Hiding Processing Approaches For Digital Images Encryption Using Wavelet Transform

Dr. Hameed A. Younis, Dr. Turki Y. Abdalla**, Dr. Abdulkareem Y. Abdalla **

**Dept. of Computer Science, College of Science, University of Basrah, Basrah, Iraq.*
***Dept. of Computer Engineering, College of Engineering, University of Basrah, Basrah, Iraq.*

Abstract

The use of image communication has increased in recent years. In this approach, the encryption process is performed by hiding the processing steps of the wavelet transform. The attacker cannot obtain the original image unless processing steps are known. In this paper, the performance of three different hidden wavelet-based schemes are applied. First, hiding filter types encryption scheme (HFT), second, hiding wavelet packet tree encryption scheme (HWPT), lastly, by combining the previous two methods (HFTWPT). Several experiments are given to illustrate the performance of the proposed schemes.

Keywords: Image, Wavelet transform, Wavelet packet transform, Encryption.

طرق إخفاء المعالجة لتشفير الصور الرقمية باستخدام التحويل المويجي

د. حميد عبد الكريم يونس*، د. تركي يونس عبد الله**، د. عبد الكريم يونس عبد الله*

*قسم علوم الحاسبات، كلية العلوم، جامعة البصرة، البصرة، العراق.

**قسم هندسة الحاسبات، كلية الهندسة، جامعة البصرة، البصرة، العراق.

المستخلص:

ازداد الاهتمام في اتصالات الصور في السنوات الأخيرة.في هذه الطريقة، أنجزت معالجة التشفير بواسطة إخفاء معالجة التحويل المويجي. المهاجم لا يستطيع الحصول على الصورة الأصلية ما لم يعرف خطوات المعالجة. في هذا البحث، طبقت ثلاث طرق إخفاء باستخدام التحويل المويجي. أولا، طريقة التشفير بإخفاء أنواع مرشحات التحليل، ثانيا، طريقة التشفير بإخفاء شجرة التحليل المويجي الحزمي، وأخيرا، طريقة التشفير بدمج الطريقتين السابقتين. طبقت العديد من التجارب على هذه التقنيات لحساب انجازيتها.

الكلمات المفتاحية: صورة، التحليل المويجي، التحليل المويجي الحزمي، التشفير.

1. Introduction

Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data, irrespective of the fact that the data is being transmitted over a medium or is stored on a storage device [1]. It provides a powerful means of verifying the authenticity of data and identifying the culprit, if the confidentiality and integrity of the data is violated. Because of the development of electronic commerce, cryptographic techniques are extremely critical to the development and use of defence information systems and communications networks.

Unlike text messages, image data have their special features such as bulk capacity, high redundancy, and high correlation among pixels. It is mentioned that they are usually huge which together make traditional encryption methods difficult to apply and slow to process [2].

The important of wavelet as a multiresolution technique comes from its decomposition of the image into multilevel of independent information with changing the scale like a geographical map in which the image has non-redundant information due to the changing of scale [3]. In this way every image will be transformed in each level of decomposition to a one low information image and three details in horizontal, vertical and diagonal axis image. Also, the low information image can be decomposed into another four images. These approaches of decomposition process provide us 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 [4].

In previous study, we have found some articles on image encryption: In 2002, Pommer et al [5] investigated the approach to encrypt just subband structure information of zerotree encoded wavelet packet data. In 2003, the same researchers [6] showed the ability of selective encryption to strike a balance between security and processing demands.

In this paper, several proposed encryption schemes will be presented. These approaches are wavelet based image encryption schemes by hiding the processing steps of the wavelet transform [7].

2. Wavelet Transform

The wavelets transform have two terms, each one is a set of functions takes the forms [8, 9]:

2. Wavelet Transform

The wavelets transform have two terms, each one is a set of functions takes the forms [8, 9]:

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

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

These sets of functions are formed by dilation and translation of a single function $\psi(x)$ is called the mother function or wavelet function in equation (1), and second function in equation (2), $\phi(x)$ is called the scale function, where g_k's and h_k's are analysis filters coefficients with h and g be the analysis filters [10-13]. Figure (1) shows the analysis and synthesis filters of a 2-D, 1-level of wavelet decomposition; where h and g are the synthesis filters. The upsampling process is indicated by $\uparrow 2$, and the downsampling process is indicated by $\downarrow 2$. 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 details); and, the high-high (HH) subband (the diagonal details).

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 [9]. The low-frequency content is the most important part. Since it 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 [14].

