image into four quarter.

- Determine the threshold level and find the coefficient that are below that level and extracted the bits of data from these coefficients using the PN-sequence to reduce the noise.

- Extract the bits (text, image) from the coefficients.

- Combine the extracted data bits into an actual image or text.

- Output is the message or image . The algorithm shown in fig (4).

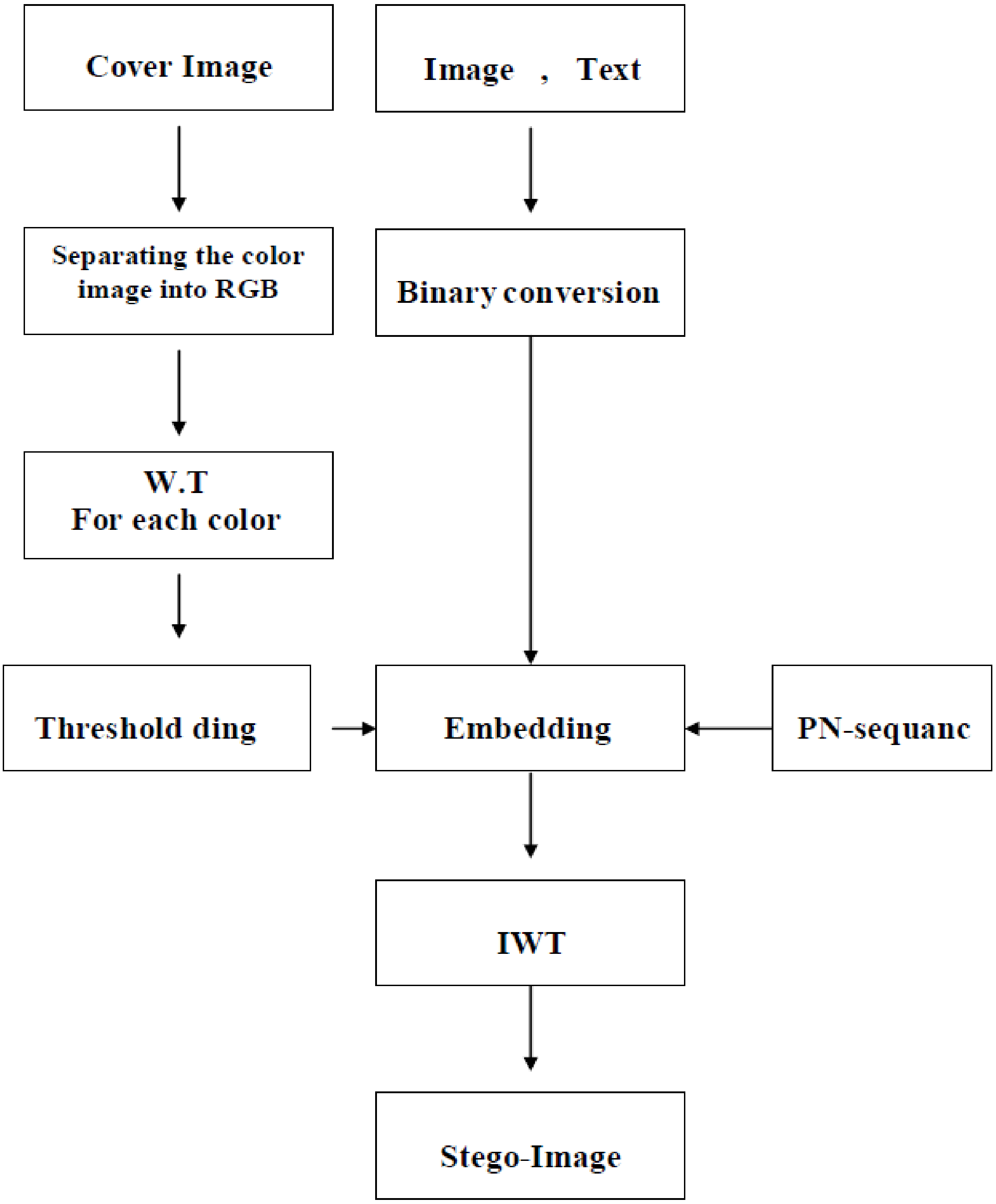

Figure (3) Embedding algorithm

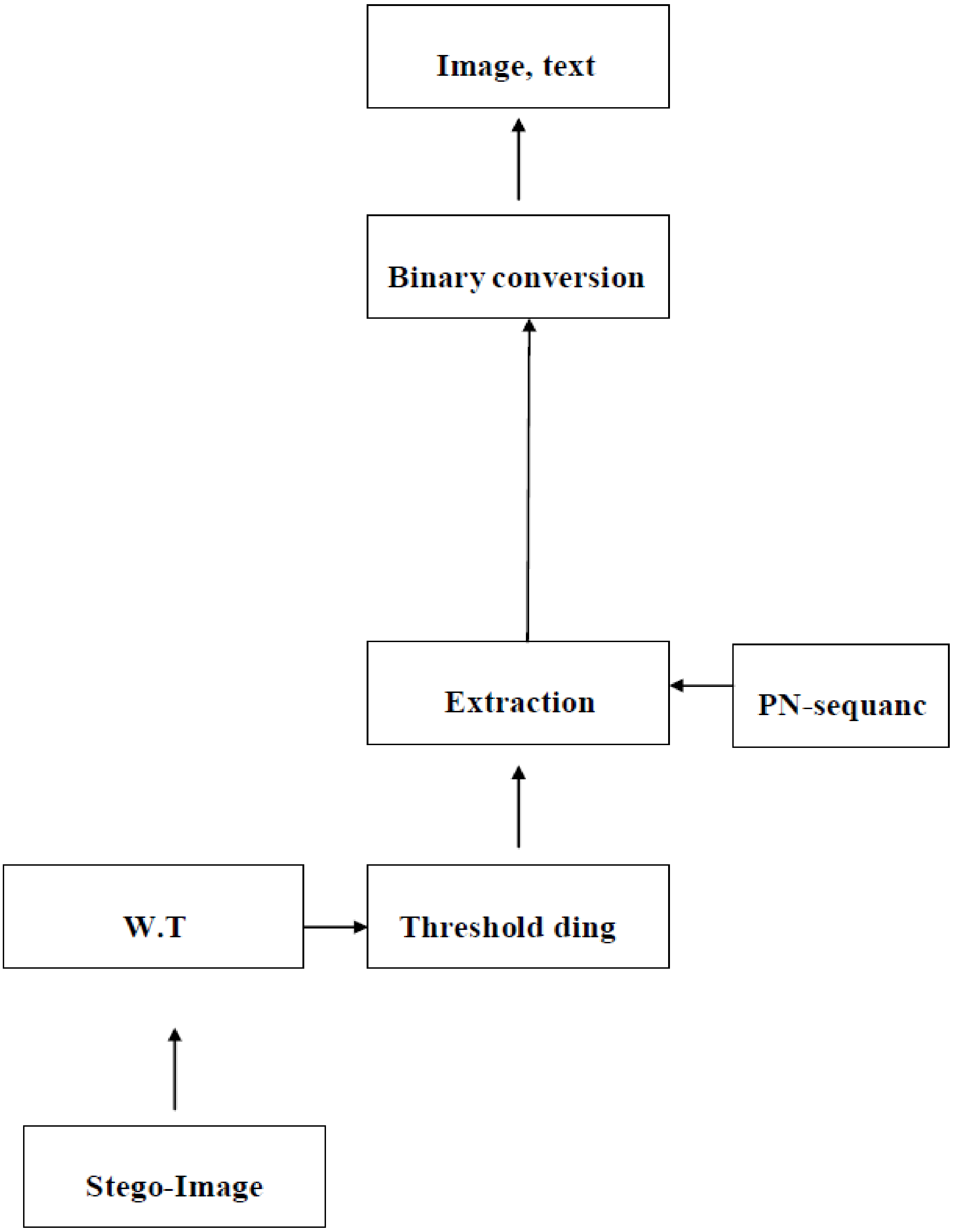

Figure (4) Extraction algorithm

5. Results:

We can classify the models in to three types:

1. The data (image, text) (64 x 64) its airplane which is the secret and the cover image (256 x256) which is the autumn called. we see that the modified image not effected by this hidden image. The histogram of the cover image not defer from the (cover + data).the histogram of the cover image is approximately the same as the histogram of the modified image. As shown in fig (5, 6). Hence the robustness is very good in this method; hence we get an increase in capacity and security.

