Wavelet -Based Modified Intermediate Significant Bit Insertion for Text Steganography

Qaswaa K. Abood
Baghdad University / Collage of science
Department of computer science

ABSTRACT

In this paper, we propose and investigate the use of a *modified* version of Intermediate Significant Bit (ISB) insertion algorithm, so-called here as MISB algorithm for secret text steganography. The secret text is passed through a sequence of ciphering techniques. A *Modified Intermediate Significant Bit* MISB insertion algorithm is proposed for hiding the bit sequences of the cipher text into the time-frequency domain using wavelet transform of the image pixels, in order to improve the robustness of the Steganography system. Results demonstrate the effectiveness of *wavelet Modified Intermediate Significant Bit* WMISB while evaluating its performance using Peak Signal to Noise Ratio PSNR measure. Moreover, additional experiments are evaluated for noising, and image compression for cover images to compare their Peak Signal to Noise Ratio PSNR. The drawn results confirm the effectiveness of the proposed *Wavelet-based Modified Intermediate Significant Bit Insertion* WMISB, Also, Bit Error Rate BER, is a key parameter that is used in assessing systems that transmit digital data from one location to another.

KEY WORDES: RSA, wavelet transforms, ISB, MISB.

I. Introduction:

Generally, steganography is defined as the art and science of communicating in covert fashion, allows for authentication, copyright protection and embedding of messages in the image or in the transmission of the image [1]. Steganography scheme consists of: stegano embedding and stegano extracting steps. Embedding steganography into the image is performed usually by modifying the image characteristics, such as luminance values or transform domain coefficients. Selection of the coefficients depends on perceptual criteria as well as on a key instrumented permutation to increase the security and robustness of the system. Embedding can be done in an image dependent / independent additive

manner or by some substitution mechanisms. It is often necessary to utilize Human Visual System (HVS) models for adaptively embedding the Stegano. These can reduce the impacts of the modifications on image quality or for the same visual quality a much stronger Stegano can be embedded [2].

Steganography has become a significant topic of computer science due to the increasing popularity of the internet and the essential need of data security This paper propose a new bit insertion algorithm, modified from wavelet-based modified Intermediate Bit Insertion algorithm (WMISB) , to be utilized for hiding bits of the ciphered secret message into the intermediate bit planes of the cover image in wavelet domain[2].

The paper is organized as follows. Section II describes briefly wavelet transform of image. Section III presents the modified ISB used. Section IV outlines the steps of the embedding and extracting process. Finally simulation results are illustrated in section V followed by the drawn conclusion in section VI.

II. Wavelet transforms

Wavelets are functions defined over a finite internal and having an average value of zero. The basic value of the wavelet transform is to represent an arbitrary function $x(t)$ as a super position of a set of such wavelets or basis functions. These basis functions obtained from a single prototype wavelet called the mother wavelet, by dilation or contractions (scaling) and transitions (shift).

The wavelet transform is given by: [4]

$$X_W(a, b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} h^* \left(\frac{t - b}{a} \right) x(t)\, dt. \quad \text{--------(1)}$$

Where a and b are wavelet function parameters and x(t) is the signal to be transformed. The

prototype wavelet function is given by:[4]

$$h_{a,b}(t) = \frac{1}{\sqrt{a}} h \left(\frac{t - b}{a} \right) \quad \text{----------(2)}$$

The discrete wavelet transform of a finite length signal $X(n)$ having N component, expressed by NxN matrix, the last array called the wavelet transform of the original array [4]. The simplest wavelet imaginable and certainly the earliest is the (Harr) system. The main property of this system is the support length of wavelet function (ψ) and the scaling function (φ) is $2N-1$. The number of vanishing moment of ψ is N.

- The asymmetry is very pronounced.

- The regularity increases with the order. when N becomes very large,
- The analysis is orthogonal.[4][5]

III. Modified Intermediate Significant Bit Insertion Algorithm.

A digital image is a set of bits having the same position in the respective binary numbers. In gray scale image representation, there are 8 bit-planes: the first bit-plane contains the set of the most significant bits (MSB) and the 8th bit-plane contains the least significant bits (*LSB)*. The set in between i.e. from 2nd to 7th bit-planes are intermediate significant bits ISB as shown in figure 1.

