Novel Technology for Image Steganography Based on Multi-level DWT and Block Permutation System

Hussam Abd Ali Darweesh

Department of Computer Technology Engineering, University of Madenat Al-Elem, Baghdad- Iraq (Email: hussamuot@ yahoo.com).

Abstract

This paper proposes a novel technology for image Cryptography, steganography system and embedded high capacity data at the same time. The proposed technologic first encrypted the information by using Zigzag Order Block Permutation (ZOBP), which divides the image into sub-block of size (8*8), then permutated the Blocks depend on Cipher Key. The permutation blocks pixels by zigzag order. The Encrypted information has been converted by Discrete Wavelet Transform (DWT) series of bits in order to increase the power coefficients. The secret information bits embedded into Binary of the cover image after converted by Multi-level DWT. The secret bits replace by bits in cover coefficients. The image results after Inverse Discrete Wavelet Transformation (IDWT) called stego-image. This embedded information casing statistically significant modification to the cover image. The simulation results calculate Peak Signal to Noise Ratio **(PSNR)**, and Correlation test **(Cor)** as parameters of robustness, and quality of reconstruct image. The proposed system hides high capacity of data depends on the level of DWT to cover image that hiding Capacity parameter calculated by Bit per Pixel **(BPP)**. The proposed method hidden high capacity information with most security and quilility system.

Keywords: Imgesteganography, Image Cryptography, Multi-level Discrete wavelet Transform, Zigzag order Block Permutation (ZOBP), Peak Signal to Noise Ratio (PSNR), Correlation test (Cor.), Bit per pixel (Bpp).

تصميم تقنية جديده لأخفاء الصور السرية باستخدام المويجة المتقطعة الرقمية المتعددة بعد تشفير الصورة بواسطة تضمين اجزاء صغيرة من الصورة

المستخلص

البحث المقدم يقترح نظاماً جديداً يقوم بتشفير وإخفاء المعلومات ذات السعة الكبيرة. يعمل النظام المقترح اولاً بتشفير الصورة السِرّية وذلك بتقسيمها الى اجزاء ذات حجم (8*8) وتضمن باستخدام طريقة الزيكزاك (zigzag order) وبعدها يضمن كل جزء في الصورة المقطعة بالاعتماد على مفتاح سري (cipher key) لتوليد الصورة المشفرة (Encrypted Image). وتقوم عملية التشفير بتحويل الصورة المشفرة الى معاملاتِ Discrete Wavelet Transform (DWT) . وعن طريق زيادة طاقة المعاملات ثم تحولها الى متسلسلة من البت (stream of secret bits). ولكي نكمل عملية تشفير الصورة نقوم بتحويل صورة الغطاء(Cover Image) الى معاملات DWT ولعدة مرات (Multi-level). وبعدها نقوم بإخفاء المعلومات السرية (secret bits) داخل البت لصورة الغطاء وبعد الانتهاء من التحويل نعيد الصورة باستخدام Inverse Discrete Wavelet Transform لغرض توليد الصورة الحاملة stego-image. تتم المرحلة االاخيرة من العملية من خلال برنامج المحاكاةَ يقوم بالإضافة إلى برنامج الإخفاء بحساب نسبة طاقة الاشارة الى طاقة الضوضاء Peak Signal to Noise Ratio (PSNR) وعامل التقارب Correlation test (Cor) لحساب دقة الصورة المسترجعة بالمقارنة مع الصورة السرية الاصلية. تعتمد سعة الاخفاء للصورة السرية على عدد مرات اخذ Discrete Wavelet Transform لصورة الغطاء وكذلك يحسب نظام المحاكات عدد البت المخفية بالنسبة الى عدد وحدات الصورة (Pixels) في صورة الغطاء Bit per Pixel (Bpp) كعامل لسعة الاخفاء. وبهذه الطريقة تمكنا من أخفاء المعلومات ذات السعة الكبيرة وبكفاءة وأمنية عاليتين مقارنة مع طريقة الاخفاء بالبت الاخيرة (Least significant bit (LSB)) وطريقة المحولات (transformation methods).

1. INTRODUCTION

Data security is the methods to protecting data of computer and communication systems from unauthorized disclosure and modification [1]. Data in computer systems are in danger from many threats including indiscriminate searching, leakage, inference and accidental destruction [2].

Protecting security data is an important demand and there are two techniques available to transmit data using unprotected communication media [3]. First Cryptography can be defined more specifically as the area within cryptology that is making communication unintelligible to all except the intended recipient or it may be defined as the science of hiding Enciphering the contents of secret message from an attacker [4]. The secret message is scrambled and can be reconstituted only by the holder of the key [5]. Second Steganography represents a class of process used to embed data into various forms of media such as image, audio or text with minimum amount of degradation to the cover image, so that the fact secret message is being transmitted is also a secret [6].

In cryptography, the structure of a message is changed to render it meaningless and unintelligible unless the decryption key is available, cryptography makes no attempt to disguise or hide then coded message [4]. Steganography does not alter the structure of the secret message, but hide it inside a cover [7]. The system has been proposed combines the techniques by encrypting message using cryptography and then hiding the encrypted message using Steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged.

The challenge in information-hiding method can operate with either high payload capacity or high robustness to modification, but not both [8]. Robustness: The embedded data should be as immune as possible to modifications from intelligent attacks. Capacity: Ideally we want large capacity but would affect Imperceptibility and robustness. Security: the inability of adversary to detect hidden images accessible only to the authorized user [9].

