Fast Techniques For Partial Encryption of Wavelet-based Digital Images

Hameed A. Younis*, Turki Y. Abdalla, 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 paper, new partial encryption schemes are used to encrypt only part of the data. Only 6.25-25% of the original data is encrypted for four different images, resulting in a significant reduction in encryption and decryption time. In the encryption step, the Advanced Encryption Standard (AES) cipher, stream cipher and permutation cipher are used. On the other hand, we will use a combination of two encryption methods may be used to achieve high security and make brute fore attack infeasible. The effect of size of encrypted data on performance of the proposed techniques are studied. The proposed partial encryption schemes are fast and secure.

Keywords: Image, Encryption, AES cipher, Stream cipher, Wavelet transform

قنيات سريعة للتشفير الجزئي معتمدة على التحويل المويجي للصور الرقمية

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 هذا البحث، اقترحـت طرقـا للتشفير الجزئي الجديدة، والتي فيها تقوم خوارزمية التشفير بتشفير جزء مـن البيانـات. وشـفر بحدود (6.25-25%) من البيانات الأصلية المستخدمة (أربع صور مختلفة) للحصول على تقليل مهم في زمن التشفير وفك الشفرة. في مرحلة التشفير، استخدمت طرق تشفير متقدمة مثل التشفير القياسي المتقدم (AES) والتشفير الانسيابي (Stream cipher). من ناحية أخـرى، اسـتخدمنا تجميع طريقتي تشفير لإنجاز سرعة عالية وجعل هجوم القوة المعادية مسـتحيل. درسـت تـأثير اجزاء بيانات مختلفة على انجازية التقنيات المقترحة. أنظمة التشفير المقترحـة تكـون سـريعة وسرية.

الكلمات المفتاحية: صورة، التشفير، التشفير القياسي المتقدم (AES)، التشفير الانسيابي، التحليل المويجي.

1. Introductio*n*

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 [Ş̲chneier B., 1996]. 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, not to mention that they usually are huge which together make traditional encryption methods difficult to apply and slow to process [Borie J., Puech W., Dumas M., 2004].

The important of wavelet as a multiresolution 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 K., Bell A., 2004]. 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 decompositio[Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A., 2003].

Partial encryption is a secure encryption algorithm which is used to encrypt only part of the data [Cheng H., 1998]. It is used to reduce encryption and decryption time.

These algorithms all have important part that provides a significant amount of information about the original data [Cheng H., Li X., 2000]. The remaining parts may not provide much information without the important ones. If this is the case, the remaining are called the unimportant parts. For simplicity, we consider all important parts as one important part. The remaining parts are grouped into one unimportant part, provided that it does not provide significant information about the original data.

In previous study, we have found some articles on image encryption: In 2000, Cheng H., Li X. [Cheng H., Li X., 2000] proposed a solution called partial encryption, in which a secure

encryption algorithm is used to encrypt only part of the compressed data. In 2003, Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A. [Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A., 2003] discuss computationally effect techniques for confidential storage and transmission of medical image data. Two types of partial encryption techniques based on AES are proposed.

In this paper, several proposed encryption schemes will be presented [Younis H. A., 2006]. These approaches are wavelet based image partial encryption schemes using a well-known encryption algorithms.

2. Basic Principles

n 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

2.1 Wavelet Transform

The wavelets transform have two terms, each one is a set of functions takes the forms [Antonini M., Barlaud M., Daubechies I., 1992, Baxes G. A., 1994]:

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

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

These sets of functions are formed by dilation and translation of a single function $\psi(x)$, called as the mother function or wavelet function in equation (1).The 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 [Gonzalez R. C., Woods R. E., 1992, Saha S., 2001, Tang L., 1997, Xiong Z., Ramchandran K., Orchard M. T., Zhang Y., 1999]. In general, 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 [10]. 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 B. E., 2001].