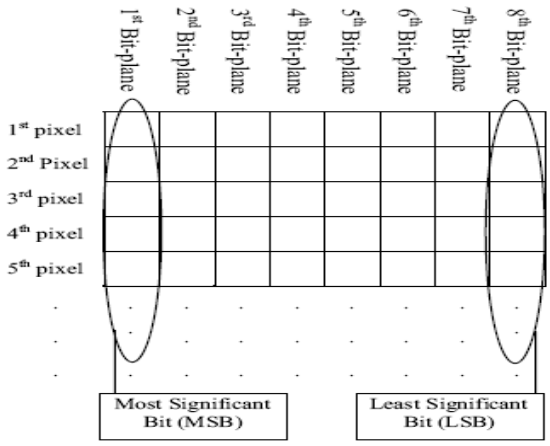


Figure (1) A bit-plane of digital images

Least Significant Bit (LSB) technique is the earliest developed technique in steganography and watermarking and it is also the most simple, direct and common technique. It essentially involves embedding the watermark by replacing the least significant bit of the image data with a bit of the secret data. Thus, we can state 2LSB insertion algorithm as replacing the two least significant bits with another two destination bits. Note that in case of embedding information into bit planes of an image, a source pixel value will not be changed when the required embedded bit equals the selected pixel's bit (i.e. embedded bit is 1 and the selected bit of the original pixel value was 1 too, or embedding 0 and the original pixel bit value was 0 too). The disadvantage of LSB is that it is not robust against attacks.

ISB method uses one bit-plane to embed the watermark object into a selected bit-plane.

The next step after selecting one bit-plane for embedding is finding ranges (the value of each bit of the 8 bit-plane can be represented as 2^{n-1} , where n

is order of the plane starting from 1 to 8. The maximum value that can fit in 8 bits is 255 and the minimum value is 0) .Any modification to the 8^{th} bit-plane will change the pixel value by ±1. The length of the range L is 2^{n-1} (L is the maximum value of each range – the minimum value of the range + 1) and the number of ranges in each bit-plane is 256 / L.

We can notice that in each range the bit either from 0 to 1 or 1 to 0 The number of ranges for the first bit-plane are 2 only, as follows [0:127] and [128:255]. In other words, the bit in the first range is 0, while the bit in the second range is 1 and the length of each range of the first bit-plane is 128. For the second bit-plane there are 4 ranges as follows: [0:63] [64:127] [128:191] [192:255] and the length of the ranges is 64, and so on.

During the embedding there is no changing to the pixel if the same bit will be embedded. In other words, the same range will be selected to locate the watermarked pixel (i.e. embedded bit is 1 and the selected bit of the original pixel value was 1 too, or embedding 0 if the original pixel value was 0). But if the selected bit of the original binary pixel is not the same as the embedded one, the previous or next range will be selected. The new range will be determined depending on its distance to the original pixel value.

The proposed *Wavelet-based Modified Intermediate Significant Bit* (W*MISB*) algorithm can be realized in four steps:

1. The original text is passed through sequence of ciphering techniques starting from Rail Fance, Ceaser ending by RSA algorithm [3], where the output of one cipher method will be as input for the next cipher method.
2. Embedding process will be held as one secret bit per image pixel in both wavelet LH & HL parts, as shown in figure (2).
3. If the required embedded bit and the pixel value in the 2^{nd} bit-plane are equal, then no embedding operation will be performed. Otherwise embedding will be performed. After reading each bit in ciphered character as binary bits in sequence and altering the corresponding pixel's bit values in the destination planes (i.e. this is equivalent to XOR operator).
4. Modify 2^{nd} …, $(i\text{-}2)^{th}$ ISBs of the resulted pixel in the wavelet image to maximize the robustness. After embedding through step 3 the ^{2nd} bit equal one, then reset it to zero and set all remaining intermediate bits to one (i.e., 3^{rd} …$(i\text{-}2)^{th}$), e.g. if the value of the resulted wavelet pixel was (11100001) then the modified operation will make it (10111111). In order to show the improvement, take as an example

where the insertion have been made on the 2nd bit plan with 650 character. In this case, we can clearly see the appearance of noise at the boundary of the image. However, continuing bit insertion operation until 4th bit plane vanishes this drawback.