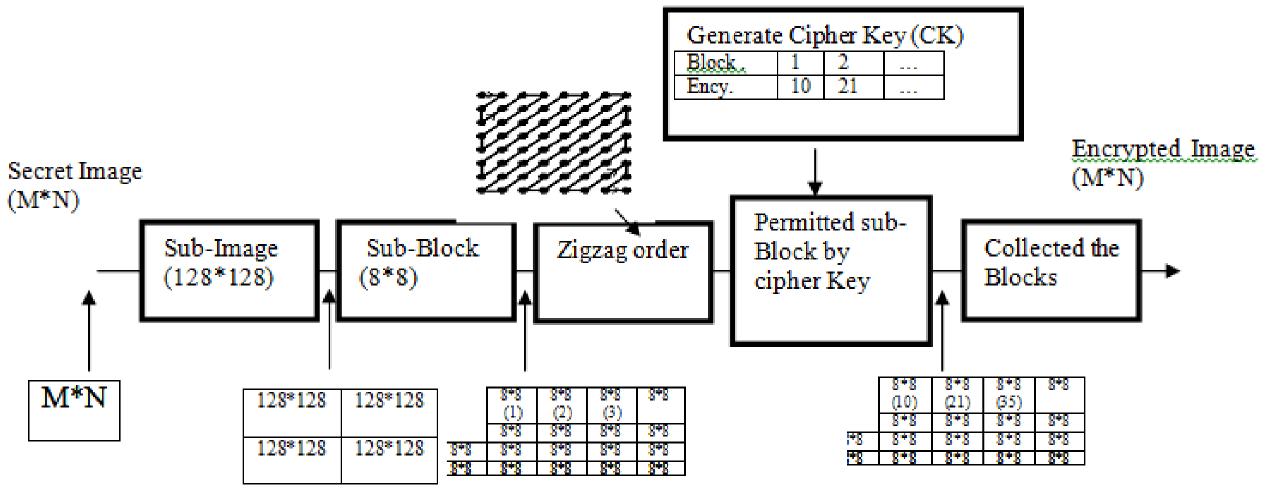
Contribution of this paper as, is that the secret image has been embedded in the detailed bands of the Covert image. The two primary classes of digital image steganography are least significant bit (LSB) steganography and transform based steganography [10]. LSB steganography is more susceptible to image manipulation than transform based steganography [7]. Transform based steganography has the potential to achieve higher payload capacity than LSB steganography [11].

In this work the secret image is encrypted using Zigzag Block order ZOBP, increasing DWT power coefficients, then embedded the secret binary in binary cover image wavelet coefficients. This method results high quality and capacity embedded data and more security.

2. The PROPOSED CRYPTOGRAPHY SYSTEM

The proposed cryptography technique is shown in Fig.(1) and can explain by the following steps:

1. Divide the image into not join sub-image of size (128*128).
2. Divide every sub-image into not join sub-block of size (8*8).
3. Name every sub-block by sequence number start with one to up-left corner sub-block then increased the block numbers row by row.
4. Generate Cipher Key contain integer unrepeated numbers between (1 to number of sub-Blocks).



1- Every sub-block permuted by using Zigzag order as shown in Fig.(1) [12].
2- Permuted the sub-blocks depend on numbers in cipher Key as shown in Fig.(2).

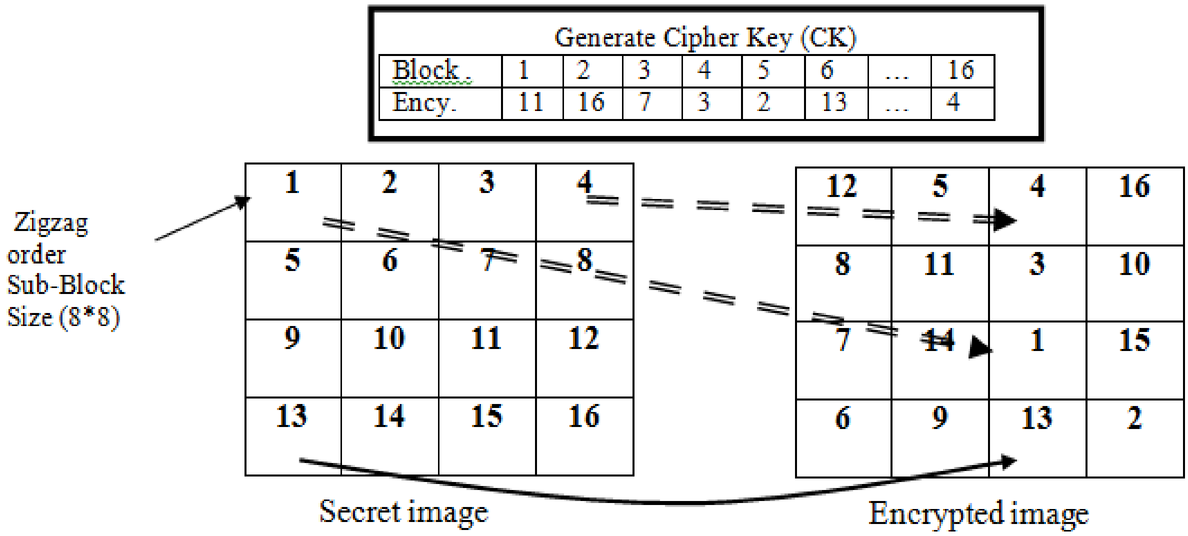
The Encrypted and Decrypted system used the same cipher key to reconstructed image.

3. THE PROPOSED IMAGE STEGNOGRAPHY SYSTEM

I. Embedding of secret image

The embedding block diagram shown in Fig.(3) consist of the following steps:

1. The cover Gray-level image which have a flat histogram. This image is almost perfect distribution of pixel, which can hide the secret image in.



Generate Cipher Key (CK)

Block	1	2	3	4	5	6	…	16
Ency.	11	16	7	3	2	13	…	4

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

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

Fig. (2). Schematic of Encrypted System.

