Wavelet Based Fast Technique For Images Encryption

Maytham A. Shahed
Computer Science Dept.- Science College- Basrah University- Basrah- IRAQ

Abstract

In recent years, image encryption and compression plays an essential roll in modern data communication fields, such as images storage in database.

This paper presents a fast technique which is used to encrypt four different images into one encrypted image having a size less than the sum of the sizes of the original images -which have different sizes- using wavelet transform. This technique has many advantages: low storage requirements for the resultant image, simple, fast, and secure.

Several examples are given to illustrate the performance of the proposed technique and it gives good results for both grayscale and RGB color images.

Keywords : Image Cryptography, Image, Wavelet Transform

تقنية سريعة لتشفير الصور معتمدة على التحويل المويجي

ميثم ابوالهيل شهيد
قسم علوم الحاسبات- كلية العلوم- جامعة البصرة- البصرة- العراق

المستخلص

في السنوات القليلة الماضية, لعب تشفير الصور وضغطها دوراً اساسياً في مجالات اتصالات البيانات الحديثة كخزن الصور في قواعد البيانات.

البحث الحالي يعرض تقنية سريعة تهدف الى تشفير اربعة صور مختلفة الابعاد لانتاج صورة مشفرة ومضغوطة حجمها اقل من مجموع حجوم الصور الاصلية وذلك بالاعتماد على التحويل المويجي. تمتلك الطريقة الحالية عدة ايجابيات منها: استفادة قصوى في وسائل الخزن والبساطة والسرعة والسرية.

تم استعراض عدة امثلة لبيان اداء التقنية المقترحة باستخدام صور عادية وملونة وقد كانت النتائج جيدة.

الكلمات المفتاحية : تشفير الصورة, الصورة, التحويل المويجي

1. Introduction

Cryptography has an extensive and mesmerizing history. The traces of cryptography can be found some 4000 years ago in the Egyptian civilization. It's an art and science of scrambling information. But this very feature of information scrambling is nowadays becoming an impediment because government agencies across the world are trying to control the use of cryptography. These agencies think cryptography is hindering their intelligence gathering activities. This move resulted in widespread study of steganography. Steganography which literally means, *"covered writing"* includes methods of transmitting secret message through innocuous cover mediums in such a manner that the existence of the embedded messages is undetectable. Researchers have shown how both these techniques, if usedtogether can provide a high level of security (Zenon et al., 1997).

Unlike text messages, image data have their special features, such as bulk capacity, high redundancy, and high correlation among pixels, not to mention that they usually are huge which together make traditional encryption methods difficult to apply and slow to process (Borie et al., 2004).

The importance of wavelet as a multi-resolution technique comes from its decomposition of the image into multilevel of the independent information with changing the scale like a geographical map in which the image has non-redundant information due to the changing of scale (Varma and Bell, 2004). In this way, every image will be transformed in each level of decomposition to a one low information image and three detailed images in the horizontal, vertical, and diagonal axises. Also the low information image can be decomposed into another four images. These approaches of decomposition process provide us with a number of unrealizable features in the original image, which appear in the their levels after the application of

transformation. So, the wavelet can be regarded as the most efficient transform that deals with image, sound or any other pattern since it provides a powerful time-frequency representation (Norcen et al., 2003).

In the present technique, the wavelet transform was used to encrypted four different images with different sizes to produce one image having high security and small size .

This paper is organized as follows: Sec. 2, are the researches of image cryptography summary. Sec. 3, an introduction to wavelet transform. Sec. 4, explains the proposed technique. Sec. 5, evaluates the proposed technique using grayscale and RGB color images, and finally Sec. 6, shows the conclusions.

