Novel security Image Steganography Based on DWT and Pseudorandom Sequences

Asst. Prof. Dr.Refat Talib Hussein
Department of Electrical & Electronic Engineering
University of Technology.

&

M.Sc. Awatf A. Jafar
Department of Electrical Engineering
Al-Mustansiriya University.

Baghdad-Iraq, 2008.

Abstract

In this paper, a new technique that address the problem of high capacity and data security in steganography is proposed. A robustness system is achieved by choosing a transform domain technique for embedding. The proposed system is based on the idea of 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.

High security system is achieved by generation of three PN-sequences; one to encrypt the secret image and the others to choose the position of embedding. The quality of the stego-image is very close to that of the original one and the recovered image is similar to the hidden secret image (Corr.≈1).

Key words: *Steganography, Cover image, Stego-image, Pseudorandom sequences.*

الخلاصة

تم في هذا البحث اقتراح تقنية جديدة تركز على السعة العالية مع السرية في نظام إخفاء المعلومات . فللنظام المقترح تم اختيار تقنية حيز التحويل لغرض الإخفاء من اجل الحصول على نظام متين. إن النظام المقترح يستند إلى فكرة المويجة على أساس الاندماج . في هذه الطريقة تم دمج تحليل المويجة للصورة الغطاء والصورة السرية لتكوين الصورة المضمنة(stego-image) .

لقد تم الحصول على سرية عالية وذلك من توليد ثلاث متسلسلات عشوائية الأولى لغرض تشفيرا لصورة السرية و الآخران لاختيار مواقع الإخفاء . إن جودة الصورة المضمنة قريبة جدا من الصورة الأصل كما و إن الصورة المسترجعة مشابهة للصورة السرية (عامل التشابه يساوي تقريبا 1)

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 communications methods that conceal the message’s existence [1]. Although 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 [2].

A famous example of steganography is Simmons 'Prisoners' problem. Bob and Alice are in a jail and wish to escape. Their cells are far apart from each other and the only allowed communication is sending messages via prison warden. If warden detects any sign of conspiracy, they will secure their cells even more. Bob and Alice are well aware of these facts.[3]. Steganography techniques can be divided into various categories and in various ways. The basic and most common used partitioning of hiding techniques is the spatial domain, frequency domain and parametric domain steganography. Three types of steganography can be identified. Their difference is in the nature and combination of inputs and outputs[2]:

- pure steganography
- secret key steganography
- public key steganography

Steganography have to guarantee these requirements [3]:

- robustness – the embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition.
- undetectability – embedded information is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn.
- perceptual transparency – it is based on the properties of the human visual system or the human audio system. The embedded information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not.
- security – the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, and the knowledge of at least one carrier with hidden message.

Many different approaches and techniques for information hiding can be used. Havancak et.al [1] have derived a technique based on Discrete Wavelet Transform DWT with permutation of secret message. Neil et.al [2] discussed the method based on statistical analysis of pairs of values (PoVs) that are exchanged during message embedding. Haider [4] proposed a Combination between steganography and cryptography to embed four secret images into the cover image.

Silva [5] uses Discrete Cosine Transform (DCT), Fast Fourier Transform (FFT), Haar Wavelet Transform and Hadamard Transform to transform and they replace the insignificant coefficients of transformed image by the scaled payload. Tolba et.al [6] have designed a scheme that is based on the idea of merging wavelet decomposition of both the cover image and the secret message into a single fused result using an embedding strength factor. K B Raja et.al [7] developed an algorithm in which payload bit stream is encrypted and embedded into wavelet coefficients of the cover image to derive a stego-image.

2. General Model of Steganographic System

Each steganographic communication system consists of an embedding and extraction algorithm. To accommodate a secret message, the original image, also called the cover image, is slightly modified by the embedding algorithm.

As a result, the stego image is obtained [5]. The following terms are used along the embedding and extraction process:

Cover-object, c: the original object where the image has to be embedded. Message, m: the image that has to be embedded in the cover-object. Stego-object, s: the cover object, once the image has been embedded. Stego-key, k: the secret key shared between A and B to embed and retrieve the image. Figure (1) presents the model of steganography system [6].