3. Wavelet Based Image Encryption Schemes by Hiding Processing Steps of The Wavelet Transform

In this approach, the encryption process is performed by hiding the processing steps of the wavelet transform [7]. The attacker can not obtain the original image unless knows processing steps. In this approach, two schemes were proposed. In the first scheme, the type of filters are selected randomly from a pool of filter types that contains a set of standard filters. The way of selection of filters is the key. In the second scheme, we

In the hiding filter type encryption scheme (HFT) on an image a choice of a set of filters out of a multitude of possible filters for the transformation step is made. Then usually, an index or a parameter to generate the filter, must be encrypted. The reason why this works up to a certain degree is that obviously different filters, filter different frequencies by a varying amount. When the filter for reconstruction is not known, the attacker has to guess randomly, the frequencies get a different weight and the reconstructed image looks distorted. The degree of distortion can vary from a non-observable distortion to a non-observable image. We use a set of filters [3, 9]. We put them into a pool of filters and randomly selecting one from them.

Generalised wavelet decompositions (where different filters are used at different decomposition levels) are employed in the encryption process and the information describing the structure of these decompositions is encrypted. The used wavelet filters are Haar filter, Daubechies wavelet filters family (db1, db2, db3, db5, db8), biorthogonal wavelet filters family (bior1.1, bior3.3, bior1.3, bior2.2 and bior3.5), coiflet wavelet filters family (coif1, coif2, coif3, coif4 and coif5) and symlet wavelet filters family (sym2, sym3, sym4 and sym5). The size of the keyspace (i.e., the size of the parameter space we use to describe the decompositions) then depends on the filter library (l = 19), the decomposition depth (n= 5), and using of generalised decomposition method, it is l^n keys. In the current implementation we choose the transform approach, during the encryption process the index of the filter in the library used at different decomposition levels is chosen randomly. When the correct filters are applied in the reconstruction process, smooth image data is generated, but when the filters are incorrect, distortion appear and the resulting image data is more noisy.

In this scheme, it is also suggested to improve the performance by allowing the decomposition depth to be also secret. Here we may take any number of levels. During this technique, the number of levels is chosen randomly (i.e., 1-level, 2-level,.....). The size of the keyspace will be $\sum_{i=1}^{no.of\ levels(n)} l^i$, and the resistance against attacks will be increased.

3.2 Hiding Wavelet Packet Tree Encryption Scheme (HWPT)

In this scheme, wavelet packet tree based encryption approach is performed. The tree can be generated completely random. To decide the decompositions, it is also possible to use a best-basis algorithm [6] as a first step and make random alterations to it. Using a decomposition tree generated by the best-basis algorithm, the attacker cannot obtain the original image unless he know the tree structure. The subband tree carrying the

3.2 Hiding Wavelet Packet Tree Encryption Scheme (HWPT)

In this scheme, wavelet packet tree based encryption approach is performed. The tree can be generated completely random. To decide the decompositions, it is also possible to use a best-basis algorithm [6] as a first step and make random alterations to it. Using a decomposition tree generated by the best-basis algorithm, the attacker cannot obtain the original image unless he know the tree structure. The subband tree carrying the subband structure information of the data is secured for transmission. The size of the keyspace is $2^{2^{2n}}$, where n-level decomposition. Figure (2) shows the tree decomposition structure.

3.3 Hiding Filter Types and Wavelet Packet Tree Encryption Scheme (HFTWPT)

The HFTWPT scheme is an attempt to hide both types filters and packet tree structure. The packet tree structure is generated randomly with several randomly selected filters. The tree can be generated completely random, to decide the decompositions. Hiding filter type encryption scheme on an image a choice of a set of filters out of a multitude of possible filters for the transformation step is made. Then the choice of the filter, usually an index or a parameter to generate the filter, must be encrypted. The attacker cannot obtain the original image unless he know the tree structure and the types of filters.

The security of this method depends on the structure of tree and the number and types and sequence of filters. The size of the keyspace is $(2^{2^{2n}})^{\sum_{i=1}^{levels(n)} no.of\ l^i}$.

4. Experimental Results

In this section, a number of experiments are used to examine our proposed wavelet based image encryption algorithms are presented. The algorithms are programmed in MATLAB version 6.5 on a Pentium IV PC (2.4 GHz) using four grayscale images of (256×256) pixels.

To evaluate each of the proposed wavelet based image encryption schemes, three aspects are examined [15, 16]:

1. **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 [17]:

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad \ldots(3)$$

Where:

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

3. **Histograms of encrypted images.** Select several 256 gray-level images with size of 256×256 that have different contents, to calculate their histograms. One can see that the histogram of the cipher-image is significantly uniform and different from that of the original image.