2. Image Cryptography

Image cryptography was not studied as normal cryptography or visual cryptography. It was used by Zenon (Zenon et al., 1997), to encode digital media (images and video) to provide confidentiality and intellectual property protection against unauthorized access. They proposed a version of digital image cryptography by using random phase mask for encrypting image. The authors consider image encoding as a new form of image encryption. They accomplish this using a transformation technique based on random phase masks. Their technique of encryption consists of four major steps. Fourier transform of initial image, phase modification, inverse Fourier transform and finally image conversion. It is a good concept but the weakest link lies in the use of steganography. Zenon (Zenon et al., 1997) used image cryptography and steganography to increase security but they have not considered the use of image cryptography to disguise text cryptography which would provide enhanced privacy and confidentiality in cryptographic communication.

Cheng and Li (Cheng and Li, 2000) proposed a solution called *partial encryption*, in which a secure encryption algorithm is used to encrypt only part of the compressed data. Norcen et al. (Norcen et al., 2003) discuss computationally effect techniques for confidential storage and transmission of medical image data.

3. Wavelet Transform

The wavelet transform have two terms, each one is a set of functions takes the forms (Antonini et al., 1992, Baxes, 1994):

$$\psi(x) = \sqrt{2} \sum_{k=-\infty}^{\infty} g_k \psi(2x - k) \quad \ldots(1)$$

$$\phi(x) = \sqrt{2} \sum_{k=-\infty}^{\infty} h_k \phi(2x - k) \quad \ldots(2)$$

These sets of functions are formed by dilation and translation of a single function $\boldsymbol{\psi(x)}$, called as the *mother function* or *wavelet function* in equation (1). The second function in equation (2), $\boldsymbol{\phi(x)}$ is called the *scale function*. Where $\boldsymbol{g_k}$'s and $\boldsymbol{h_k}$'s are analysis filters coefficients with $\boldsymbol{h}$ and $\boldsymbol{g}$ be the analysis filters (Saha, 2001, Xiong et al., 1999). The wavelet transform performs an octave subband decomposition of an image. The output of the first analysis stage is the low-low (LL) subband (an approximation of the original image); the high-low (HL) subband (the horizontal detail); the low-high (LH) subband (the vertical detail); and, the high-high (HH) subband (the diagonal detail).

Wavelet analysis allows the use of long time intervals where we want more precise low-frequency information, and shorter regions where we want high-frequency information (Baxes, 1994). The low-frequency content is the most important part. It is what gives the signal its identity. The high-

frequency content, on the other hand, imparts flavour or nuance. Subband coding is a coding strategy that tries to isolate different characteristics of a signal in a way that collects the signal energy into few components. This is referred to as energy compaction. Energy compaction is desirable because it is easier to efficiently code these components than the signal itself (Usevitch, 2001). An example of three level decomposition of image into subbands using wavelet transform is illustrated in Figure 1 (a), whereas Figure 1 (b) shows parent/children relationship among levels.

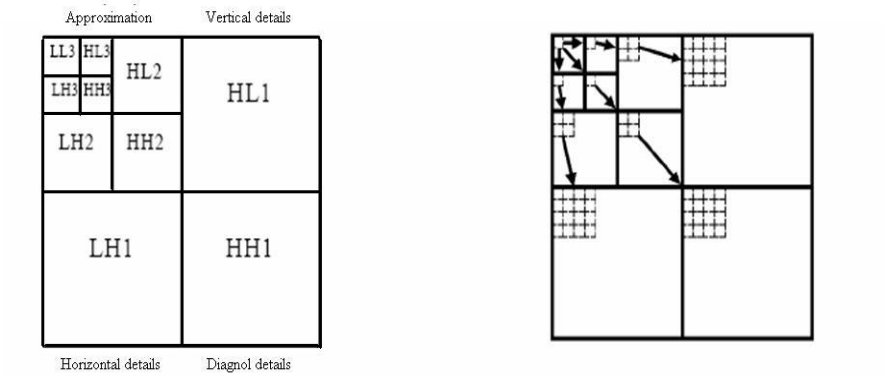

Figure (1): (a) 3 level wavelet decomposition, (b) Relationship between higher and lower level coefficients(parents/children)