2.2 Permutation Cipher

In this system, the position of the plaintext letters in the massage rather than the letters of alphabet are permuted, while the permutation is the key. For the digital image the position of pixels are rearranged for different algorithms according to a key, such as image reversal, row transposition, column transposition, and block or matrix transposition [Al-obaidi H. H., 2004, Stallings W. 2003].

2.3 Stream Cipher

Stream ciphers convert plaintext to ciphertext one bit a time [Schneier B., 1996]. A keystream generator (sometimes called a *running-key generator*) outputs a stream of bits: K_1, K_2, K_3,……,K_i. This keystream is XORed with a stream of plaintext bits, P_1, P_2, P_3,….,P_i to produce the stream of ciphertext bits C_1, C_2,……C_i.

$$C_i = P_i \oplus K_i \qquad \ldots(3)$$

2.4 Advanced Encryption Standard (AES) Cipher

The AES cipher described by Rijndael (called also *Rijndael encryption algorithm*) [Stallings W. 2003], it is a block cipher that converts cleartext data blocks of 128, 192, or 256 bits into ciphertext blocks of the same length. The AES cipher uses a key of selectable length (128, 192, or 256 bits). This encryption algorithm is organized as a set of iterations called *round transformations*. In each round, a data block is transformed by series of operations. The total number of rounds depends on the largest of round *r* and key length kl, and equals 10, 12, and 14 for lengths of 128, 192, and 256 bits, respectively. All round transformations are identical, apart from the final one. The AES algorithm takes the cipher

key, and performs a key expansion routine to generate a key schedule. For number of round = 10 and key length = 128 bits, the key expansion generates a total of 44 words. The resulting key schedule consists of a linear array of 4-byte words, denoted by [wi], with i in the range $0 \leq i < 44$.

3. Partial Encryption Scheme of Image Using Wavelet Transform

3.1 Hiding Filter Types Encryption Scheme

In this approach, some of the well-known encryption algorithms are used, such as AES cipher, Stream cipher, Chaotic cipher and Permutation cipher to partially encrypt images.

The basic idea behind wavelet coding is very simple: when looking at images and their distributions of frequencies, it can be seen that the most energy (information) lies in the lower frequency bands. One can utilise this by dividing an image into two parts: a low-frequency part and a high-frequency part using appropriate low- and high-pass filters [Varma K., Bell A., 2004].

After this frequency separation the important low-frequency part can be coded and the high-frequency part can be thrown away, or coded at a lower bit rate [Pommer A., Uhl A., 2003]. Because an image is a two-dimensional object, this partitioning has to be performed in both directions resulting in 4 subbands; they are labelled LL, HL, LH, HH, one subband which is low-pass filtered in both directions, two subbands which are mixed low-and high-pass filtered and one high-pass filtered subband. This low- and high-pass filtering concentrates the energy: most energy is contained in the LL-subband, it contains a small-scale version of the original image. The other three subbands contain just edge information and almost no energy. It is desirable to concentrate that energy even further, and it is possible because of the underlying multiresolution analysis theory. In practice this is usually repeated n times, and it is repeated just on the LL-subband. After the transformation of the image into distinct subbands the most important part will be encrypted.

In partial encryption, only part of image (i.e., L_1, L_2 or L_3 subband image) (important part) is encrypted whereas the remaining part (unimportant part) is transmitted without encryption. To investigate the performance of such partial encryption scheme, several encryption methods will be proposed to be used and their results will be compared.

Wavelet–PE Algorithm:

1. Encryption key selection.
2. Wavelet filter selection.
3. Decomposition (filtering) the image, here discrete wavelet transform (1, 2 or 3 levels) is used.
4. Partial encryption.

The important part may be encrypted by using one of the following ciphers:

- AES cipher (AES-PE).
- Stream cipher (Stream-PE).