In this work, three experiments are presented. These experiments run with hidden filters, hidden wavelet packet tree, and hidden both filters and wavelet packet tree

Experiment 1

In this experiment, the hidden filter types encryption scheme are used to encrypt an image. The filter type for each level is selected randomly from a pool of filters. Here 19 filter types were selected. They are Haar, db2, db3, db5, bior1.1, bior3.3, coif1, coif3, db1, coif4, coif5, bior1.3, bior2.2, bior3.5, sym3, sym2, sym4, sym5 and db8 when 5 levels are applied. The size of the keyspace is $\sum_{i=1}^{5} 19^i$. During this experiment, the sym5, bior3.5, bior2.2, db8 and coif4 are used (selected randomly from the pool). Table (1) presents results of this experiment. Figure (3) shows the result obtained for Lena image. Four different images (Lena, house, birds and boys) were examined.

In Table (1), the first column gives the images. The second column gives the correlation of the cipher-image with the original image. Lastly, the third column gives the correlation of the reconstructed-image with the original image. Figure (4) shows histogram of the cipher-image and the original image.

Experiment 2

In this experiment, HWPT is considered. The special case of wavelet packet tree structure is shown in Figure (2). The packet tree structure is chosen randomly and keep secret (encryption key).

Table (2) shows the results for the images. Figure (5) shows the result obtained for Lena image. The encryption key is the wavelet packet tree structure. The size of the keyspace is $2^{2^{2(5)}}$, here the number of levels $n = 5$. Figure (6) shows histogram of the cipher-image and the original image.

Experiment 3

The HFTWPT scheme is an attempt to hide both filters and packet tree structure. The packet tree structure is generated randomly with several randomly selected filters.

The security of this method depends on the structure of the tree and the number and types and sequence of filters. During this experiment, the sym5, bior3.5, bior2.2,

randomly and keep secret (encryption key).

Table (2) shows the results for the images. Figure (5) shows the result obtained for Lena image. The encryption key is the wavelet packet tree structure. The size of the keyspace is $2^{2^{2(5)}}$, here the number of levels $n = 5$. Figure (6) shows histogram of the cipher-image and the original image.

Experiment 3

The HFTWPT scheme is an attempt to hide both filters and packet tree structure. The packet tree structure is generated randomly with several randomly selected filters.

The security of this method depends on the structure of the tree and the number and types and sequence of filters. During this experiment, the sym5, bior3.5, bior2.2, db8 and coif4 are used, when 5 levels are applied. The size of the keyspace is $(2^{2^{2(5)}})\sum_{i=1}^{5}19^i$. Table (3) presents results of this experiment. Figure (7) shows the result obtained for Lena image.. Figure (8) shows histogram of the cipher-image and the original image.

5. Conclusion

Out of the results, one can see that the correlation between the original image and the reconstructed-image is nearly equal to one, while the correlation with the cipher-image is nearly equal to zero (in case L_1). This indicates that the encryption scheme works well to protect the image data. The reconstructed-images are the same as the original images.

In experiment 1, the attacker cannot obtain the original image unless he knows the type of filters, the number of analysis levels and the sequence of filters.

From experiment 2, we conclude that the attacker cannot obtain the original image unless he knows the tree structure. Besides this in experiment 3, the attacker cannot obtain the original image unless he knows the type of filters, the number of analysis levels and the sequence of filters, and the tree structure.

In Figures (4, 6, and 8), one can see that the histogram of the cipher-image is significantly different from that of the original image. By this difference between the two histograms, the positions and the values of the pixels of original image are rearranged with the user key. As a result, the cipher-image is able to reach good properties of confusion and to protect the image data from unauthorized access. The method used in experiment 3 has more security since the keyspace is very large (2^{128}).

Visual Data", ACM Multimedia System Journal, pp. 67-70, 2002.

[6] **Pommer A.,and Uhl A.,** ***"Selective Encryption of Wavelet-packet Encoded Image Data-Efficiency and Security"***, ACM Multimedia Systems Journal, 9 (3), pp. 279-287, 2003.

[7] **Younis, H. A.,** ***"New Techniques For Partial Encryption of Wavelet-based Compressed and Uncompressed Images"***, Ph.D. Thesis, Department of Computer Science, College of Science, University of Basrah, Basrah, November 2006.

