

Modification Approach Method for RC4 Using 2D Wavelet Transform

Assist. prof. Dr. Hala Bahjat AbdulWahab
Computer Science Department,
University of Technology,
Baghdad, Iraq.

Assist Lecture Maisaa Abid ali Khodher
Computer Science Department,
University of Technology
Baghdad, Iraq.

الخلاصة:

في السنوات القليلة الماضية أمنيّة البيانات أخذت بأعادة تطوير لمواجهة التكنولوجيا الحديثة والتطبيقات الجديدة والتي جلبت معها تهديدات جديدة، مما أدى الى العمل على طرح جديد للأمنيّة وميكانيكية جديدة. واحدة من المشاكل التي تعاني منها الانظمة الامنية هي كبر حجم البيانات المراد تنقلها عبر شبكات الاتصالات او الانترنت وبدون فقدان المعلومات العامة وكذلك الحفاظ على الخصوصية والسرية. هذا البحث يطرح طريقة تعمل على دمج مابين خوارزميات التشفير وخوارزميات ضغط البيانات للوصول الى خوارزمية جديدة تعمل على تقليص حجم الصورة الى المستوى الثالث وتشفيرها بشكل يحافظ على سرية المعلومات. ان النتائج التي تم الحصول عليها في الخوارزمية المقترحة ثم اختبارها وقد اجتازت كافة الفحوصات الشائعة وكانت النتائج مقبولة.

Abstract:

Every few years, computer security has to reinvent itself. New technologies and new application bring new threats, and force us to invent new protection mechanisms. One of the problems of the security systems is the increase the information that wanted to transfer without loss any information and keep the information with secrecy manner in this paper produce new approach aim to combine between two direction, cryptography algorithm and compression algorithm to reach to a new algorithm increase the secrecies with reduced the size of information from the selected image in three level according to the compression algorithm that selected in this paper, without loss any important information, the proposed algorithm.

Result is passing all popular tests and the result give accepted result.

1-Introduction:

Partial encryption enables information of different levels of security and / or destined for different uses to be encrypted into the same ciphertext. This property has many applications. It is known that an image can be considered as a combination of correlated and uncorrelated data as well as most of the perceptual information are present in the correlated data rather than the uncorrelated data. Hence, the amount of residual intelligence present in an encrypted image depends on the correlated data. It is, therefore, sufficient to encrypt the correlated data instead of encrypting the entire image in order to speed up the entire operation. From the perception point of view, the most significant bit (MSB) planes have high adjacent correlation between the pixels whereas the least significant bit (LSB) planes contain comparatively more uncorrelated data. PRS with simple hardware like m -sequences and Gold sequences have less correlation between the adjacent bits.

2- Image Compression:

Image compression is the application of Data compression on digital images. In effect, the objective is to reduce redundancy of the image data in order to be able to store or transmit data in an efficient form. Image compression can be lossy or lossless. Lossless compression is sometimes preferred for artificial images such as technical drawings, icons or comics. This is because lossy compression methods, especially when used at low bit rates, introduce compression artifacts. Lossless compression methods may also be preferred for high value content, such as medical imagery or image scans made for archival purposes [3].

3- cryptography:

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [6].

Cryptographic systems are characterized along three independent dimensions:[1,2]

- 1- The type of operations used for transforming plaintext to ciphertext. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged.
- 2-The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption.
- 3-The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block.

4- Wavelet Transform 2D:

Human visual perception is known to function at multiple scales. Wavelet transforms were developed for the analysis of multiscale image structures. Unlike traditional transform domain methods, such as the Fourier transform, wavelet-based methods not only dissect signals into their component frequencies but also enable the analysis of the component frequencies across different scales. As a result these methods are more suitable for such applications as image data compression, noise reduction, and edge detection [4].

4-1-Wavelet-Based Image Compression:

There are two types of image compression: lossless and lossy. With lossless compression, the original image is recovered exactly after decompression. Unfortunately, with images of natural scenes it is rarely possible to obtain

error-free compression at a rate beyond 2:1. Much higher compression ratios can be obtained if some error, which is usually difficult to perceive, is allowed between the decompressed image and the original image. This is lossy compression. In many cases, it is not necessary or even desirable that there be error-free reproduction of the original image [4].

4-2- Lossy Compression:

This paper on the following methods of losses compression: DWT (Discrete Wavelet Transform).

Quantizing refers to a reduction of the precision of the floating point values of the wavelet transform, which are typically either 16 or 32 or 64 bit floating point numbers [5].

To use less bits in the compressed transform which is necessary if compression 8bpp or 12bpp images is to be achieved these transform values must be expressed with less bits for each values. This leads to rounding error. These approximate, quantized, wavelet transforms will produce approximation to the images when an inverse transform is performed. Thus creating the error inherent in lossy compressed see image compressed in figure (1) and image decompressed in figure (2) [5].