Also, a combination of two encryption methods may be used to achieve high security and to make the brute force attack infeasible. The Stream cipher and, Permutation cipher (Stream-Permutation-PE) proposed:

In this work, to hide the details of the cipher image and increase the security further. We suggest to use the *smoothing process*. The smoothed ciphered image does not give any suspensions about the secret images. Smoothing process is obtained by finding the difference operation between each neighbouring two pixels both row and column directions. The smoothing process will start in row direction, which means each element (pixel) except the first pixel is determined by finding the difference operation between each two neighbouring pixels in the same row but in the different columns. For example, the second element of the first level-smoothed image will be found by subtracting the first element of the transformed image from its second element, while the first element of the first level-smoothed image in the second row will be found by subtracting the last element of the transformed image in the first row from its first element in the second row. This process continues until all pixels of first level-smoothed image are determined. The second level-smoothed image (column direction) is started by finding the difference operation between each two neighbouring pixels of the first level-smoothed image in the same column but different rows. For example, the second element of the second level-smoothed image will be found by subtracting the first element of the first level-smoothed image from its second element, while the first element of the second level-smoothed image in the second column will be found by subtracting the last element of the level-smoothed image in the first column from its first element in the second column. Also, this process is done to all the elements in the first level-smoothed image.

4. Experimental Results

In this section, a number of experiments which are used to examine our proposed wavelet based image encryption algorithms will be presented. The algorithms were 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 [Li S., Li C., Lo K. T., Chen G., 2006, Öztürk Ï, Sogukpinar Ï., 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 many advanced algorithms are adopted, such as AES, and Stream ciphers that make them difficult to cryptanalyze.
2. **Speed**. Less data (important part) to encrypt means less CPU time required for encryption. So, in general partial encryption algorithms are used to reduce encryption and decryption time.
3. **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 H. H., 2004]:

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

…(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:

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

. . . (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:

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

. . . (6),

where:

M: height of the image.

N: width of the image.

r and c: row and column numbers.

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.
5. **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, several experiments on the proposed partial encryption schemes are done. Different cases were considered.

Experiment 1

In this experiment, different proposed methods for partial encryption of images will be presented. Four different parts of images are chosen for this experiment, which are full, L_1, L_2 or L_3:

a) AES-PE:

In this method, AES partial encryption scheme is considered. Results obtained by applying partial encryption of image using AES encryption algorithm are presented in Table (1). Figure (1) shows the results obtained for Lena image.

In Table (1), the first column gives the amount of encrypted part of images. The second column gives the correlation of the cipher-image with the original image. The third column gives the correlation of the reconstructed-image with the original image.

The encryption key is "2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c". An amount 100%, 25%, 6.25% or 1.5625% of the original data are encrypted for the four different images. The size of the keyspace is 2^{128}. Figure (2) shows histograms of the original Lena images and the cipher-images.

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0012	0.999894
L_1	0.0208	0.999918
L_2	0.0633	0.999976
L_3	0.1391	0.999983

(a)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0053	0.999913
L_1	0.0374	0.999934
L_2	0.1174	0.999951
L_3	0.1592	0.999967

(b)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0019	0.999909
L_1	0.0119	0.999925
L_2	0.0434	0.999979
L_3	0.1051	0.999987

(c)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0006	0.999847
L_1	0.0148	0.999902
L_2	0.0558	0.999927
L_3	0.0644	0.999975

(d)

Table (1): Results of encryption of different amounts for images using AES-PE
(a) Lena (b) House (c) Birds (d) Boys