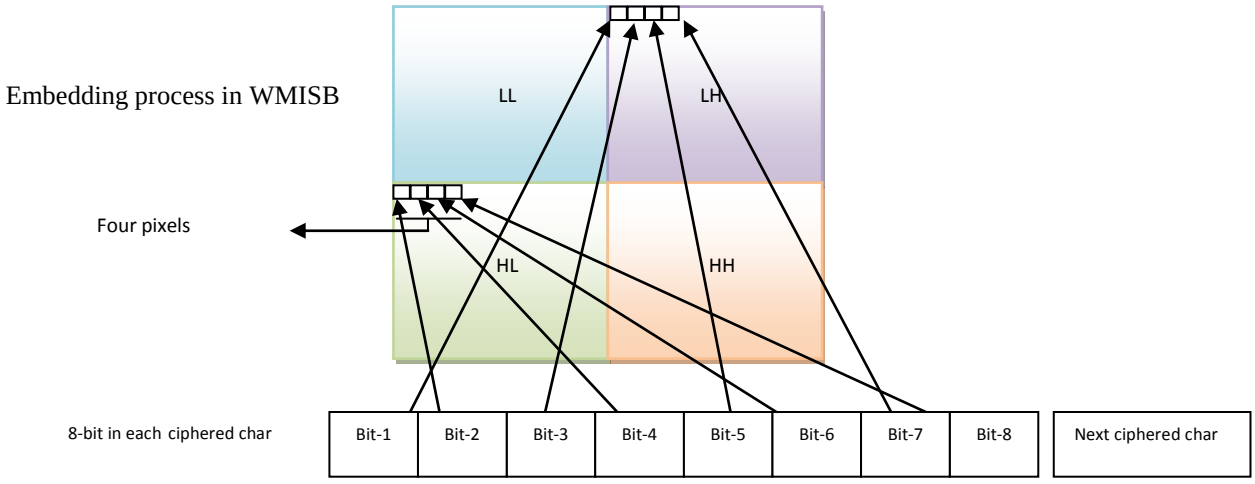


Figure (2) Embedding technique using WMISB algorithm.

We can propose mathematical representation for WMISB proposed method:-

$C = ciphertext = K(M), K =$ Multi ciphering key generation

$D = DWT[w'(i,j)]$,DWT discrete wavelet transform functions , $w'(i,j)$ embedded image (covered image)

$WMISB = [\ C_B(c) XORD_{LH,HL}(k) ORSHR(3E_H)\ ]$ $\forall_c, 1 \le c \le 8*n$ And $k \in \{2 \cdots 7\}$

C_B =cipher in binary k = bit plan place in each pixel. n=No. of character.

IV. Embedding Process.

In this paper, stegano embedding in six bit-planes will be done (for every embedding the robustness and the quality of stegano image will be measured).To improve the security of the text, the stegano object is encrypted using multiple ciphering technique additionally, the steganography data is scrambled in order to ensure additional security. One of the best methods has been used here to encrypt the embedding position and determine the pixel bit, for embedding in the host image is called the Random Pixel Manipulation Technique [6].

a) Stegano embedding algorithm

Input: input plaintext, input cover (gray Baboon image)
Output: cipher text, and wavelet image.
Step 1: convert plaintext to cipher text using multiple ciphering techniques.
Step 2: perform the wavelet transform to the input image to split the image to the following sub bands (LL, LH, HL, and HH)
Step 3: specify 2- area from the above sub bands (choose the area in the middle frequencies band) for hiding binary data using modified intermediate significant bit algorithm (MISB)
Step 4: perform the wavelet reconstruction (inverse wavelet transform) as in figure (3-a)