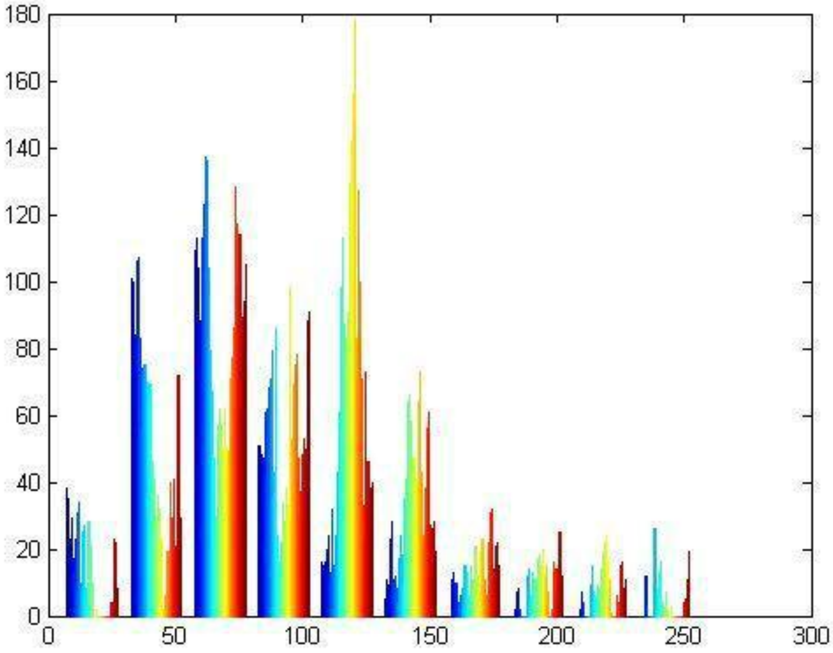

Figure (5) Histogram of cover image of model one

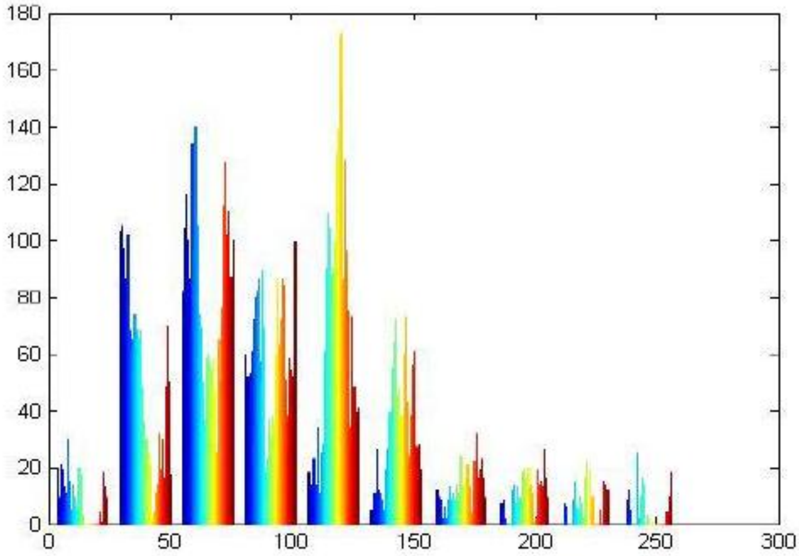

Figure (6) Histogram of stego-image of model one.

2. The data is small (64 x 64) and the cover image very big (1024 x 768). We see that the modified image not effected by this hidden image. The histogram of the cover image not defer from the (cover + data).the histogram of the cover image is approximately the same as the histogram of the modified image. As shown in fig (7, 8).

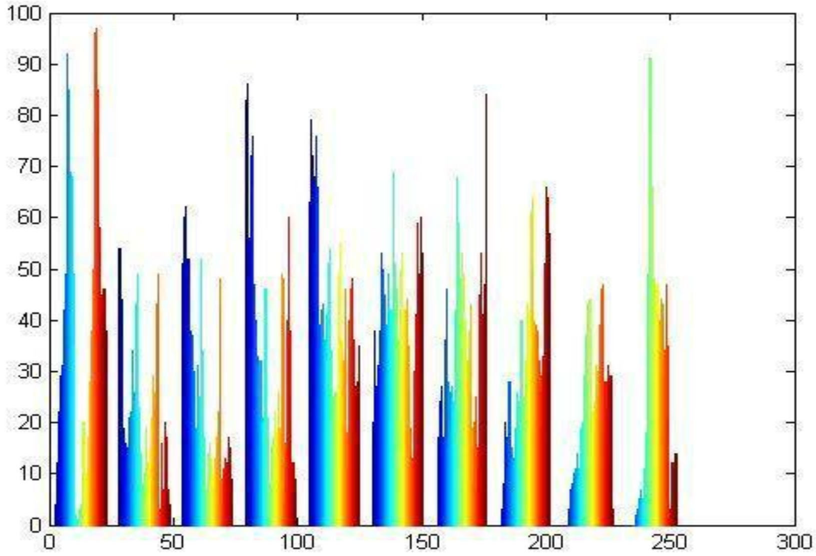

Figure (7) Histogram of the cover image of model two.