2. The DWT is considered to the cover image. The DWT2 divides the cover image into four quarters as shown in Fig.(4-a) [13] the upper-left (LL) is the cover image but with small scale. The three quarters (LH, HL, and HH) are the shadow of the cover image that the secret information will be embedded in these quarters, another DWT2 taken into LL of the first level to have second level DWT2 to increase the place of hiding data …atc as shown in Fig.(4-b). the vector **U** for n-level DWT2 are

$$\mathbf{U}=[LHn, HLn,HHn,\ldots,LH_1,HL_1,HH_1] \qquad \ldots.(2)$$

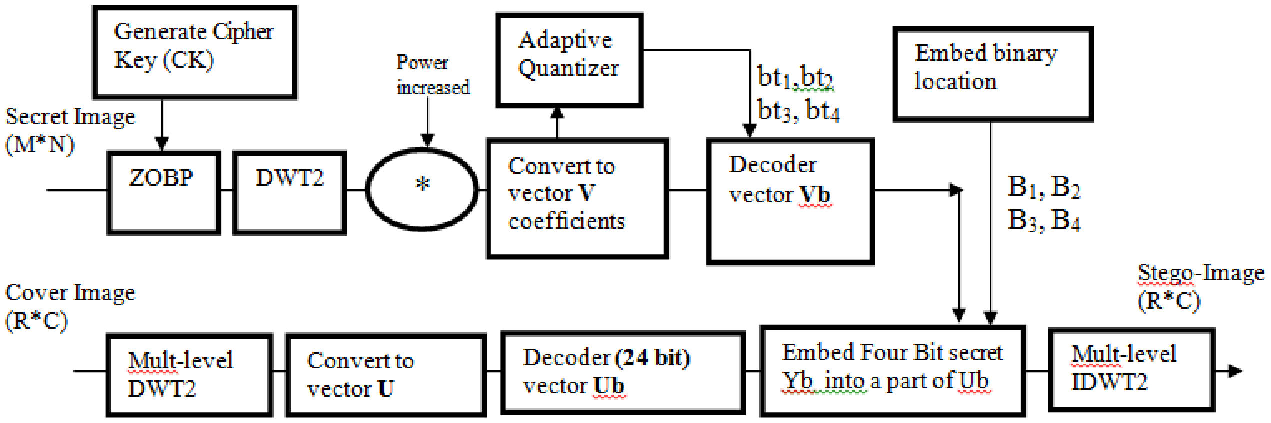


Fig. (3). Proposed Embedding System.

1. Re-arrange the cover coefficients as one dimension vector start from high level down to low-levels (expected the LL) as in eq.(2), then convert it by fixed decoder of 24 bit as shown in Fig.(5). The vector $\mathbf{U_b}$ are:

$$\mathbf{U}=[LHn*24, HLn*24, HHn*24 ,\dots, LH_1*24, HL_1*24, HH_1*24] \quad \dots (3)$$

2. The **secret image** transfer by DWT2 then increased the power of secret DWT coefficients by factor (Pinc), that result high equality to the reconstructed image.
3. Re-arrange the secret coefficients as one dimension vector as

$$\mathbf{V} = [LL, LH, HL, HH]. \quad \dots.(4)$$

4. The number of bits for every part of Vector **V** decided by adaptive quantizer [13]. The part power is the more important parameter to decide number of bit, the analogy to digital converter shown in Fig.(1) design uniform fixed decoder for every part of secret coefficients this generate binary vector $\mathbf{V_b}$.

$$\mathbf{Vb} = [LL*bt1,LH*bt2,HL*bt3, HH*bt4] \quad \dots..(5)$$

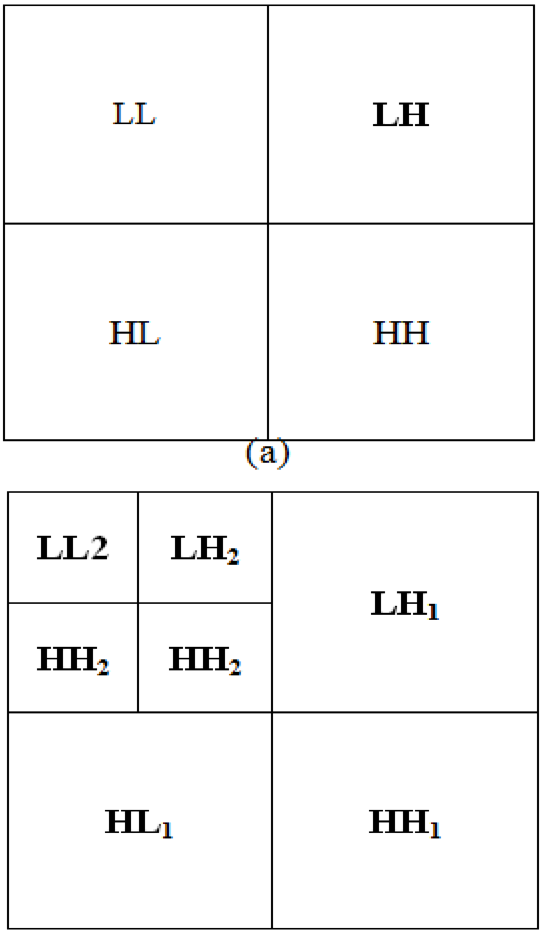
Where

bt1: number of bits to decode LL.

bt2: number of bits to decode LH.

bt3: number of bits to decode HL.

bt4: number of bits to decode HH.



(a)

(b)

Fig.(4) Discrete Wavelet Transformation Decomposition [13]

(a) 1-level DWT (b) 2-level DWT .