***b) Stegano recovery algorithm*:** This algorithm is used to extract cipher text from reconstructed image then decrypts the output cipher text to find plaintext as follows:
Input: reconstructed image.
Output: plain text and covered image.
Step 1: perform wavelet transform to the stegano image (covered image).
Step 2: Extract embedded bits from the sub bands embedded part using the same technique used in the embedding operation.
Step 3: perform inverse ciphering methods used to the binary bit then converted it to character form. as in figure (3-b)

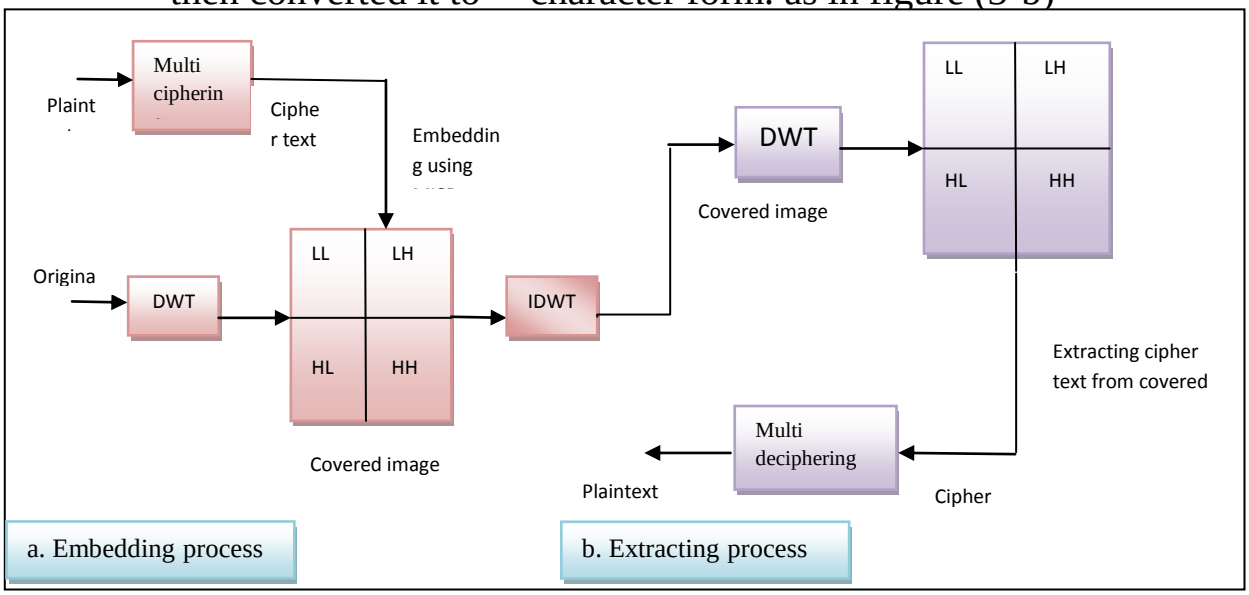


Figure (3) Illustrate embedding & extracting process.

V. Simulation Results

To evaluate the performance of the proposed system, some experiments were performed on a gray cover image of size 256x256. The length of the

stego cipher text was chosen in the range from 128 to 650 characters. To verify the robustness of the proposed method, the peak signal to noise ratio PSNR will be used. In general, a processed image is acceptable to the human eyes if its PSNR is greater than 30 db. The larger the PSNR, the better is the image quality. The PSNR is defined as given by (3) [8][9].

$$PSNR = 10\log_{10} \frac{(255)^2}{\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(w(i,j)-w'(i,j))^2} db \text{ ----------(3)}$$

Where $w(i,j)$ is the original image in which the coordinates are (i, j) and $w'(i,j)$ is the covered images in which coordinates are (i, j). (m, n) is the size (in pixel) of the cover image and stegano image, respectively.

The peak signal to noise ratio $PSNR$ and the mean square error (MSE) are inversely proportion. Thus, when the MSE value of the image increases the $PSNR$ value decreases and this will mean that the quality of the image is not good, but when the MSE value of the image decreases the $PSNR$ value will increase and in this case the quality of the image will be best. In our experiments, we used $PSNR$ rather than MSE.