At the sender terminal, the message is embedded in a digital image by the stegosystem encoder which usually uses a key. The embedding function E is a function that maps the tripled Cover-object c, message m and stego-key k to a stego-object

$$E(c, m, k) = s \quad (1)$$

At the reception terminal, the retrieving function D is a mapping from(s) to (m) using the stego-key (k).

$$D(s, k) = m \quad (2)$$

In some stego systems the original cover-object (c) may be needed as, input to the retrieving function D [**7**].

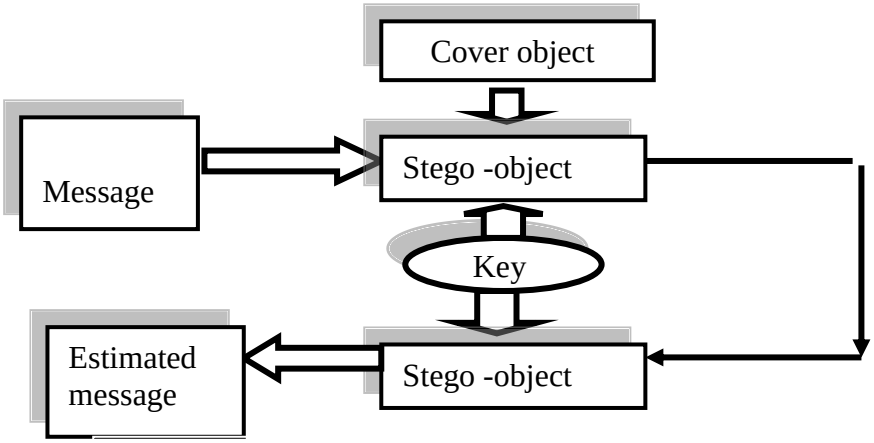


Figure (1) The steganography model.

2-1 Wavelet Transform

One of the well known wavelet basis functions that can be used in steganography is Haar Wavelet Transform. It is also the only quadrature mirror filter that have a finite impulse response. The low frequency wavelet coefficients (approximation band coefficients A_i) are generated by averaging the two pixel values as given in equation (3) and the high frequency coefficients (detail band coefficients D_i) are generated by taking half of the difference of the same two pixels as given in equation (4).

$$A_i = \frac{P_{2i-1} + P_{2i}}{2} \tag{3}$$

$$D_i = \frac{p_{2i-1} - p_{2i}}{2} \tag{4}$$

Where p_i is the i-th pixel value in the input spatial domain signal [5].

2-2 Image Fusion

The fusion of images is the process of combining two or more images into a single image retaining important features from each. 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 ω of the two registered input images $I_1(x,y)$ and $I_2(x.y)$ together with the fusion rule(ϕ).

Then, the inverse wavelet transform ω^{-1} is computed, and the fused $I\ (x,y)$ is reconstructed [**8**].

$$I\ (x,y) = \omega^{-1}(\phi(\omega\ (I_1(x,y)), \omega\ (I_1(x,y)))) \quad (5)$$

This process is depicted in Figure (2)

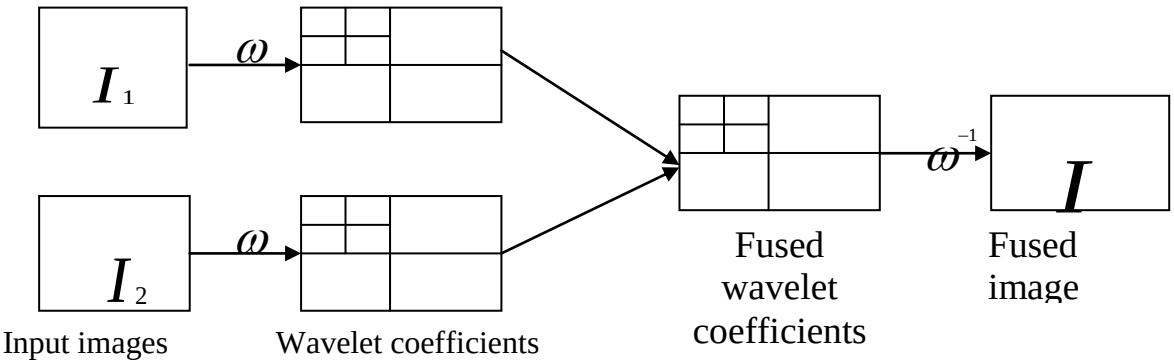


Figure (2) Fusion of the wavelet transforms of two images.