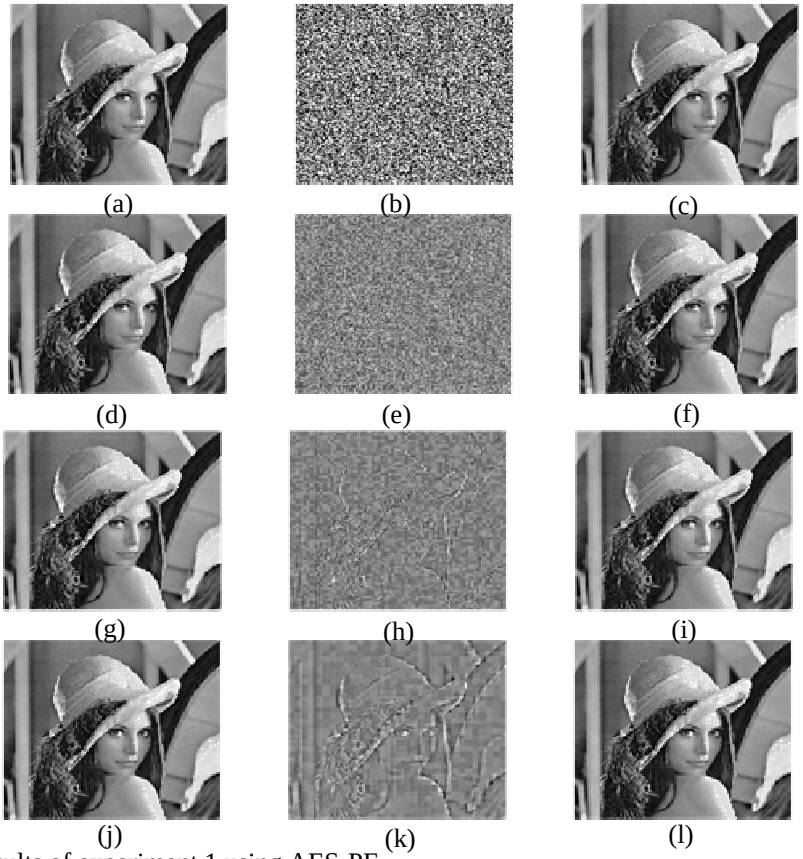
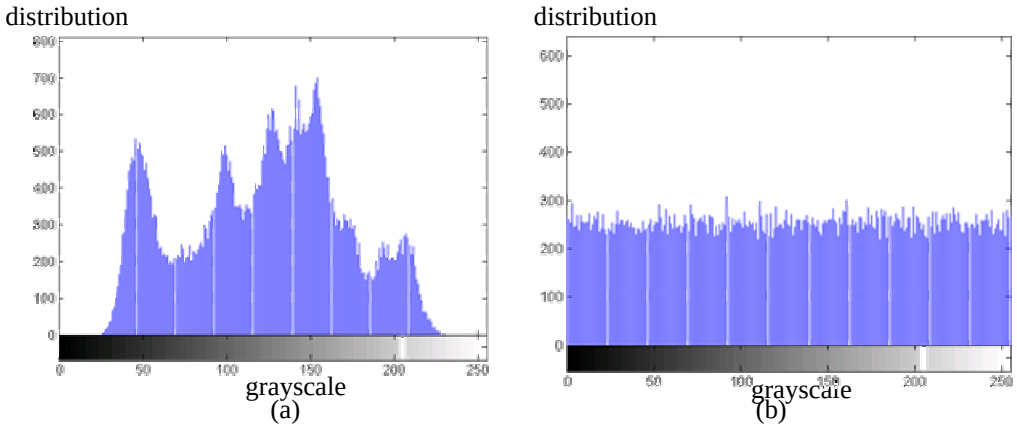


Figure (1): Results of experiment 1 using AES-PE

(a), (d), (g), (j) Original Lena image.

(b), (e), (h), (k) Image resulting from encryption with full, L_1, L_2 or L_3 size, respectively.

(c), (f), (i), (l) Reconstructed image in each case.