4. Proposed Technique

The proposed technique aims to encrypted four different grayscale or RGB images – which have different sizes – to produce one image with size 256×256 or 512×512 by using wavelet transform. After resizing the four images and the key image to one of the previous sizes, the wavelet transform is applied to the four images and the subband LL1 is taken to produce transposition image by coping a block of pixel defined by the user from each image to the transposition image according to the image sequence defined by the user and this operation is repeated until all pixels in the four images are copied to the transposition image. Then the pixel-pixel XOR

operation is performed between the transposition image and the key image after rearrange it by using zigzag scan to get the final encrypted image. The encryption algorithm steps summarize as follows :

1. Read four different original images numbering {1,2,3,4}, respectively and the encryption key (image). Each images have any size.
2. Read an integer value N (where, N= 256 or 512).
3. Save the dimensions of the original images in a vector (ISIZE) and resize all images in step (1) to the size N×N pixels by using nearest neighbor interpolation.
4. Rearrange the N×N encryption key (image) by using zigzag scan to obtain a vector, and then reshape the resulted vector to N×N pixels image.
5. Read an integer value (BSIZE) in form (2^m, $0 \leq m \leq 7$), which represents the number of *adjacent pixels* that will be copied from original images to the transposition image in each time.
6. Read an integer vector (IORDER) having ($4 \times k$, $1 \leq k \leq 32$) items. Each adjacent four items in this vector contain the images numbers {1,2,3,4} scattered (permutation form), which determine a sequence of original images that will be copied its pixel(s) to the transposition image (e.g., 4231, 41232143, 423113244123, …, etc).
7. Apply Discrete Wavelet Transform (DWT) for one level for each image resulting from step (3) alone, excepted the key (image) and select subband (LL1) for each image (result from DWT) to obtain image (N/2 × N/2) pixels and neglecting the other subbands.
8. Copy BSIZE of adjacent pixels from each image resulting from step (7) in transposition image according to the images sequence determined by the IORDER and repeat this step by considering IORDER as a circular

vector until all pixels in the four images (N/2 × N/2 pixels) were copied to the transposition image to obtain N×N pixels image, then save the ISIZE vector in candidate place within the transposition image.

8. Apply XOR operation (pixel-pixel) between the transposition image and the key (image) resulting from step (4) to obtain final compressed and encrypted image N×N pixels.

The diagram of encryption and decryption steps of proposed technique is shown in Figure (2). The current technique has many advantages:

The proposed technique is simple technique because it does not need complex arithmetic operations. It takes little processing time compared with other well-known technique, such as AES cipher and stream cipher. The encryption algorithm needs low storage requirement because its encrypted four images with different sizes in one image having size less than the sum of sizes of the original images.

It has high security and making brute force attack infeasible.