3. Proposed Steganographic Model

The main idea of the proposed system is called the wavelet based fusion. Data fusion refers to the processing and synergistic combination of information from various knowledge sources.

3-1 Embedding Model

Since, the cover image and the secret image are both in true color format, the 2D DWT is applied separately for both but for each color plane. Two level DWT is applied for the cover image then each coefficient will be converted to 24 bits.

The secret image is encrypted by using the PN-sequence PN3 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 original and final encrypted image are shown in Figure (3).

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

(a)Original image

9	15	1	11
12	6	8	4
3	5	16	10
7	14	2	13

(b)Encrypted image

Figure (3) Schematic of secret image Encryption.

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 of the cover image. This process is explained in Figure (4).

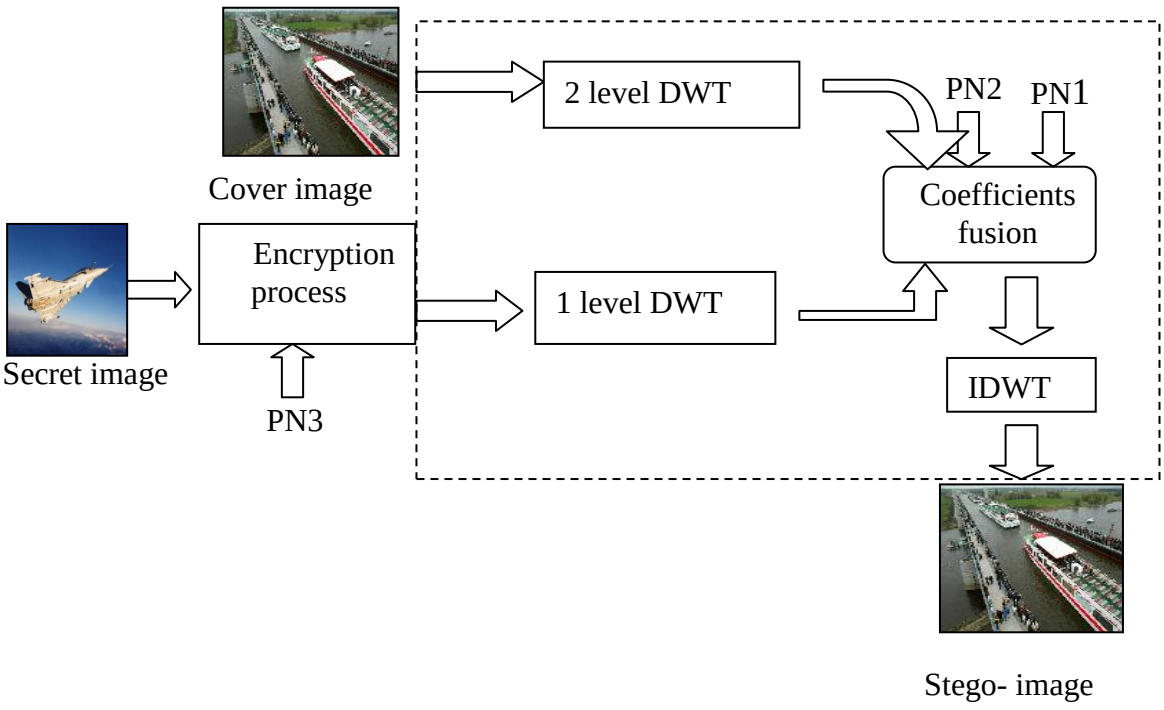


Figure (4) Embedding a true color secret image into a true color cover image.

After all coefficients of the secret image are successfully embedded in the coefficients of the cover image, new vectors of coefficients will be obtained. For wavelet coefficients, taking inverse wavelet transform, using the same filters according to the filter bank theory and number of 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 image.

3-2 Extraction Model.

The recipient will certainly get the stego-image. But the extraction of the secret information out of the cover could not be done without knowledge of which keys (PN1, PN2 and PN3) have been used in the embedding process.

The extracting process can be done by handling the stego-image by 2-level wavelet decomposition using the same filters used in the sender stage, and the resulted coefficients are rearranged in a manner similar to that in the sender.