(a) (b)

Continued

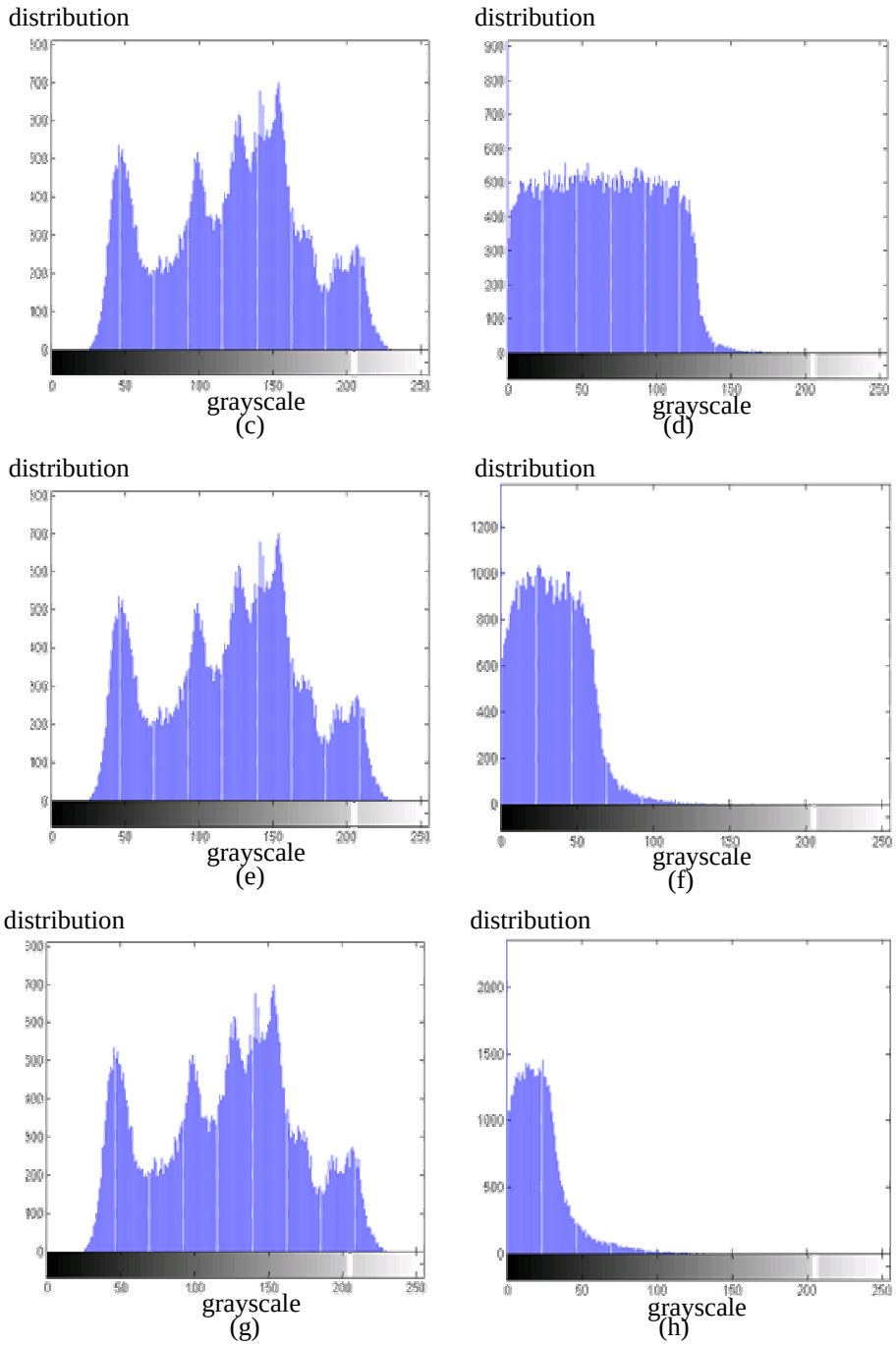


Figure (2): Histograms of experiment 1 using AES-PE
(a), (c), (e), (g) the original Lena image.
(b), (d), (f), (h) the cipher-image with full, L_1, L_2, or L_3 size, respectively.

b) Stream-PE:

In this method, Stream partial encryption scheme is considered. Results obtained by applying Stream partial encryption to the image after wavelet transform operation are presented in Table (2). Figure (3) shows the results obtained for Lena image.