$PSNR$ =10 $\log_{10}$[power/MSE at which power =$1/mn\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}w^2(i,j)$ and

MSE=1/mn$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[w(i,j)-w'(i,j)]^2$ ----------(4)

A bit error rate is defined as the rate at which errors occur in a transmission system. This can be directly translated into the number of errors that occur in a string of a stated number of bits. The definition of bit error rate can be translated into a simple formula:

BER = number of errors / total number of bits sent

If the medium between the transmitter and receiver is good and the signal to noise ratio is high, then the bit error rate will be very small - possibly insignificant and having no noticeable effect on the overall system However if noise can be detected, then there is chance that the bit error rate will need to be considered.

Figures (4) and table 1 present the evaluated results for text steganography using WMISB algorithms.

(2ND bit plan)	24.0002	23.9231	17.4807db
(3rd bit plan)	29.7935db	28.6437db	27.5447db
(4th bit plan	30.3954db	30.0872db	29.7640db
(5th bit plan	30.5129db	30.4173db	30.3335db
(6th bit plan	30.5383db	30.4900db	30.4610db
(7th bit plan	30.5443db	30.5113db	30.4977db

Table (1) PSNR computation using WMISB.

The second part of this section will support our claim for the effectiveness of WMISB. This is done by adding additional noise with factor =0.05, or by image compression with compress ratio between 0 and 1 using Db4 filters and entropy encoding. For both groups of images, we also evaluated their PSNR. Table (2, 3) present PSNR the results.

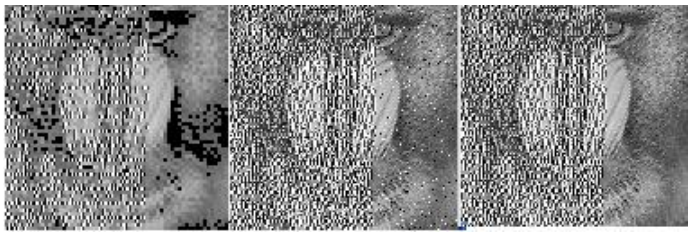
(2ND bit plan)	26.5298	26.4960	26.2946
(3rd bit plan)	26.9655	26.9129	26.8254
(4th bit plan)	26.9404	26.7723	26.5296
(5th bit plan)	26.9682	26.9290	26.7161
(6th bit plan)	27.2066	27.1384	26.9903
(7th bit plan)	27.2189	27.1270	27.1141

Table (2) PSNR computation with image noise in db

(2ND bit plan	22.6009	20.0957	18.4455
(3rd bit plan	27.0298	26.8892	26.7865
(4th bit plan	27.1213	27.0798	27.0558
(5th bit plan	27.1321	27.1138	27.1134
(6th bit plan	27.1358	27.1285	27.1137
(7th bit plan	27.1386	27.1295	27.1261