The same (PN1) and (PN2) sender keys are used to select the coefficients where the data has been embedded and to extract the coefficients of the final secret image. By taking the inverse of the ways used in embedding process and decryption of the result scrambled image, the secret image is perfectly reconstructed. Figure (5) explain this process.

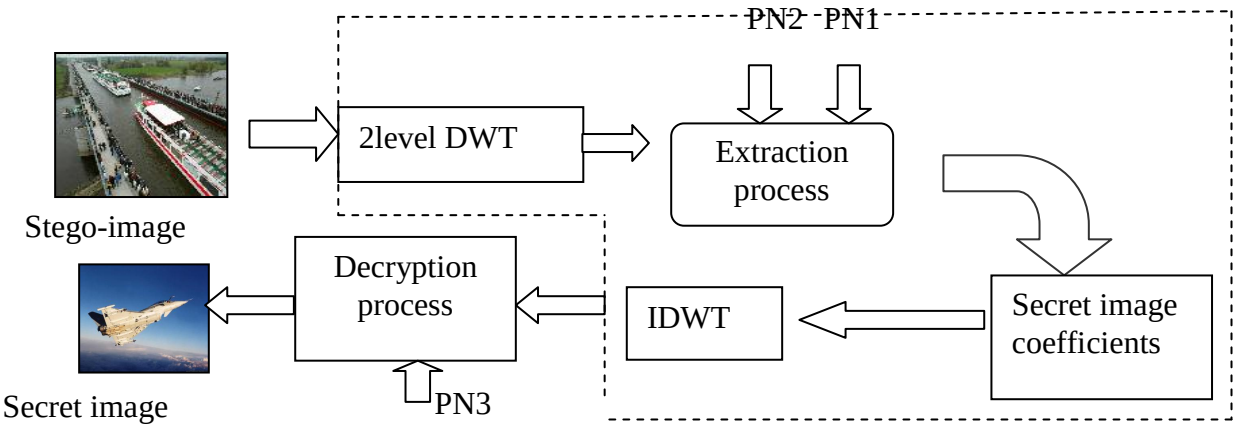


Figure (5) Extraction of secret image from a true color stego-image.

4. Experimental Results and Evaluation

4-1 Experimental result

4-1-1 Case Study (1): Secret Image (128 x 128)

The secret image is a true color image of size (128x128) and the cover image is a true color image of size (256x256). From this result, perfect reconstruction for the secret image can be seen as shown in Figure (6). For stego-image,the PSNR=63.1201dB; Correlation=0.9999940.

The Peak Signal to Noise Ratio (PSNR) present the distortion measured in Decibels (db) caused by the hidden image in the cover image. It is derived from the Mean Square Error (MSE). The later term refers to a metric used to quantify the distortion in images generated by the digital steganography after the embedding process [5]. The equations are follows:

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(I - I^{*})^{2}}{NxM} \quad \textbf{(6)}$$

where, I and I* are the cover image and the stego image respectively, N and M are the numbers of rows and columns of the image.

$$SNR = 10\log_{10}(X_{\max}^{2} / MSE) \quad (7)$$

$$PSNR = 10\log_{10}(255^{2} / MSE) \quad (8)$$

Where, Xmax is the maximum of luminescence in the image.

On the other hand, Correlation is the similarity between the cover-image and stego-image. When the stego-image is perceptually similar to the original cover-image, then the correlation equals one. The correlation can be calculated using [5]:

$$Cor = \frac{\sum_{r=1}^{M}\sum_{c=1}^{N}(I(r,c)-\bar{I})(I^{*}(r,c)-\bar{I^{*}})}{\sqrt{\left[\sum_{r=1}^{M}\sum_{c=1}^{N}(I(r,c)-\bar{I})^{2}\right]\left[\sum_{r=1}^{M}\sum_{c=1}^{N}(I^{*}(r,c)-\bar{I^{*}})^{2}\right]}} \quad (9)$$

where:

r: row number

c: column number

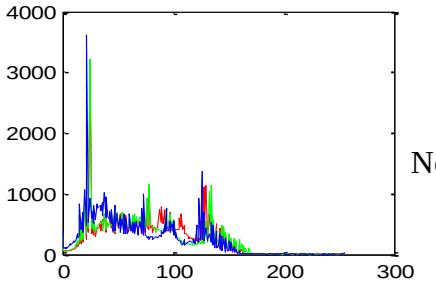
M: height of cover image (or stego-image)