The encryption key is "initial state 01100001, feedback function 00010101". In this case, 100%, 25%, 6.25% or 1.5625% of the original data size are encrypted for different images. The size of the keyspace is 2^{16}. Figure (4) shows histogram of the original Lena image and the cipher-image when the size of the encryption part is 25%.

In this scheme, it is also suggested to improve the performance by performing smoothing process explained in section (3.1) to the final encrypted data. Figure (5) shows the result for Lena image with smoothing process (size L_1). Figure (6) shows histograms of after smoothing process.

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0037	0.999884
L_1	0.0616	0.999918
L_2	0.2307	0.999986
L_3	0.4491	0.999989

(a)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0044	0.999916
L_1	0.0831	0.999932
L_2	0.2713	0.999939
L_3	0.4725	0.999948

(b)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.001	0.999904
L_1	0.067	0.999949
L_2	0.182	0.999951
L_3	0.330	0.999984

(c)

Amount	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Full	0.0012	0.999870
L_1	0.0210	0.999956
L_2	0.1228	0.999978
L_3	0.2739	0.999980

(d)

Table (2): Results of encryption of different amounts for images using Stream-PE
(a) Lena (b) House (c) Birds (d) Boys

Figure (3): Results of experiment 1 using Stream-PE

(a), (d), (g), (j) Original Lena image.

(b), (e), (h), (k) Image resulting from encryption with full, L_1, L_2 or L_3 size, respectively.

(c), (f), (i), (l) Reconstructed image in each case.

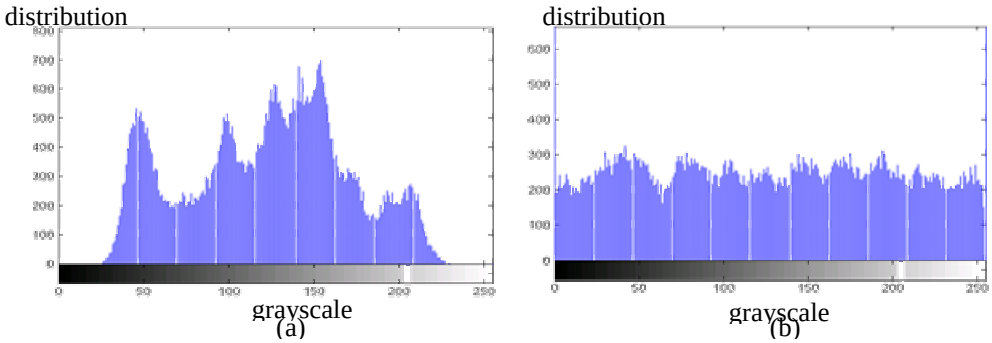
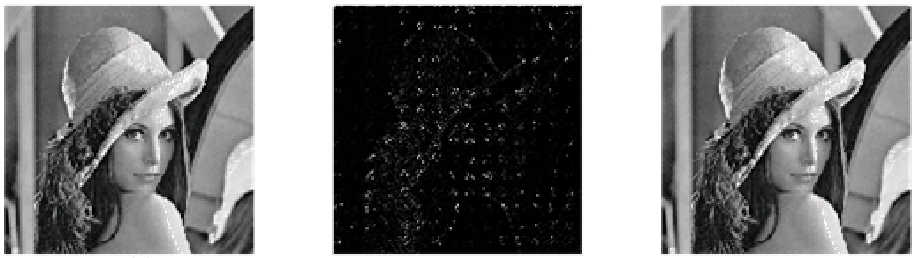
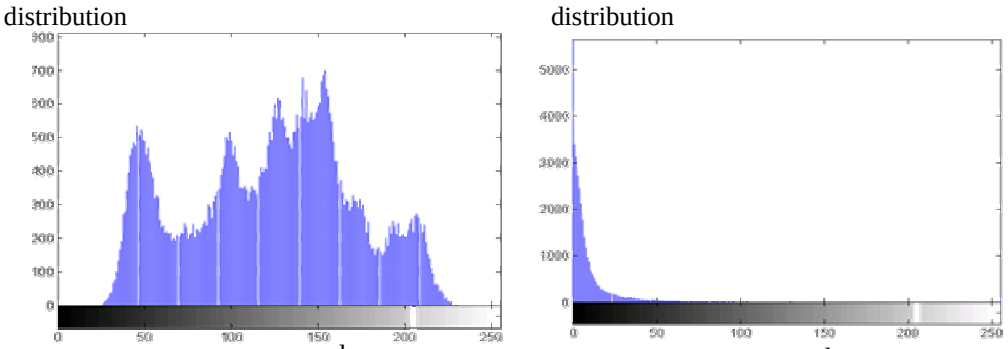