Table (3) PSNR computation after image compression in db

Original image



After compression With noise Embedding using WMISB in 2nd

After compression With noise Embedding using WMISB in 3rd

After compression With noise Embedding using WMISB in 4th

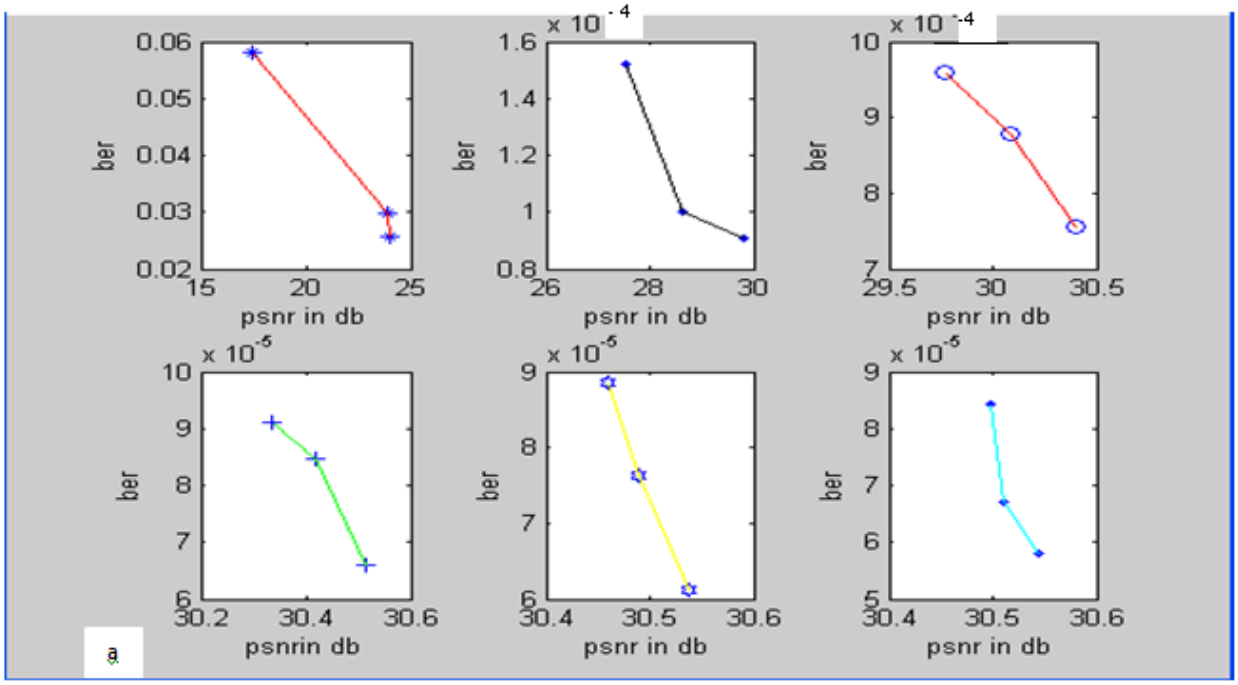
After compression With noise Embedding using WMISB in 5th

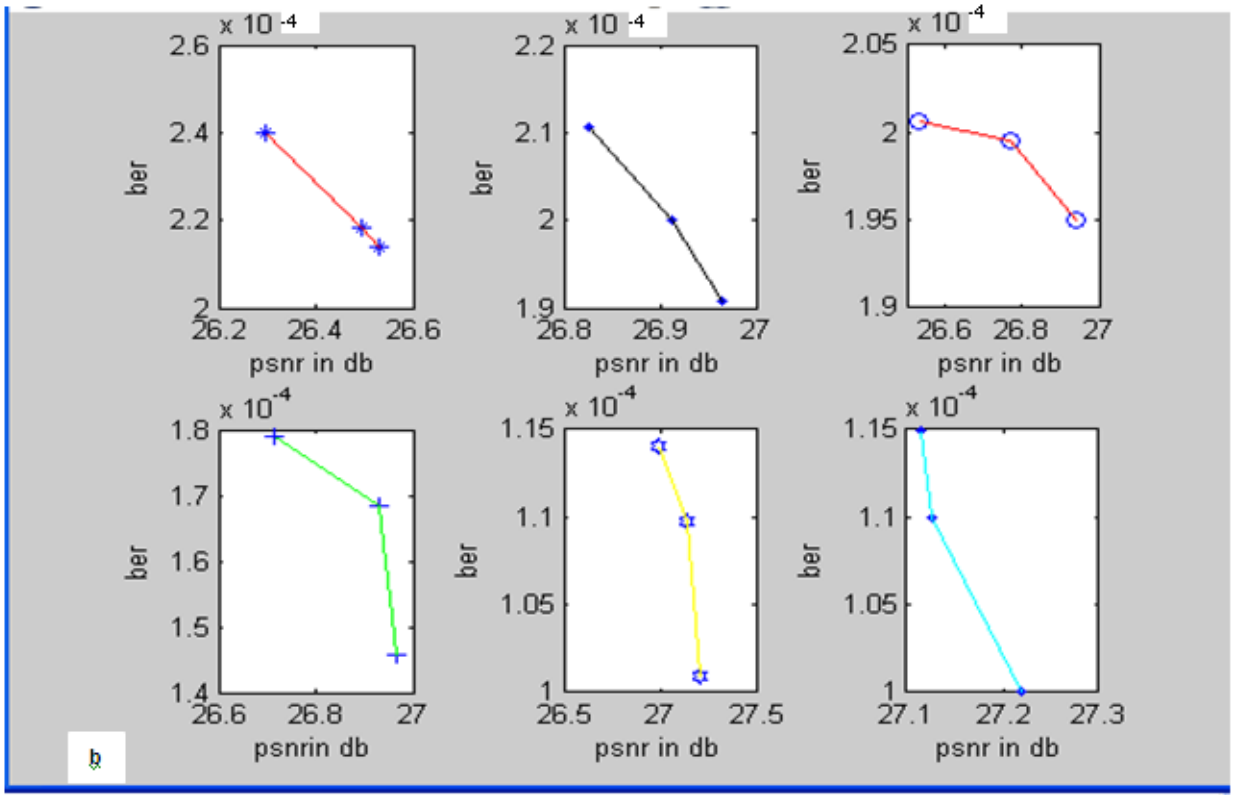
After compression With noise Embedding using WMISB in 6th