N: width of cover image (or stego- image)

$\bar{I}$: mean of cover image

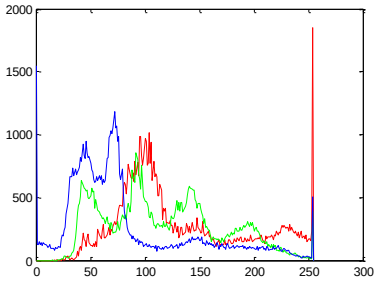
$\bar{I}^{*}$: mean of stego-image

Secret image



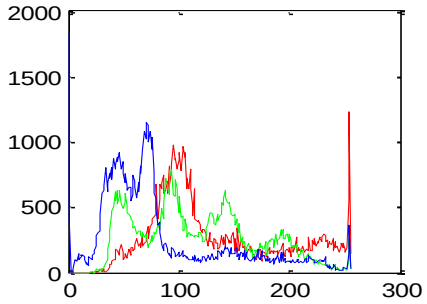
Histogram of the secret image

Cover image



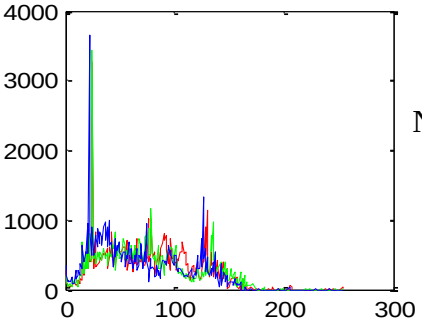
Histogram of the cover image

Stego- image



Histogram of the stego-image

Recovered secret image



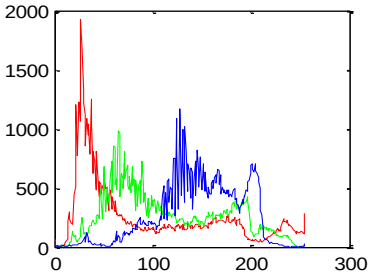
Histogram of the recovered secret image

Figure (6) stego-image and recovered secret image with related histogram for case study (1).

4-1-2 Case Study (2): Secret Image (128 x256)

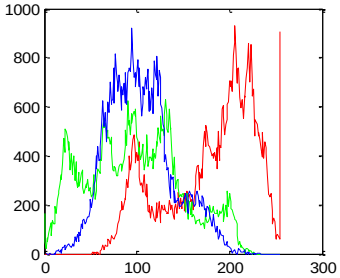
In this case secret image is a true color image of size (128x256) and the cover image is a true color image of size (256x256). From this result, perfect similarity between the secret image and recovered image can be seen as shown in Figure (7). For stego-image the PSNR= 62.3557 dB ; Correlation= 0.99999332 .

Secret image



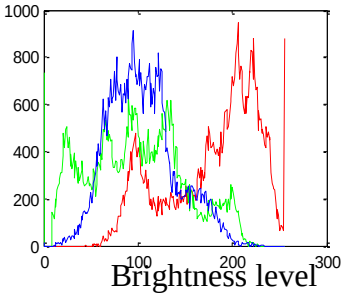
Histogram of the secret image

Cover image



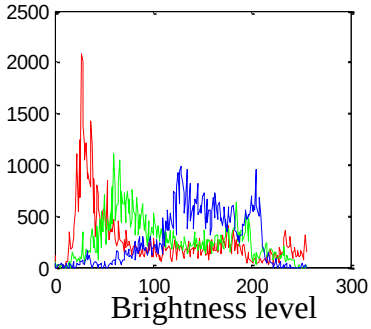
Histogram of the cover image

Stego-image



Histogram of the stego- image

Recovered secret image



Histogram of the recovered image

Figure (7) stego-image and recovered secret image with related histogram for case study (2).