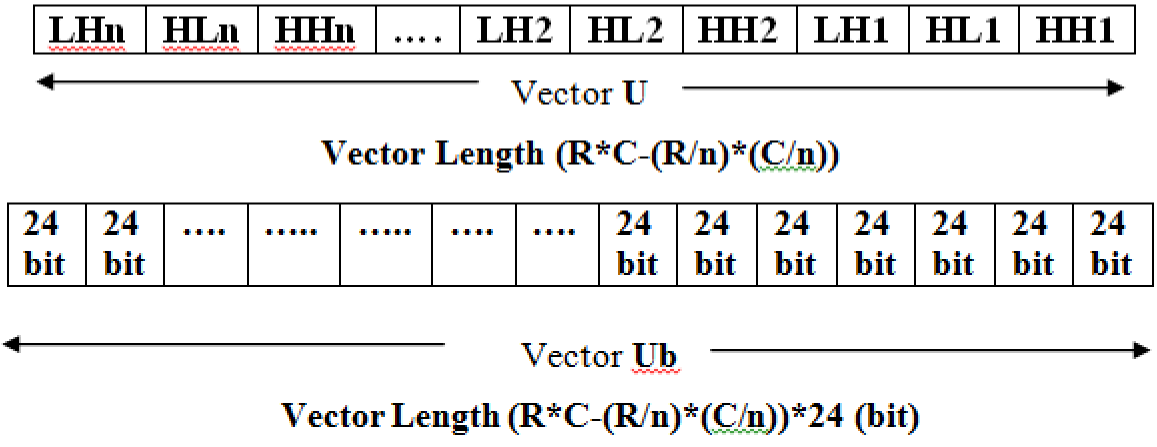


Fig.(5) Vector (U) Form n-level DWT2 Coefficients of Cover Image, and vector Ub (binary vector of cover image) .

3- Replacing every sequence four bits of the cover image, by the four sequence bits of the secret information.
4- The locations of embedded bits [B1, B2, B3, B4] can be generated randomly to increase degree of cipher.
5- The (n) -level IDWT2 to the cover coefficients generate stego-image.

II. Extraction of the secret Image

This process work powerfully to reconstruct secret image if same parameters of the embedded process received. The DWT of cover image levels (n), start location of embedded bit (Bi), number of bits that convert secret image DWT bands to Binary, power factor increasing of the secret image (P_{inc}), and Cipher key (CK).

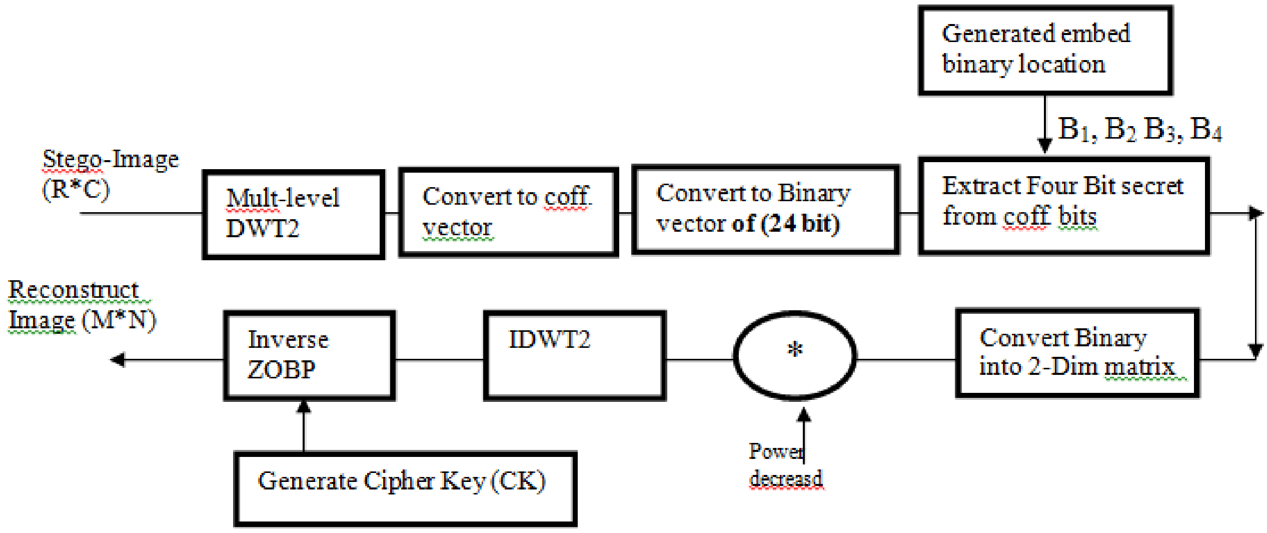


Fig.(6) Proposed Reconstructed System

The Reconstructed block diagram shown in Fig.(6) it consist of the following steps:

1- The received stego-image has been transformed by n level DWT2 transform.
2- re-arrange the DWT coefficients as shown in Fig.(5).
3- Extract the sequence four bits of location (B1, B2, B3, and B4) from cover image.
4- The Binary vector reconstruct convert to two dimension DWT coefficients
5- All coefficients divided by factor (P_{inc}).
6- IDWT2 to the reconstructed values.
7- Decrypted the image use the same cipher Key in the Encrypted process.
8- Reverse the Zigzag order to all blocks
9- Collect the sub-blocks, and sub images to generate reconstructed image.

4. FIDELITY CRITERIA

There are two types of image fidelity criteria namely, the objective and subjective criteria [11]. The first one depends on equations that are used to measure the amount of the error in the reconstructed image. While the second require the definition of qualitative scale to assess image quality and this scale can then be used by human test subjective to determine image fidelity [8].