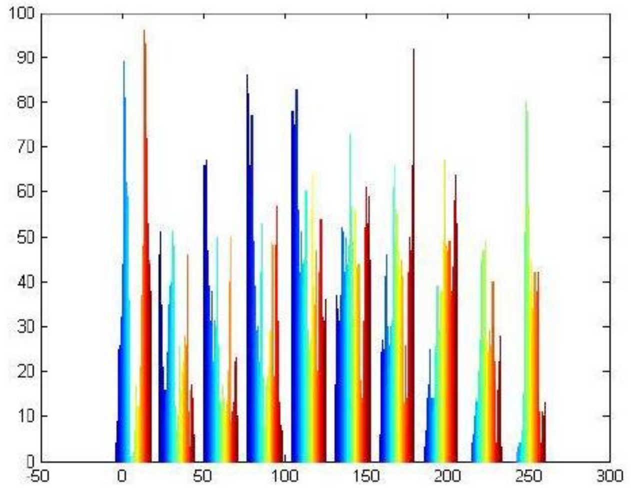

Figure (8) Histogram of stego-image of model two.

3. The data is big (256 x 256) and the cover image very big (1024x768). We see that the modified image not effected by this hidden image. The histogram of the cover image not defer from the (cover + data).the histogram of the cover image is approximately the same as the histogram of the modified image. As shown in fig (9, 10)

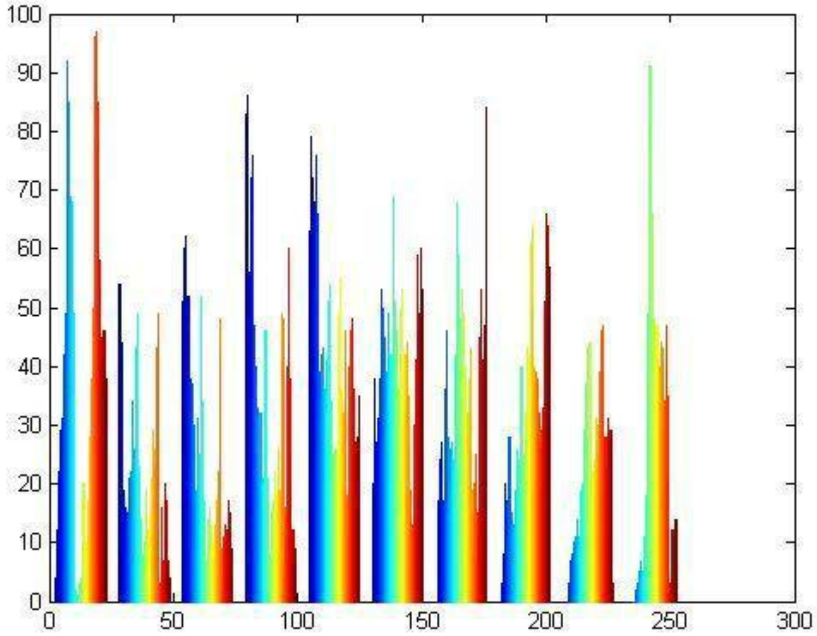

Figure (9) Histogram of cover image of model three.