4-2 System Evaluation

Two sets of evaluation results are presented; the first one is the PSNR and Correlation and the second is histogram evaluation:

4-2-1 PSNR and Correlation

To evaluate the performance of the proposed algorithm, several simulations have been performed in order to compare its performance with other existing schemes. Two types of least significant bit (LSB) insertion methods were used, fixed size (4LSB) and variable size (Adaptive LSB). The former embeds the same number of bits in each pixel of the cover image. On the other hand, the number of embedded LSB's in variable –sized embedding model depends on the local characteristic of the pixels to provide a higher capacity while keeping a better invisibility. The cover image is the bridge image of size (256x256) while the secret image is the air craft image of two sizes as shown below. Figure (8) shows the cover and the secret images that are used in the evaluations.

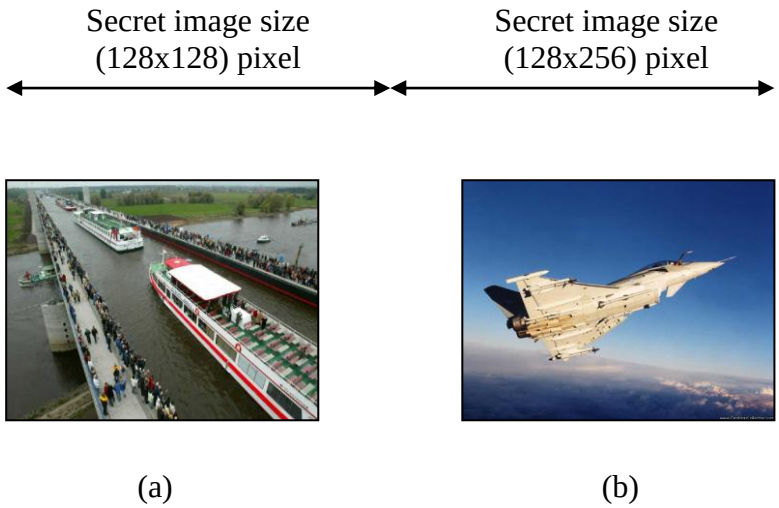


Figure (8) a-the cover image –b- the secret image.

Table 1 shows the measured PSNR and the correlation for each method. Two sizes of secret image are taken (128x128) pixel and (128x256) pixel, while the size of the cover image is (256x256) pixel.

According to the results listed in Table 1, the adaptive LSB method provides an embedding capacity a little bit more than 4 bits per pixel. While the proposed method can embed up to 8 bit per pixel. Furthermore, the proposed method provides the best performance.

Table 1: Correlation ,PSNR (dB) and capacity values for stego image

Method	Capacity	PSNR/dB	Correlation	PSNR/dB	Correlation
4LSB	4BpP	33.7888	0.9938580	30.4363	0.9913310
AdaptiveLSB	4.03BpP	39.2264	0.9998533	34. 6271	0.9991935
Proposed method	8BpP	63.1201	0.9999940	62.0125	0.9999933

4-2-2 Histogram Test

The existence of a hidden or embedded image can be provided by subtracting the histogram of the stego-image from the histogram of the cover image and notice the result that shows if there is a hidden image or not [9]. Figure (9) shows the subtraction of histogram for three methods: LSB, adaptive and the proposed methods.