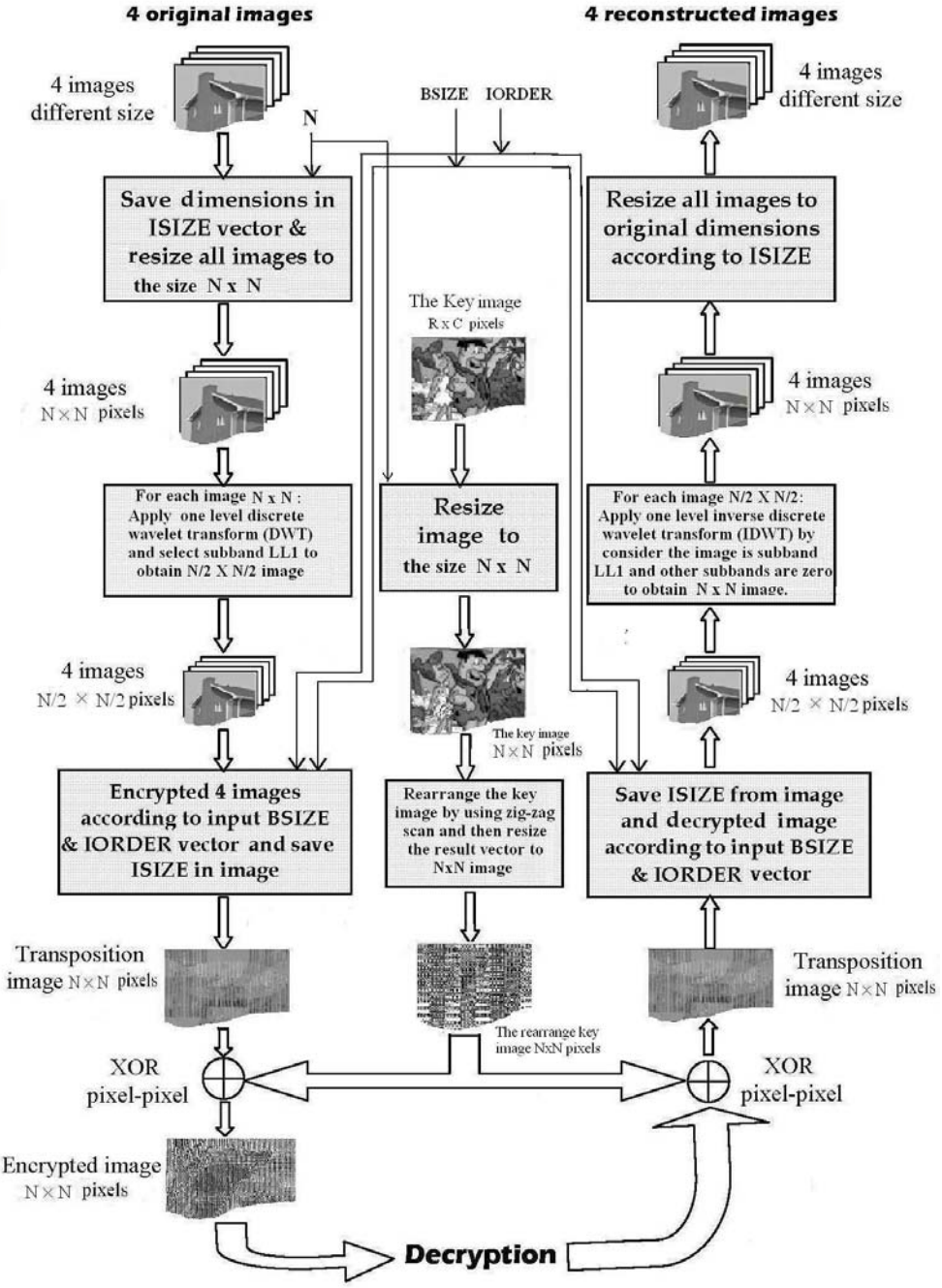

Figure (2): The proposed images encryption technique diagram

5. Results

In this section, a number of tests which are used to examine the proposed wavelet based images encryption algorithm will be presented. The algorithm was programmed in MATLAB version 6.5 on a Pentium IV PC (2.26 GHz) using *8-bit greyscale* and *24-bit RGB color* images with different sizes.

To evaluate the proposed technique, five aspects were examined (Li et al., 2006, Öztürk and Sogukpinar**,** 2004):

1. **Security**. Security in this work means confidentiality and robustness against attacks to break the images. It is obvious that the goal is not 100% security, but used encryption technique that make them difficult to cryptanalysis.
2. **Speed**. Less data to encrypt means less CPU time required for encryption. So, the current technique do not used complex arithmetic operations which resulted in reducing encryption and decryption time.
3. **Compression Ratio (CR).** Measures the compression ratio between the compressed image size (represent here encrypted image size) and the uncompressed image size (represent here the sum of the original input images sizes). It is defined as (Saha, 2001) :

$$CR = \frac{Compressed\ image\ size}{Uncompressed\ \ image\ size} \qquad \ldots (3)$$

When CR=0.6, this means that the data occupies 60% of its original size after compression. The aim is to get a CR near to zero.