[8] **Antonini M., Barlaud M,and Daubechies I.,** ***"Image Coding Using Wavelet Transform"***, IEEE Transactions on Image Processing, Vol. 1, No. 2, pp. 1716-1740, April 1992.

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

[10] **Gonzalez R.C.,and Woods R. E.,** ***"Digital Image Processing"*** ,Addision-Wesley, Inc., USA, 1992.

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

[12] **Tang L.,** ***"Methods for Encryption and Decryption MPEG Video Data Efficiently"***, Proceedings of the Fourth ACM International Conference on Multimedia, pp. 219-229, 1997.

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

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

[15] **Li S., Li C., Lo K.T.,and Chen G.,** ***"Cryptanalysis of an Image Encryption Schemes"***, Journal of Electronic Imaging, 2006.

[16] **Öztürk İ,and Sogukpinar İ,** ***"Analysis and Comparison of Image Encryption Algorithms"***, IEEE Transactions on Engineering, Computing and Technology, Volume 3, ISSN 1305-5313, December 2004.

[17] **Al-obaidi H. H.,** ***"Encryption Using Wavelet Coded Image Data"***, M.Sc. Thesis, Computer Engineering Department, College of Engineering, Basrah University, June 2004.

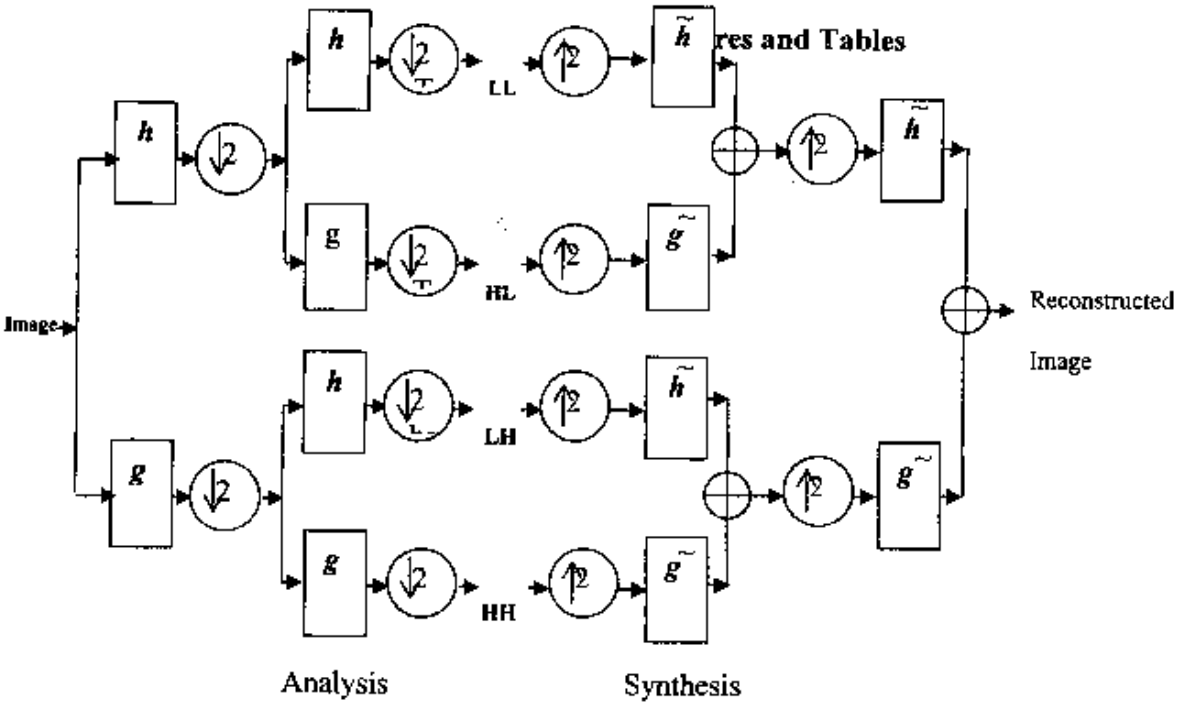


Figure (1) The analysis and synthesis of 2-D, 1-level discrete wavelet decomposition where ↑2 and ↓2 denotes upsampling and downsampling, respectively.