Figure (4): Histograms of (a) the original Lena image (b) the cipher-image using Stream-PE (size L_1)



(a) (b) (c)

Figure (5): Results of experiment 1 using Stream-PE after smoothing process
(a) Original Lena image.
(b) Image resulting from encryption.
(c) Reconstructed image.



(a) (b)

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

Experiment 2

In this experiment, we will use a combination of two encryption methods to encrypt the important part of the image (L_1) to achieve high security and to make the brute force attack infeasible.

Stream-Permutation-PE:

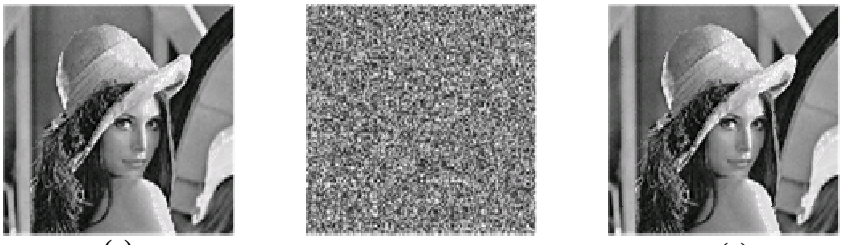
Stream-Permutation-PE consists of two phases: Stream cipher and Permutation cipher. Results obtained by applying partial encryption to the image after wavelet transform operation are presented in Table (3) for four test images. Figure (7) shows results obtained for Lena image.

The encryption key is "initial state 01100001, feedback function 00010101" and positions of 16409 pixels randomly generated for Permutation cipher. 25% of the data is

encrypted for the used images. The size of the keyspace is $(2^{16})(16409!)$. Figure (8) shows histograms of the cipher-image and the original image.

Image	Cipher-image Correlation (Corr)	Reconstructed-image Correlation (Corr)
Lena	0.0032	0.99961
House	0.0043	0.99956
Birds	0.0021	0.99967
Boys	0.0028	0.99903
Average	0.0031	0.99946

Table (3): Results for images using Stream-Permutation-PE



(a) (b) (c)

Figure (7): Results of experiment 2 using Stream-Permutation-PE
(a) Original Lena image.
(b) Image resulting from encryption.
(c) Reconstructed 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 indicate that the encryption scheme works well to protect the image data. The reconstructed-images are the same as the original images.

From out of the results of experiment 1, one can see that as the amount of the encrypted part is decreased, the execution time is decreased too, but as the amount of the encrypted part is decreased, the correlation of the cipher-image with the original image is increased. Figure (9) shows these facts.

Results of experiment 2 show that the correlation between the cipher-image and the original image is very small when two different ciphers are combined. The security of the

resulted image will be bigger and that will increase the robustness of this combination against attacks through ciphers but it takes more time.

On the other hand, in Figures (2 and 4), one can note that AES-PE method is better than that of stream-PE method since the histogram in them are largely different. This high difference led cipher very to be strong (good properties of confusion).

In Figure (2), the method AES-PE has more secrecy than the another method because the histogram is highly uniformed and different from that of the other methods and makes the brute force attack infeasible. This is also because the correlation of the cipher-image with the original image is very low but the time is long.