4. **Keyspace Analysis**. A good image encryption algorithm should be sensitive to the cipher key, and the keyspace should be large enough to make brute-force attack infeasible. In current work, the size of the keyspace is (512×512 = 262141) or (256×256 = 65536) according to N value.
5. **Correlation**. Correlation (*Corr*) measures the similarity between the original image and the reconstructed image. The aim is to get a

correlation value closed to 1. The correlation can be defined as (Al-Obaidi, 2004):

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad \ldots(4)$$

Where,

$I_1(r,c)$: is the value of pixel at *(r,c)* of the original image.

$\bar{I}_1$: is the mean of the original image that:

$$\bar{I}_1 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_1(r,c) \quad \ldots(5)$$

$I_2(r,c)$: is the value of pixel at *(r,c)* of the reconstructed image (or modified image).

$\bar{I}_2$: is the mean of the reconstructed image (or modified image) that:

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_2(r,c) \quad \ldots(6)$$

Where,

M: height of the image. *N*: width of the image.

r and *c*: row and column numbers.

a.Test 1

The proposed technique was tested more than twenty five times. In each test different four *8-bit grayscale* images and key (image) were used. The results of one of these tests are summarize in Table (1), and all its images are shown in Figure (3). The original images are: *Lena, Pepper, Birds*, and *Boat* and the encryption key (image) is *Mandrill*, while the inputs parameters are :

N = 256, BSIZE = 8, IORDER = 4 2 3 1 3 2 4 1 4 2 1 3

Table (1): Comparison results of test 1

Original image		Encrypted image				Reconstructed image		
Image name	**Image size (byte)**	**Image size (byte)**	**Time (sec.)**	**CR**	**Corr. with original**	**Image size (byte)**	**Corr. with original**	**Time (sec.)**
Lena	262144	65536	0.92	0.088	0.0064	262144	0.9976	0.79
Pepper	160000				0.0164	160000	0.9965	
Birds	250000				0.0017	250000	0.9995	
Boat	65536				0.0008	65536	0.9999	
	∑= 737680				Avg= 0.0063	∑= 737680	Avg= 0.9983	

- **Test 2**

The proposed technique was tested more than fifteen times, in each test different four *24-bit RGB* color images and key (image) were used. For color images with three RGB values per pixel, the current technique applied on each color (Red, Green, and Blue) as grayscale separately then combine the three resulted grayscale images to get the encrypted color image. The definition of (*Corr*) for RGB color image is the same except that the final *Corr* is equal to the sum of the *Corr* for each color divided by three as shown in the following equation (Al-Obaidi, 2004):

$$Corr_{RGB} = \frac{Corr_R + Corr_G + Corr_B}{3} \quad \ldots (7)$$

Where, $Corr_R$:correlation to *Red* color image.

$Corr_G$:correlation to *Green* color image. $Corr_B$:correlation to *Blue* color image.

The result of one of these tests is explain in Table (2), and all its images are shown in Figure (4). The original images are: *Map, Birds, Boys,* and *House* and the encryption key (image) is *Moth*, while the inputs parameters are:

N = 512, BSIZE =32 , IORDER = 2 4 1 3 4 3 2 1

Table (2): Comparison results of test 2

Original image		Encrypted image				Reconstructed image		
Image name	**Image size (byte)**	**Image size (byte)**	**Time (sec.)**	**CR**	**Corr. with original**	**Image size (byte)**	**Corr. with original**	**Time (sec.)**
Map	262144	262144	4.06	0.321	0.0103	262144	0.9993	3.73
Birds	177384				0.0195	177384	0.9999	
Boys	310000				0.0003	310000	0.9997	
House	65536				0.0065	65536	0.9999	
∑= 815064					Avg= 0.0091	∑= 815064		Avg=0.9997

- **Test 3**

The proposed technique is able to encrypted even a single image (a special case). In this case, the original image is resizing to the size 512×512 pixels and divided into four sub-images with size 256×256 pixels, which treated as input image. The proposed technique was tested more than fifteen times, in each test different one input *8-bit grayscale* or *24-bit color* image and key (image) were used. The result of one of these test for 8-bit grayscale image was listed in Table (3), and all its images are shown in Figure (5). The original image is *Cameraman*, and the encryption key (image) is *Woman*, while the inputs parameters are :