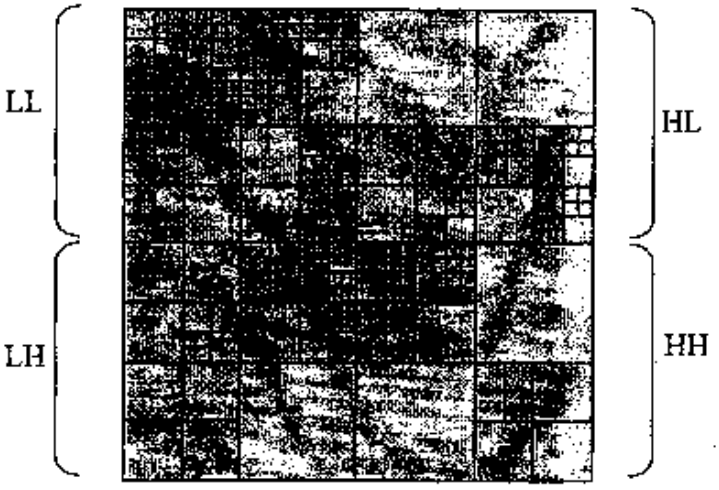


Figure (2): Decomposition tree for random wavelet packet structure .

(a) (b) (c)

Figure (3): Results of experiment 1 using hidden filter type encryption scheme
(a) Original Lena image.
(b) Image resulting from encryption.
(c) Reconstructed image.

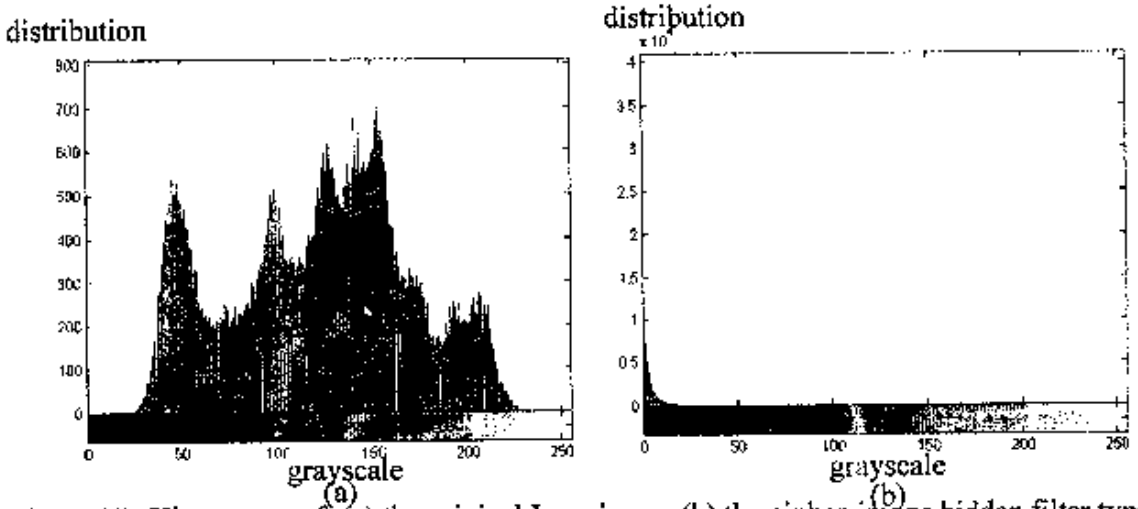
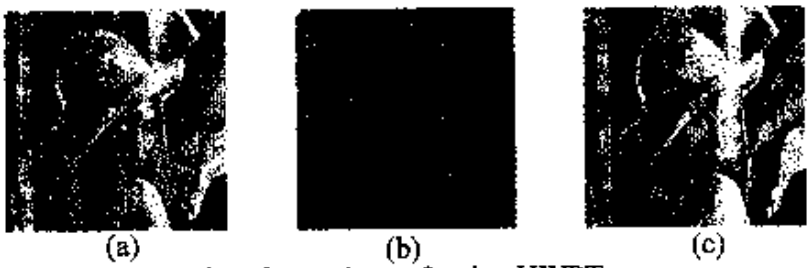


Figure (4): Histograms of (a) the original Lena image (b) the cipher-image hidden filter type encryption scheme.



(a) (b) (c)

Figure (5): Results of experiment 2 using HWPT
(a) Original Lena image.
(b) Image resulting from encryption.
(c) Reconstructed image.