After compression With noise Embedding using WMISB in 7th

Figures (4) show 650 character using WMISB with noise and compression test

After text extracting from the noised and compressed one, bit error rate used to compute missing bit the bit error rate (BER) functions compares unsigned binary representations of elements in embedding text with those in extracting text. These will be arranged as in the shown figures which show the relation between bit error rate and an image quality according to PSNR ratio in db. figure(5-a,b,c)





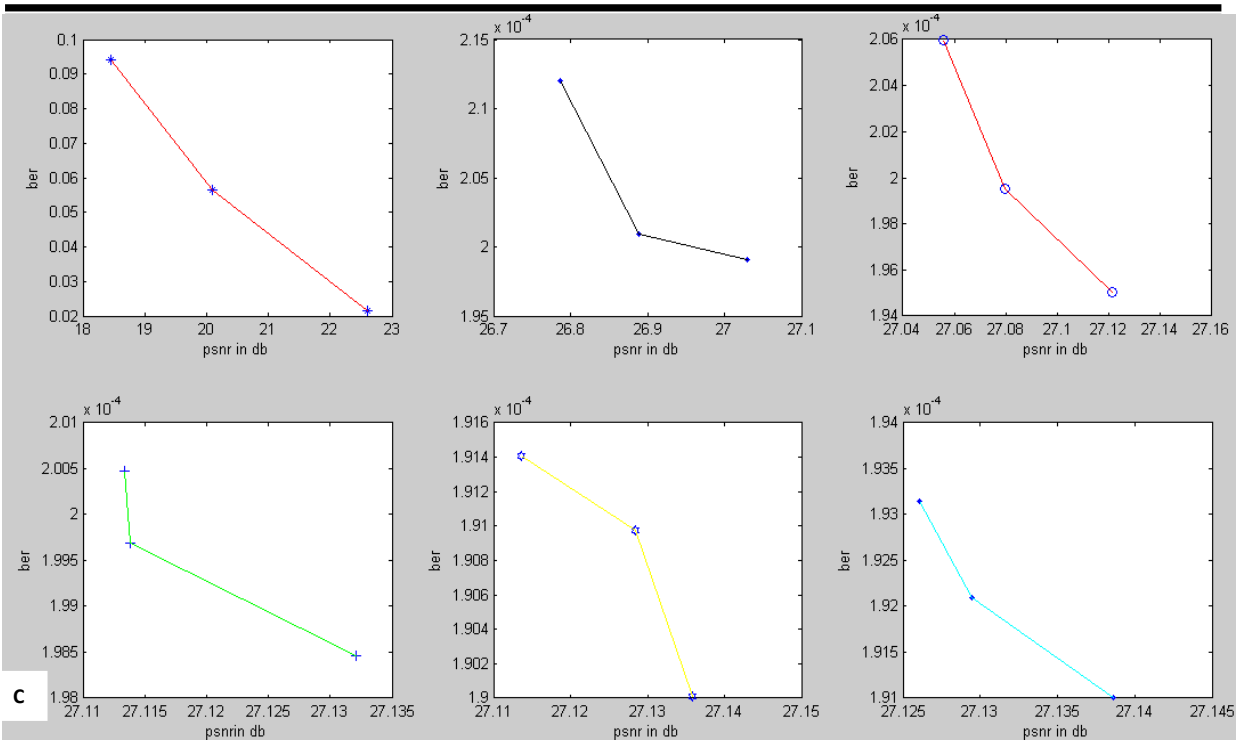


Figure (5) illustrate the relation between BER &PSNR in three cases (a) using WMISB (b) With noise ratio (c) with compress ratio.

VI. Conclusions

In this paper, we propose a bit insertion algorithm called Wavelet Modified Intermediate Significant Bit insertion algorithm (WMISB) for text steganography in gray images. The hiding of the ciphered bits is performed on both LH and HL wavelet parts of the cover image. Results were evaluated using PSNR where the acceptable robustness be obtained with (PSNR $\geq$ 30db) and BER converge to zero starting from the 4th bit plane. Visual and quantitative results demonstrate the applicability of the proposed WMISB insertion algorithm for text steganography.

References

1. " STEGANOGRAPHY FOR A LOW BIT-RATE WAVELET BASED IMAGE CODER" S.Areepongsa, Y.F.Syed ,N.Kaewkamnerd ,and K.R.Rao, The University of Texas at Arlington, Box 19016, TX 76019. Spectrapoint Wirless,1125E.Collins Blvd.,Richardson TX 75082.
2. "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit),"Akram M.Zeki and Azizah A. Manaf . World Academy of science, Engineering and Technology 50 2009 p.p 989-9 96