As shown in Figure (2), the histogram for the case of full encryption is more uniformed than other sizes, this means that security is higher. Also, the histogram for the case of 25% encryption is better than the other smaller sizes.

In Figure (6), it is noticed that performing smoothing process after encryption add more security to the resulting image because the big difference between the two histograms with and without performing this process indicates that the confidentiality and robustness against attacks to break the images are strong (the correlation is very low). The encryption of L_1-subband is a suitable choice because the correlation value of the cipher-image with the original image is very low with suitable execution time.

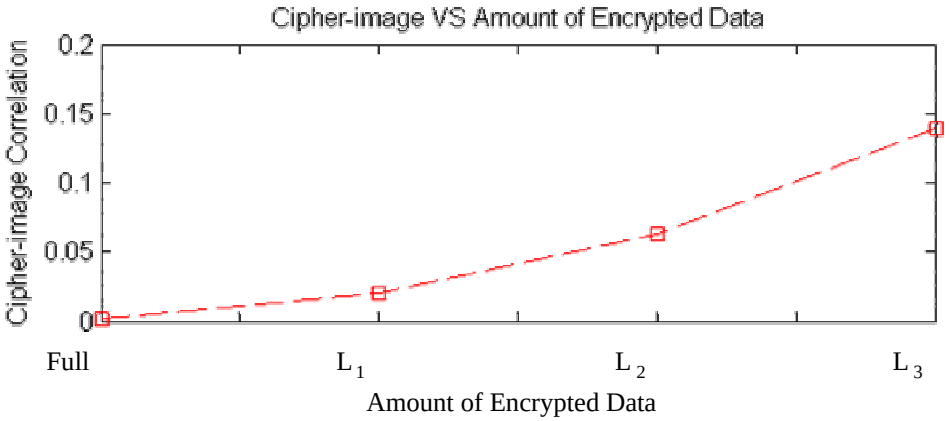


Figure (9): Cipher-image correlation versus amount of encrypted data for Lena image using AES-PE

References

[1] **Schneier B.,**

"Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C", John Wiley & Sons, Inc., USA, 1996.

[2] **Borie J., Puech W., Dumas M.,**

"Crypto-Compression System for Secure Transfer of Medical Images", 2nd International Conference on Advances in Medical Signal and Information Processing (MEDSIP 2004), September 2004.

[3] **Varma K., Bell A.,**

"JPEG2000-Choices and Tradeoffs For Encoders", IEEE Transactions on Image Processing Magazine, November 2004.

[4] **Norcen R., Podesser M., Pommer A., Schmidt H., Uhl A.,**

"Confidential Storage and Transmission of Medical Image Data", Computers in Biology and Medicine 33, pp. 277-292, 2003.

[5] **Cheng H.,**

"Partial Encryption for Image and Video Communication", M.Sc. Thesis, Department of Computing Science, University of Alberta, Alberta, 1998.

[6] **Cheng H., Li X.,**

"Partial Encryption of Compressed Images and Videos", IEEE Transaction Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000.

[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, 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., 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., 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] **Al-obaidi H. H.,**

"***Encryption Using Wavelet Coded Image Data",*** M.Sc. Thesis, Computer Engineering Department, College of Engineering, Basrah University, June 2004.

[16] **Stallings W.,**

"Cryptography and Network Security, Principles and Practice", Third Edition, Pearson Education International, Inc., USA, 2003.

[17] **Pommer A., Uhl A.,**

"Selective Encryption of Wavelet-packet Encoded Image Data- Efficiency and Security", ACM Multimedia Systems Journal, 9 (3), pp. 279-287, 2003.

[18] **Li S., Li C., Lo K.T., Chen G.,**

"Cryptanalysis of an Image Encryption Schemes", Journal of Electronic Imaging, 2006.

[19] **Öztürk İ, Sogukpinar İ,**

"Analysis and Comparison of Image Encryption Algorithms", IEEE Transactions on Engineering, Computing and Technology, Volume 3, ISSN 1305-5313, December 2004.