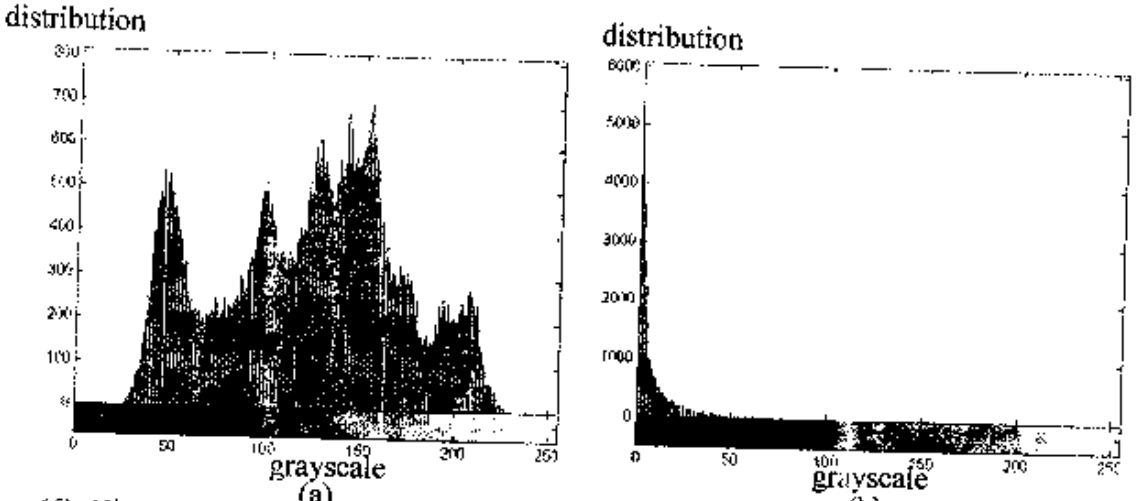


Figure (6): Histograms of (a) the original Lena image (b) the cipher-image using HWPT

Figure (7): Results of experiment 3 using HFTWPT
(a) Original Lena image.
(b) Image resulting from encryption.
(c) Reconstructed image.

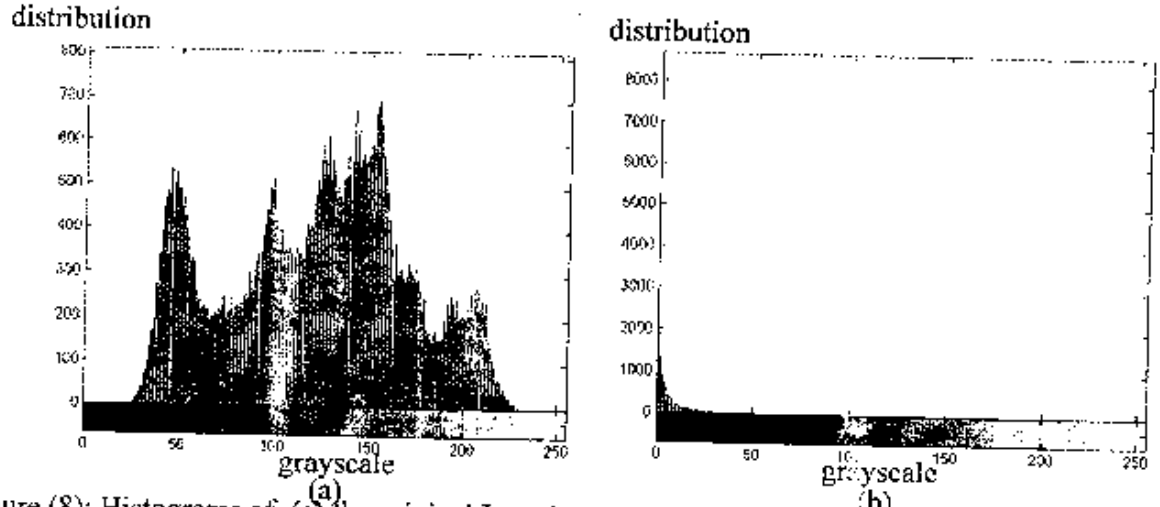


Figure (8): Histograms of (a) the original Lena image (b) the cipher-image using HFTWPT

Table (1): Results for images using hidden filter type scheme

Image	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Lena	0.0208	0.9792
House	0.0210	0.9790
Birds	0.0162	0.9838
Boys	0.0012	0.9988
Average	0.0148	0.9852

Table (2): Results for images using HWPT

Image	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Lena	0.0103	0.9897
House	0.0108	0.9892
Birds	0.0054	0.9946
Boys	0.0004	0.9995
Average	0.0067	0.9933

Table (3): Results for images using HFTWPT

Image	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Lena	0.0098	0.9902
House	0.0074	0.9926
Birds	0.0016	0.9984
Boys	0.0016	0.9984
Average	0.0051	0.9949