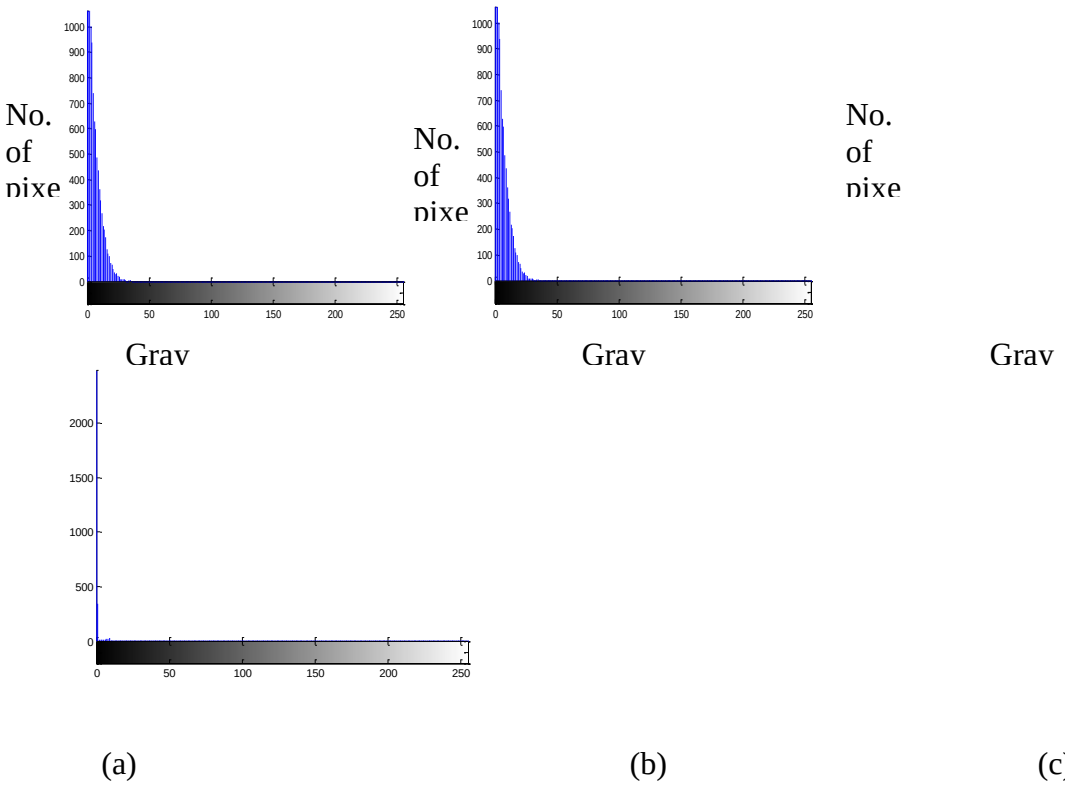


Figure (9). Histogram of subtracting the stego-image histogram from cover image histogram, (a) LSB method,(b) adaptive LSB and (c) the proposed method.

According to the histogram subtraction, the proposed method gives high invisibility compared with the other methods.

5. Conclusions

Experimental result showed that applying the idea of the suggested system provides a better performance than normal and adaptive LSB methods. A summery of some important conclusions could be the following:

- The use of all coefficients in approximate band and detailed band of the cover image in our approach results in embedding a very high capacity of secret image (a true color image that is 1/2 or 1/4 in size can be embedded in the original colored image in terms of pixel).
- The using of Haar Wavelet Transform provides good extracted secret image.
- High security proposed system is done by using PN –sequences.

6. References

[1] R. Havancak, P. Foris and D. Levicky, ''Steganography Based on DWT Transform'', Department of Electronics and Multimedia Telecommunications,Technical university of Kosice,Park Komenskeho(2004).

[2] J. Neil, D. Zoron and F. Jajodia, " Information Hiding: Steganography and Watermarking Attacks and Countermeasures", Kluwer Academic Publishers, 2001.

[3] J. Eggers, R. Bauml and B. Girod, ''A Communications Approach to Image Steganography'', Proceedings of SPIE Vol. 4675, Security and Watermarking of Multimedia Contents , 2002.

[4] H. T. AL-Haajy, ''Still Image Steganography using Wavelet Transform'', M.Sc. Thesis, College of Engineering , University of Baghdad, Iraq, 2003.

[5] E. Silva and S Agaian,'' The Best Transform in the Replacement Coefficients and the Size of the Payload Relationship Sense", IS&T'S Archiving conference, San Antonio, Texas, pp:199-203, 2004.

[6] M.F. Tolba, M. Ghonemy, I. Abdoul-Hameed and A. S. Khalifa,''High Capacity Image Steganography using Wavelet –Based Fusion'', Procedding, iscc, Ninth International Symosium, vol.:1,28 June-1,pp:430-435,July (2004).

[7] K B Raja, Venugopal K R and L M Patnaik, ''High Capacity Lossless Secure Image Steganography using Wavelet'', Proce. IEEE 2006.

[8] P. Hill, N. Canagarajah and D. Bull, '' Image Fusion using Complex Wavelets'', Dept. of Electrical and Electronic Engineering . University of Bristol , Bristol, UK-2002.

[9] A. A. Jafar, '' Image Steganographic Algorithm based on DWT and Turbo Coding '', M.Sc. Thesis, College of Engineering, Al-Mustansiriya University, 2008.