I. The Similarity Test

Similarity test is the correlation between the two images, before and after process. When the two image are perceptually similar, then the correlation equals one. The correlation can be calculated as shown below [2]

$$Corr. = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j)-\overline{X})(Y(i,j)-\overline{Y})}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j)-\overline{X})^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(Y(i,j)-\overline{Y})^2\right]}} \quad ....(6)$$

where

*M and N:*height and width of the two images (because the two images must be of the same size).

i *and* j*: row and column numbers.*
X(i, j): the original image.

Y(i,j): modified image.

$\overline{X}$, $\overline{Y}$: Mean of original and modified image, respectively, and calculated by

$$\overline{X} = \frac{\sum_{i}^{M}\sum_{j}^{N}X(i,j)}{M \times N} \quad ..(7)$$

$$\overline{Y} = \frac{\sum_{i}^{M}\sum_{j}^{N}Y(i,j)}{M \times N} \quad ..(8)$$

II. Peak Signal to Noise Test (PSNR)

According to the human visual system, some amount of distortion between the original image and the modified one is allowed. Here the *PNSR* is employed to indicate the performance of the method. *PSNR* is usually measured in *db* as given in [10].

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[Y(i,j)-X(i,j)\right]^2} \quad ..(9)$$

where:

L-1: maximum gray level (in Gray-level image equal to *L-1*=255).

The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image as a parameter of robustness, otherwise, the PSNR between secret image and reconstructed image as a parameter of equality. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego-image.

VI. Capacity Measure

The notion of capacity in data hiding indicates the maximum number of bits that can be hidden and successfully recovered by the steganographic system. Therefore the number of hidden bits varies depending on cover image size. To measure the hidden capacity bit per-pixel (BPP) is the factor of hidden capacity that given by [12]

$$BPP = \frac{Hidden\ Secret\ \ \mathrm{Im}age\ Bit}{Cover\ \mathrm{Im}age\ Pixel\ Size} \quad ...(11)$$

5. EXPERIMENTAL RESULTS

In this section, some experiments are carried out to prove the efficiency of the proposed system. The proposed technique has been simulated using the MATLAB-10 program platform. A set of 8-bit grayscale images of size 512 × 512 are used as the cover-image to form the stego-image. All results used power increased by ($P_{inc.}$=10).

The experiment results show that we can reconstruct the secret images from the stego-image without error matching image

(corr.=1 and PSNR= ∞) for hidden capacity less than 2.75 BPP.

Wherever, the different image between cover and stego-image gives the subjective criteria. The proposed system steps, shows in Fig. (7- a) is the original secret image (airplane (300*300)), Fig.(7-b) the Encrypted image by cipher Key using ZOBP method, Fig.(7-c) the DWT2 of the secret image, Fig.(7-d) the cover image (Lena), Fig.(7-e) the 2-level DWT2 to cover image, Fig(7-f) the 3-level DWT2 to cover image, Fig(7-g) the stego-image, Fig. (7-h) shows the differences image between cover image and stego-image image, and Fig.(7-i) decrypted reconstruct secret image.

The result for embedded the image airplane of size (300*300) in three different cover images (boys, City, and Flowers) the hidden capacity (3 Bpp), with 3-level DWT2 shown in Fig.(8). Fig.(9) shows the result for embedded the image MAP in the same three different cover images by used 3-level DWT2. The stego-images are the same as the cover images in visual. That shows the good transparency of the system.

The objective results shown in Table (1) corr., PSNR$_C$ (the PSNR between cover image and stego-image) for four different cover images, and PSNR$_S$ (the PSNR between secret image and reconstruct image) for two secret images. As shown in Table (1) for different secret image, the results have been recorded for 2-level and 3-level DWT2 to cover images. This result indicated the change in cover image don't gives high improved to PSNR$_C$ and don't effect at PSNR$_S$. The objective results gives little change when increased the DWT2 levels, whenever, that increase the hiding place and increased hidden data capacity as shown in Table (2). 3-level DWT2 gives improvement in the PSNR$_C$ and PSNR$_S$ compare with 2-level DWT2 and increasing the hidden data capacity.

The objective results obtain little change in PSNR$_C$ and PSNR$_S$ at hidden capacity less than 3.125 Bpp, when gives high drop in PSNR$_S$ in hidden capacity greater then 3.2 Bpp as shown in Table (2).

6. CONCLUSIONS

In this paper, a proposed Cryptography and steganography technique in DWT domain to improve security and quality of hiding data. According to the simulation results the stego-images of this method are almost identical to the original images. a proposed system also provides additional five layers of security by means of transformation (DWT and IDWT) of secret image, Multi-level DWT of cover image, encoding of secret image, location of embed bits, and secret DWT power coefficients increase.

The demand of robustness in image Cryptography and steganography filed and quality of reconstructed secret image is requested as strongly as it is in LSB methods or transformation method. In our proposed system the BZOP methods, the embedding process is hidden under the transformation of both cover and secret images, increasing the secret coefficients power. These operations and encoding of secret image keep these images away from stealing, destroying from unintended users, hence the proposed method may be more robust against brute force attack. a proposed system has hidden data capacity greater than that in LSB methods or transformation method, with matching reconstructed secret images.

Table (1) The objective results of proposal system for different secret and cover images, hidden data capacity of 2.75 BPP.