3. "RSA Cryptography" Taravat Moshtagh ,Department of Mathematics and Statistics,York University, January 19th 2006.
4."Wavelets and Filter Banks", Strang,G. and Nguyen, T., Wellesley-Cambridge Press,Wellesley,AM., 1996.
5. "Help of Mat lab Version 7", May 06,2004.

6. "Significance of Steganography on Data Security",Venkatraman, S., Abraham, A., and Paprzycki, M. Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04). IEEE Computer Society,2004.
7. "Digital Image Watermarking Using Localized Biorthogonal Wavelets" Suhad.H. ,Moussa A.,Amjad H. European Journal of Scientific Research ISSN 1450-216X Vol.26 No.4 (2009), pp.594-608 © Euro Journals Publishing, Inc. 2009 http://www.eurojournals.com/ejsr.htm.
8. "Robust and Blind Spatial Watermarking In Digital Image", Maity, S. P. Kundu, M. K., Proc. 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002), pp. 388 -393, Ahmedabad, India, 16-18th December,2002.
9. www.mathworks.com., MathWorks, Inc , last accessed on February 2007.

اسناد التحويل المويجي بإدخال قطعةِ هامّة لوسّطِ مُعَدَّلِ لفن الاختزالِ لنَصٍّ

مهندس / مدرس مساعد قصواء خالد عبود
جامعة بغداد/ كلية العلوم /قسم علوم الحاسبات

في هذا البحث تم اقتراح وتحقيق استخدام لنسخة محدثة من(ISB)المدخلة في ا لخوارزمية والتي تدعى بخوارزمية(MISB)لنص سري مشفر .النص السري يمرر من خلال متسلسلة من تقنيات التشفير وخوارزمية (ISB) المحدثة اقترحت لاخفاء وحدات متسلسلة من النص المشفر داخل التحويل المويجي لنقاط الصورة لغرض تطوير متانة النظام المشفر .النتائج توضح فعالية المويجة المطورة للـ(WMISB) بينما تحل اداءها باستخدام مقياس (PSNR) تجارب اضافية تحل للصورة المكبوسة والمشوشة لتغطية الصورلمقارنة (PSNR) لها. النتائج المستخرجة توضح فعالية(WMISB) المقترح ,كذلك BERهو المفتاح المستخدم لتقويم الانظمة التي ترسل بيانات رقمية من موقع الى اخر.