N = 256, BSIZE = 64, IORDER = 4 1 2 3

Table (3): Comparison results of test 3

Original image		Encrypted image				Reconstructed image		
Image name	**Image size (byte)**	**Image size (byte)**	**Time (sec.)**	**CR**	**Corr. with original**	**Image size (byte)**	**Corr. with origi nal**	**Time (sec.)**
Camer aman	33000 0	65536	0.65	0.198	0.0105	33000 0	0.999 9	0.34

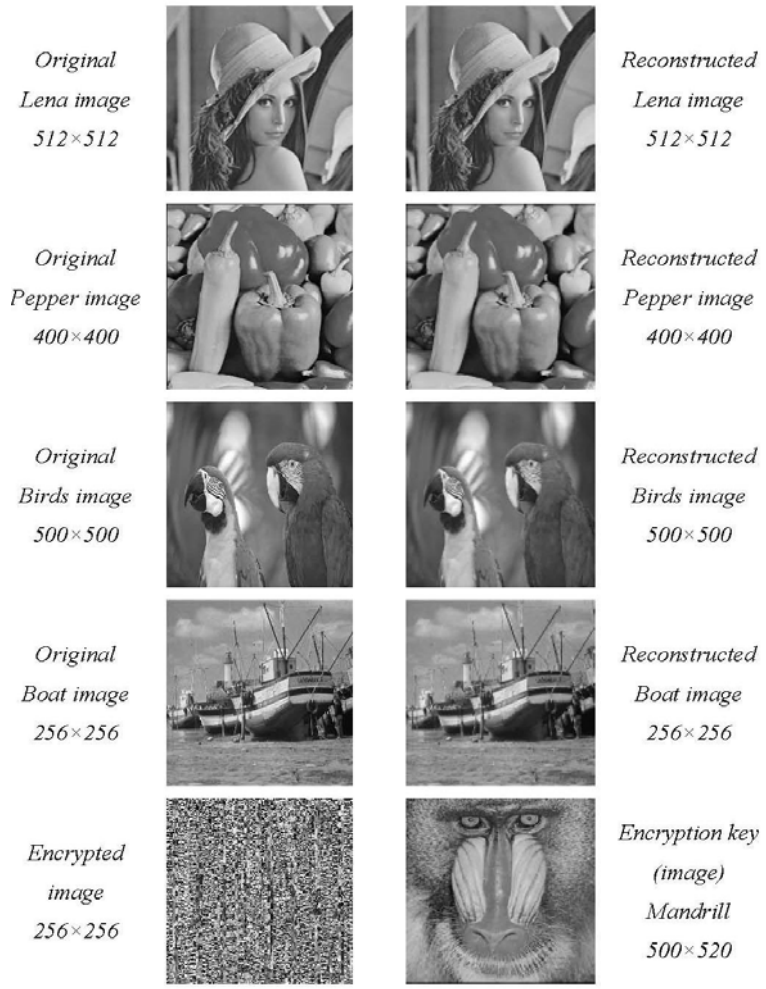

Figure (3): Images of the test 1

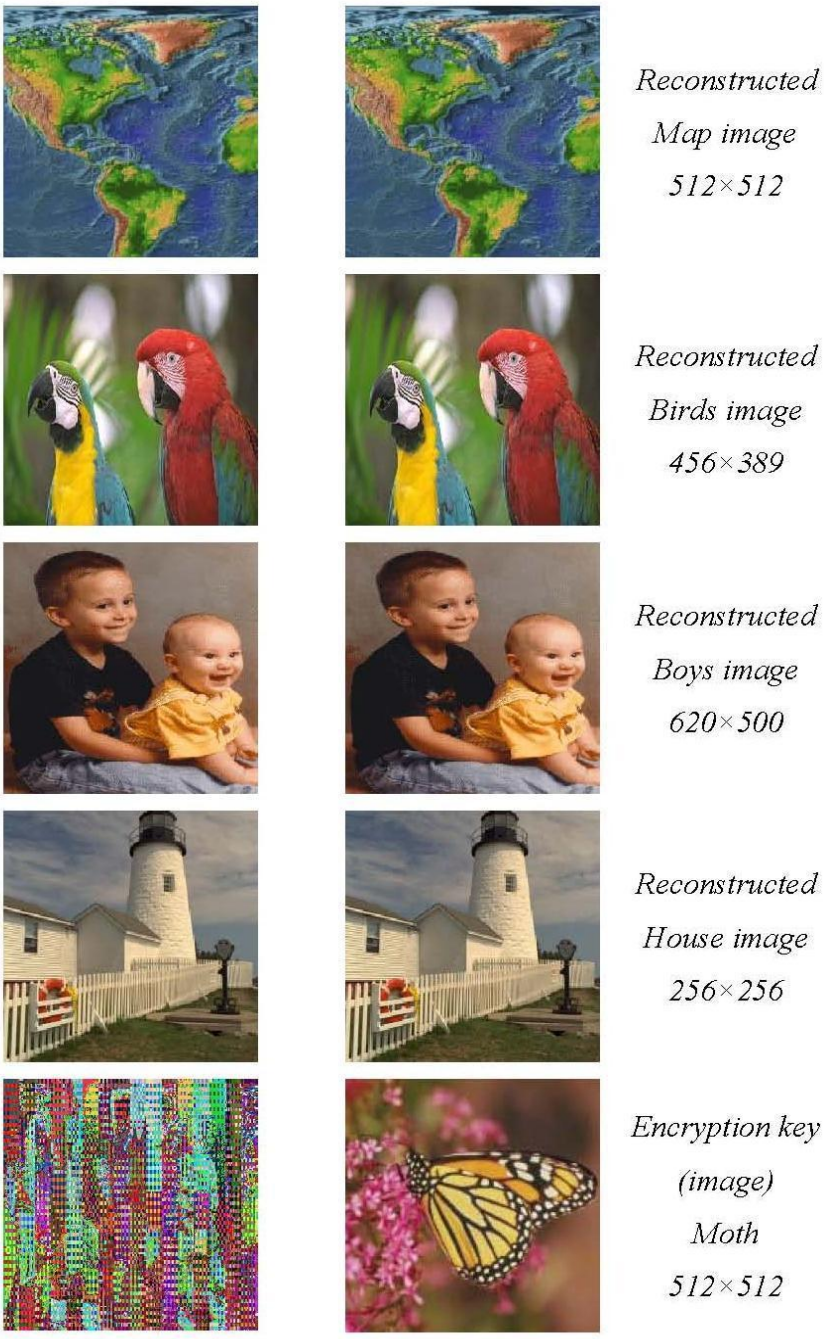

Figure (4): Images of test 2

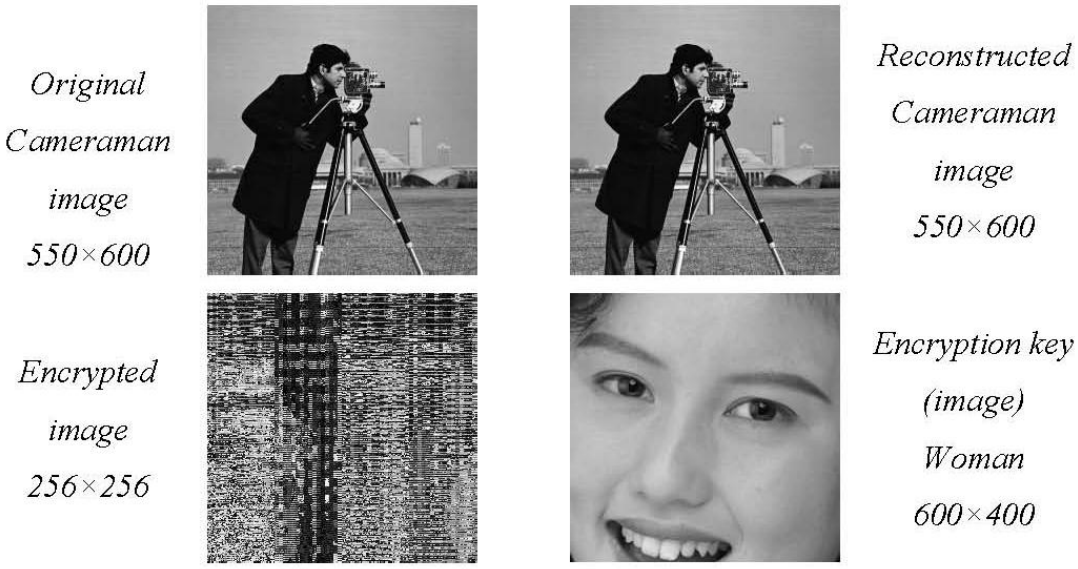

Figure (5): Images of test 3

6. Conclusions

This paper proposed a new technique which aims to encrypted four different images to produce a single image. The resulting image size is less than the sum of the sizes of the original images. This was accomplished by using wavelet transform

From the results, we can notice that the correlation between the original image and the reconstructed image is nearly equal to one for g*rayscale* and *color* images, while the correlation with the encrypted image is very small approximately to zero. This indicates that the encryption technique works well to protect the image data. In addition to, the size of resulted image is very small compared with the sum of the original images sizes. The reconstructed images approximately are the same as the original images.