2-level DWT2
Secret image airplane (300*300)

Cover Image (512*512)	Corr.	PSNR$_C$ (dB)	Corr.	**PSNRS (dB)**
Lena	0.999999591	65.692	1	**320.6**
Boys	0.99999766	66.381	1	∞
City	0.99999616	66.315	1	∞
Flowers	0.99999722	66.044	1	∞
Secret image Map (300*300)				
Lena	0.9999966	66.494	1	∞
Boys	0.99999804	67.170	1	∞
City	0.99999671	67.021	1	∞
Flowers	0.99999766	66.792	1	∞

3-level DWT2
Secret image airplane (300*300)

Cover Image (512*512)	Corr.	PSNR$_C$ (dB)	Corr.	**PSNRS (dB)**
Lena	0.99999596	67.742	1	**316.66**
Boys	0.999997679	66.413	1	∞
City	0.99999623	66.399	1	**316.66**
Flowers	0.99999724	66.0823	1	**316.68**

Secret image Map (300*300)				
Lena	0.99999666	66.576	1	**320.398**
Boys	0.99999808	67.247	1	**320.398**
City	0.99999675	65.042	1	∞
Flowers	**0.99999769**	**66.865**	**1**	**320.39**

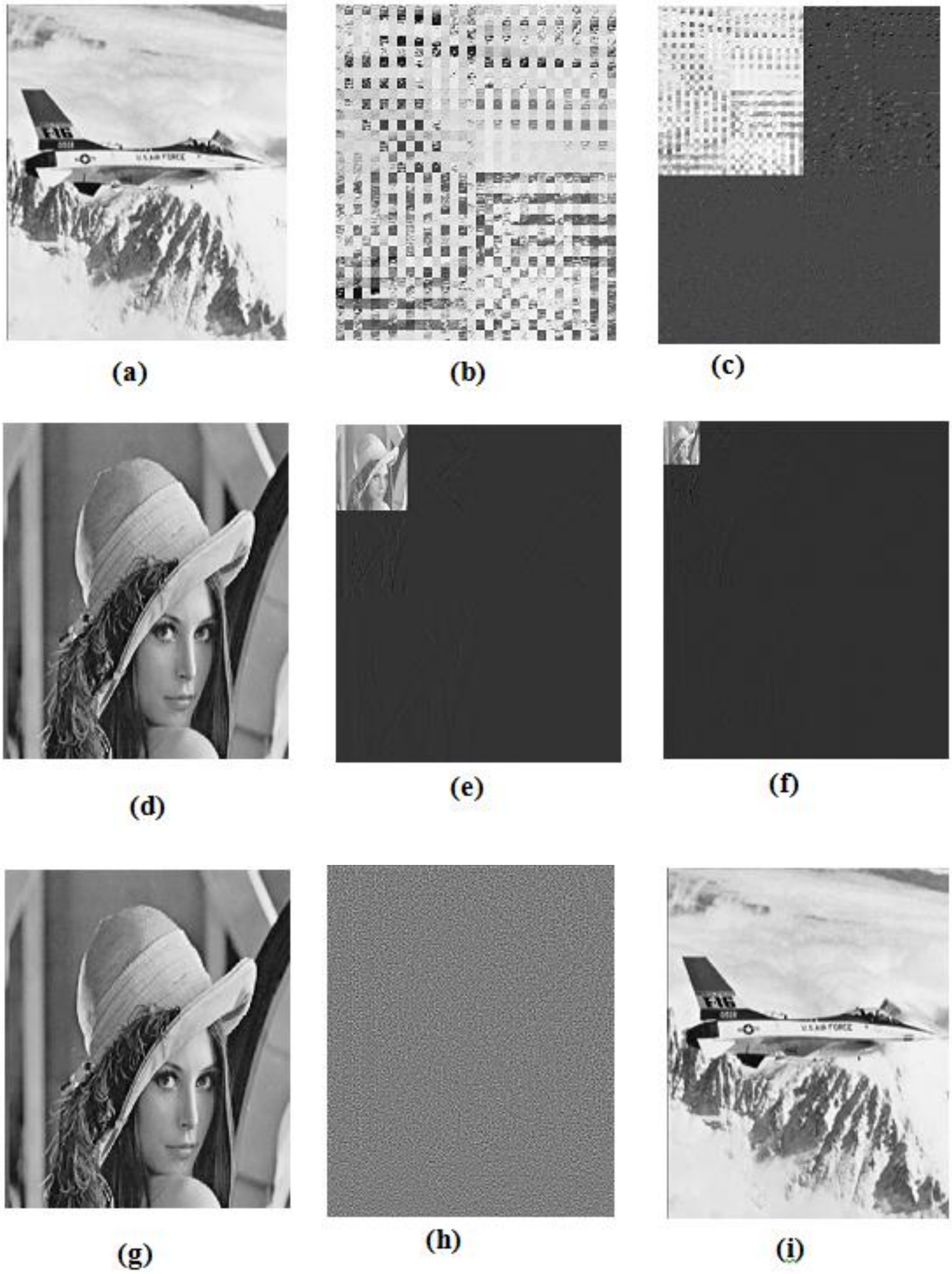
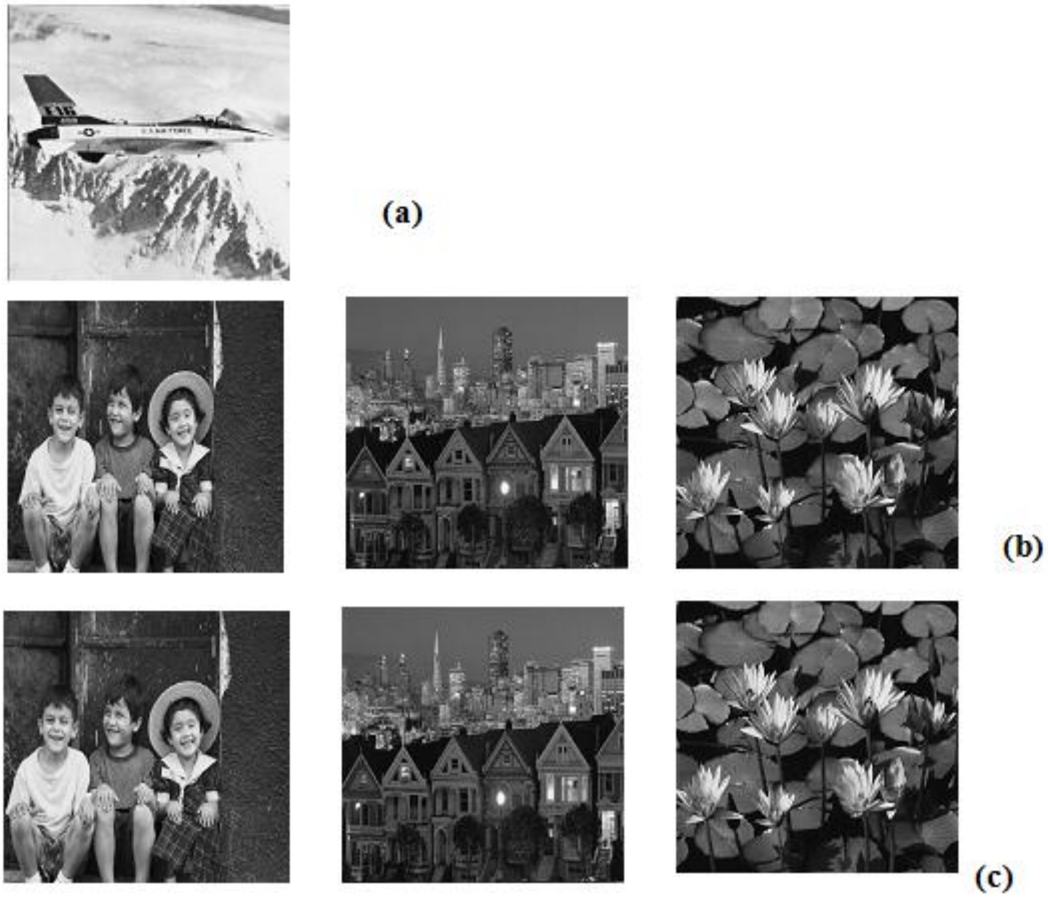