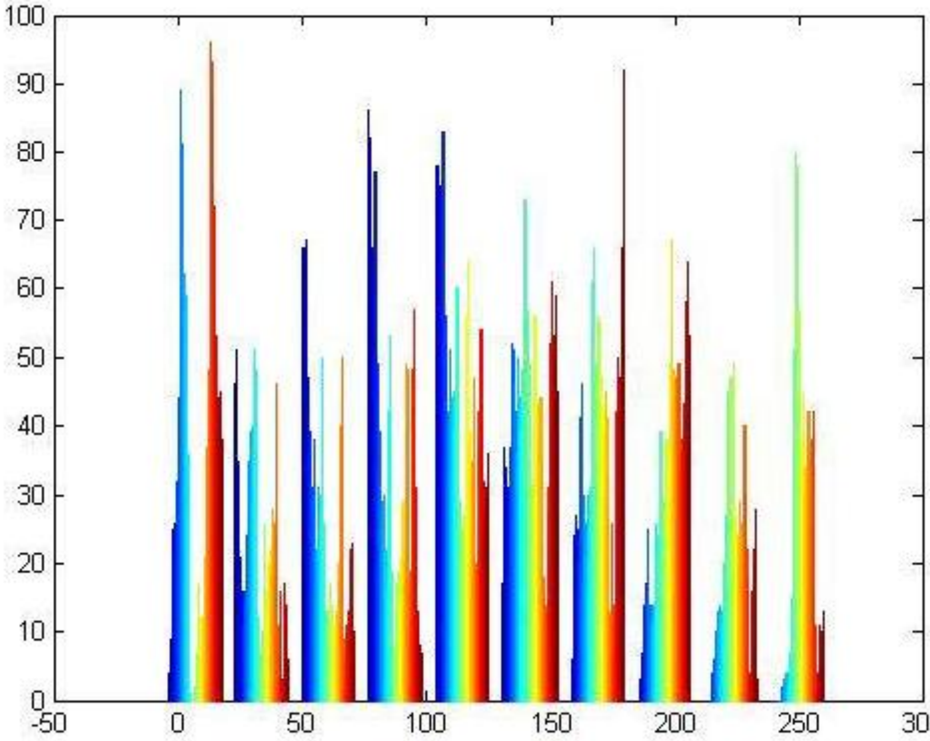

Figure (10) Histogram of stego-image of model three.

6. Conclusions

Wavelet transforms that allow perfect reconstruction of the original image. The proposed algorithm deals with color images and applies on each color plane separately. The embedding process hide up to 4 message bits in each integer coefficient for all the transform sub-bands [9].

The algorithm shows the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered [10]. The information capacity provided by the proposed algorithm can reach 50% of the original cover image size. Furthermore, experimental results showed that this schemes retains high quality of the stego-image over the existing LSB-based methods.The results shown the histograms of a stegimage and the cover images which secret information embedded in it .We see the difference between the histograms is very little . The PN sequence is used as the secret key for both embedding and extracted only who knows it receiving and transmitting.

References

[1] Birgit Pfitzmann, (*Information Hiding Terminology*) First Workshop of Information Hiding Proceedings, Cambridge, U.K. May 30 - June 1, 1996. Lecture Notes in Computer Science, Vol.1174, pp 347-350. Springer-Verlag (1996).

[2] A.R. Calderbank, Ingrid Daubechies, Wim Sweldens, Boon-lock Yeo,(*Lossless image compression using integer to integer wavelet transforms*) in the international conference on image procrssing,
Piscataway, NJ: IEEE Press, 1997, vol. I, pp 596-599.

[3] Han-Yang Lo, Sanjeev Topiwala, Joyce Wang,(*Wavelet Based Steganography and Watermarking*) Cornell University, Computer Science Department, 1998.

[4] A. R. Calderbank, Ingrid Daubechies, Wim Sweldens, Boon-Lock Yeo, *(Wavelet Transforms That Map Integers to Integers*) Applied and Computational Harmonic Analysis (ACHA), 1996.

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto, Anthony Lu,(*Techniques for Data Hiding*) IBM Systems Journal, Vol. 35, No. 3&4. Vol. 35 No. 3, 1996.

[6] Moni Naor, Omer Reingold, (*On the construction of Pseudo Random Permutation) Luby- Rancoff Revisited*, Jornal of Cryptography, vol. 12, no. 1,
1999, pp. 29-66.

[7] Richard Popa,(*An Analysis of Steganographic Techniques*,) a working report for Faculty of Automatics and Computers- Department of Computer Science and Software Engineering at
University of Timisoara, 1998.

[8] Yeuan-Kuen Lee and Ling-Hwei Chen, (*A High Capacity Image Steganographic Mode)l*, accepted by IEEE Proceedings Vision, Image and Signal Processing, 2000.

[9] Ali Bilgin, Philip J. Sementilli, Fang Sheng, Michael W. Marcellin , (*Scalable Image Coding Using Reversible Integer Wavelet Transforms*) ,1999.

[10] Neil F. Johnson, Zoran Duric and Sushel Jajodia, (Information Hiding Steganography and Watermarking) , Attacks and Countermeasers" Kluer Acadimiac Publisher 2001.

[11] M.F Tolba , M.A . Ghoncmy ,I. A. Taha and A.S. Khalifa , (Using wavelet Transform in colored image Steganography) IJICIS Vol. 4 , No. 2 July 2004.