The current technique has many advantages, such as, low storage requirements, low time requirement, and high security.

References

Al-Obaidi H. H.**,** (2004)**, *"Encryption Using Wavelet Coded Image Data",*** M.Sc. Thesis, Computer Engineering Department, College of Engineering, Basrah University.

Antonini M., Barlaud M, Daubechies I., (1992)**, *"Image Coding Using Wavelet Transform"***, IEEE Transactions on Image Processing, Vol. 1, No. 2, pp. 1716-1740.

Baxes G. A.**,** (1994)**, *"Digital Image Processing: Principles and Applications",*** John Wiley & Sons, Inc., USA.

Borie J., Puech W., Dumas M.**,** (2004)**, *"Crypto-Compression System for Secure Transfer of Medical Images",*** 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004).

Cheng H., Li X.**,** (2000)**, *"Partial Encryption of Compressed Images and Videos",*** IEEE Transaction Signal Processing, Vol. 48, No. 8, pp. 2439-2451.

Li S., Li C., Lo K.T., Chen G.**,** (2006)**, *"Cryptanalysis of an Image Encryption Schemes",*** Journal of Electronic Imaging.

Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A.**,** (2003)**, *"Confidential Storage and Transmission of Medical Image Data",*** Computers in Biology and Medicine 33, pp. 277-292.

Öztürk Ï, Sogukpinar Ï**,** (2004)**, *"Analysis and Comparison of Image Encryption Algorithms",*** IEEE Transactions on Engineering, Computing and Technology, Volume 3, ISSN 1305-5313.

Saha S.**,** (2001)**, *"Image Compression-From DCT to Wavelet: A Review",*** ACM Crossroads Student Magazine, The ACM's First Electronic Publication.

Usevitch B. E.**,** (2001)**, *"A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000",*** IEEE Transactions on Image Processing Magazine.

Varma K., Bell A.**,** (2004)**, *"JPEG2000-Choices and Tradeoffs For Encoders",*** IEEE Transactions on Image Processing Magazine.

Xiong Z., Ramchandran K., Orchard M. T., Zhang Y.**,** (1999)**, *"A Comparative Study of DCT and Wavelet-Based Image Coding",*** IEEE Transactions on Circuits and Systems for Video Technology, Vol. 9, No. 5.

Zenon, H., Voloshynovskiy, S., Rytsar, Y.,(1997), ***"Cryptography and Steganography of Video Information in Modern Communication"***, in *Third TELSIKS'97*, Yugoslavia, pp. 115-125.