Fig.(7) Experimental Result for the Proposal technique. The Objective Result are Corr.=.99999718, PSNR_C = 67.31 dB, PSNR_S= ∞ dB, and BPP = 2.75 bit/pixel

(a) Original secret image (airplane (300*300)), (b) Encrypted image by ZOBP (c) Wavelet 2-level for scaling secret image (d) Cover images (Lena (512*512)), (e) Wavelet 2-level to cover images, (f) Wavelet 3-level to cover images, (g) Stego-images, (h) Different between cover and stego-image, and cover image, (i) the Decrypted Reconstructed secret image.



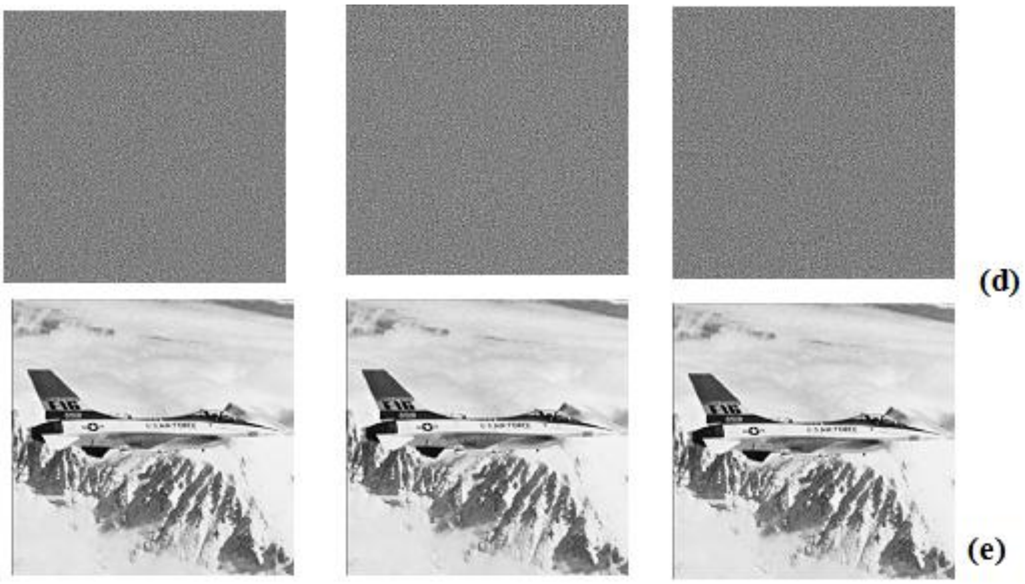


Fig.(8) Proposal System Experimental Results used Different Cover Image Hidden Capacity 2.75 BPP.

The reconstructed image matching to secret image (a) Original secret image (airplane (300*300)),

(b) Cover images (512*512), (c) Stego-images, (d) Difference between cover and stego-images,

(e) Reconstructed secret image.

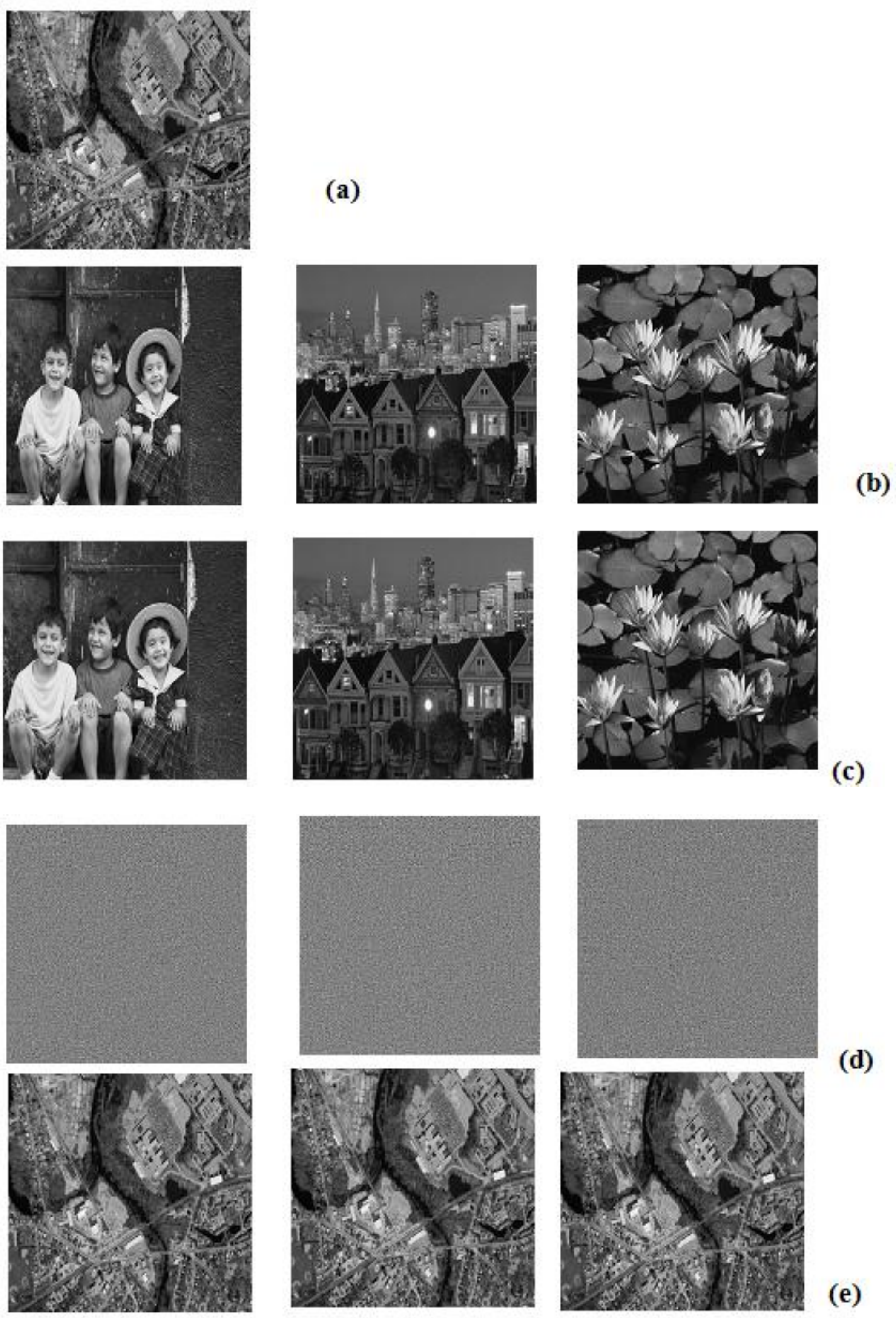


Fig.(9) Experimental Result for the Proposal System used Different Cover Image Hidden Capacity 2.75 BPP. (a) Original secret image (Map (300*300)), (b) Cover images (512*512), (c) Stego-images, (d) Difference between cover and stego-images,

(e) Reconstructed secret image.

REFERENCE

1. E. T. Lin and E. J. Delp***“R Review of Data Hiding in Digital Images”*** Purdue university, west Lafayehe, Indiana, 1999.

2. C. P. Pures., "***Security In Computing***", Prentice Hall, 2006.

3. W. Stallings "***Cryptography and Network Security Principles and Practices***", Fourth Edition, Prentice Hall, November, 2005.

4. A. Nag, S. Biswas, D. Sarkar, P.P. Sarkar, ***"A novel technique for image steganography based on Block-DCT and Huffman Encoding",*** International Journal of Computer Science and Information Technology, Volume 2, No. 3, pp. 103-112, June 2010.

5. M. S. Kasem., D. Muhammad., M. Kasem, and Khaled A., ***"Singular points detection using fingerprint orientation field reliability",***International Journal of Physical Sciences Vol. 5(4), pp. 352-357, April 2011.

6. S. Torres-Maya, M. Nakano-Miyatake and H. Perez-Meana, ***" An Image Steganography Systems Based on BPCS and IWT",***IEEE International Conference on Electronics, Communications and Computers, 2006.

7. R. C. Gonzalez and R. E. Woods ***" Digital Image Processing "***, Third Edition, Prentice Hall Upper Saddle River, New Jersey, 2008.

8. K. B. Raja, Vikas, V. KR, and L. M. Patnaik,***" High Capacity Lossless Secure Image Steganography using Wavelets"***, IEEE, 2006.

9. Y. Ying Chung, Y. Sun, ***"High Capacity Image Steganography System Using Wavelet Zerotree"***, Transations on Engineering, Computing and Technology, December 2004.

10. H. A. Darwessh., and A. Hussan, "***High Capacity Secret Image Steganography using DWT",***second conference university of Technology, April, pp 5-16, 2009.

11.C. Solomon, and T. Breckon, ***"Fundamentals of Digital Image Processing "***, John Wiley & Sons, Ltd 2011.

12.K. Mohemed., A. P. Kursem., and M. Solon, "***Image Denoising And Enhancement Using Multiwavelet With Hard Threshold In Digital Mammographic Images"***, International Arab Journal of E-Technology, Vol. 2, No. 1,pp 49- 56, January 2011.

13.P.-Yueh Chen and H.-Ju Lin *" **A DWT Based Approach for Image Steganography**"* International Journal of Applied Science and Engineering, 275-290, April 2006.