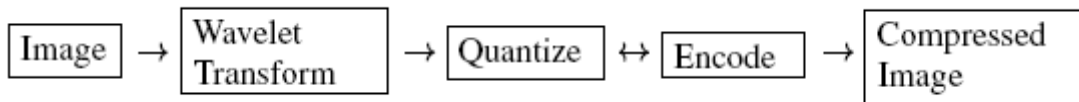


Figure (1) Compressed of Image

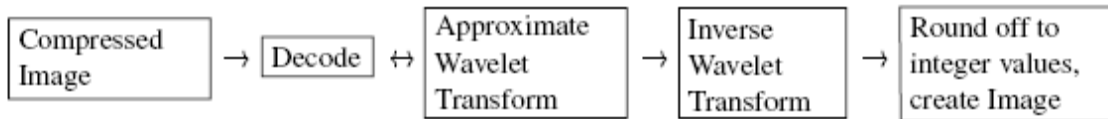


Figure (2) Decompressed of Image

5- Wavelet Thresholding:

The application of wavelet-based methods to image enhancement has been studied extensively. A widely used technique known as wavelet thresholding performs enhancement through the manipulation of wavelet transform coefficients so that object signals are boosted while noise is suppressed. Wavelet transform coefficients are modified using a nonlinear mapping. Hard-Thresholding and soft- thresholding functions are representative of such nonlinear mapping functions[4].

$$\begin{array}{lll}
 \text{if } X > T & \text{Then} & X - T \\
 \text{if } X < -T & \text{Then} & X + T \\
 \text{if } |X| \leq T & \text{Then} & 0
 \end{array}
 \quad \Phi(X) = \quad (1)$$

Small coefficients (below thresholding T or above $-T$) normally corresponding to noise and are reduced to a value near zero. Usually, the thresholding operation of equation (1) is performed in the orthogonal or biorthogonal wavelet transform domain [4].

In the following shown complete example to compress on image size(0-255) and type (BMP), shown in figure(3).

1	2	5	8	17	24	25	32
3	4	6	7	18	23	26	31
9	10	13	14	19	22	27	30
12	11	15	16	20	21	28	29
33	34	35	36	49	50	54	55
40	39	38	37	51	53	56	61
41	42	43	44	52	57	60	62
48	47	46	45	58	59	63	64

1	2	5	8	17	24	25	32
3	4	6	7	18	23	26	31
9	10	13	14	19	22	27	30
12	11	15	16	20	21	28	29
33	34	35	36	49	50	54	55
40	39	38	37	51	53	56	61
41	42	43	44	52	57	60	62
48	47	46	45	58	59	63	64

16 Parts of Images (2-level)

32 Parts of Images (3- level)

Figure (3)

6- Residual Intelligibility and Regularity of Digital image:

When ciphering systems are constructed, there must be some techniques to show the amount of *residual intelligibility* in ciphered images, and the quality of the reconstructed images. The noise (chaotic) with low *residual intelligibility* and low quality, on other side the reconstructed (deciphered) image, must give high intelligibility and high quality with high level of regularity[7].

6-1 Objective Fidelity Criteria

The objective fidelity criteria provide equations that can be used to measure the amount of error in the reconstructed (deciphered) images or to measure the amount of error between pure image and ciphered image.

Commonly used objective measures are the Root-Mean-Square error (*MSE*), Signal-to-Noise Ratio (*SNR*) and the Peak Signal-to-Noise Ratio (*PSNR*) [8].

step1: (The Mean Square Error (MSE)).

The *MSE* is the average of the square of errors (pixel differences) of the two images, it is found by taking the square root(“root”) of the error squared (“square”) divided by the total number of pixels in the image (“mean”) [10]:

$$MSE = \frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2$$

The Root Mean Square error ($RMSE$) is defined as the square root of the

Step2: ($PMSR$)

$$RMSE = \left[\frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2 \right]^{1/2}$$

Hence, the smaller the value of MSE , the better the deciphered image represents the original image and the large value of error. The better the ciphered image conceal pure image information.

Step2: ($Signal\ to\ Noise\ Ratio$).

It is fidelity parameter used to measure the distortion level caused by image cryptography can define as.

$$SNR = \frac{\sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y))^2}{\sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2}$$

And

Peak Signal to Noise Ratio (PSNR) can be defined as [9]:

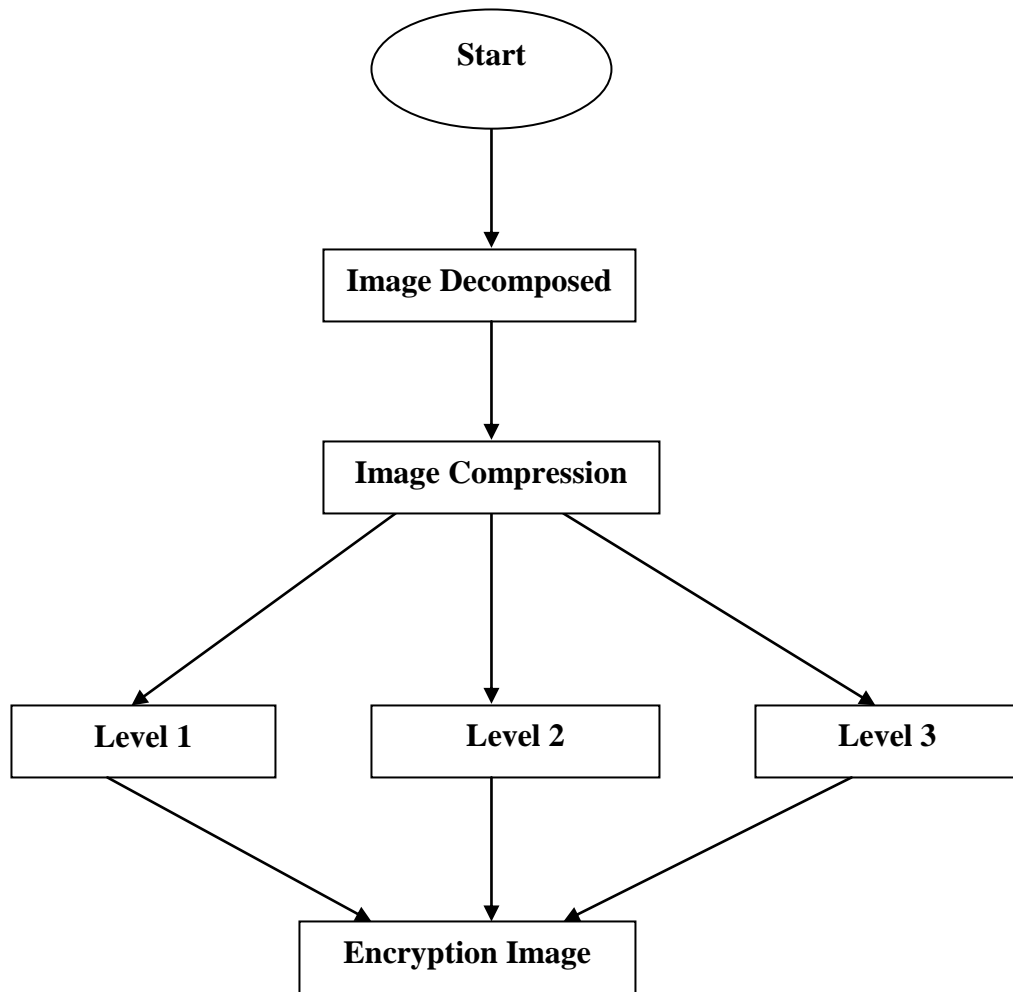
Step3:($PSNR$)

$$PSNR = 10 \log_{10} \left(\frac{(255)^2}{MSE} \right)$$

where MSE is the mean square error.

In image cryptography, the large value of $PSNR$ implies a better-deciphered image, and smaller number implies better image concealment of original image is obtained.

In down the block diagram that explain the main idea for to proposed algorithm



[Parameter of Algorithm]

A: parameter of original image.

B: parameter of image four parts.

C: parameter of image sixteen parts.

D: parameter of image thirty-two Parts.

Temp: parameter of swap.

SFC: parameter of array.

Ars: parameter of array.

7- Proposed New Approach Method for RC4 Using 2D Wavelet Transform :

In this research the photographs of the type (Bit Map Picture) and the pressure of the image to fragmentation manner Wavelet transform 2D into four parts and then take the picture in the first level LL1 as in Figure (5) that shown any part of the upper left of the original image.

{The first part in pushing the image at the first level LL1 and the sixteen to divide any part of the picture in the second level LL2 as in Figure (6) and then apply the RC4 encryption algorithm on the image}.

Process: (level one)

Input: compression Image, key (RC4 algorithm).

Output: Cipher Image.

Step1: Initial

A= Load original picture.

B= Compressed picture to decomposed with four parts (LL1).

C= Compressed picture to decomposed with sixteen parts (LL2).

D= Compressed picture to decomposed with thirty-two parts (LL3).

Step2: Encryption Process Level two:

For x= 0 to Ni2-1

For j= 0 to Nj2-1

Ars (y) = far2(x, y)

Step3: Applied the key on the picture in RC4 algorithm:

j=0

For i= 0 to Nj2-1

j=Abs ((j+Ars (i)+(i mod len(txtkey.Text)))modNj-1)

Step4: Swap in RC4 algorithm:

Temp= Ars (i)

Ars (i) = Ars (j)

Ars (j) = Temp

For y = 0 to Nj2-1

Sf (x, y) = Ars (y)

Step5: Result (Put the result of encrypted picture in E).

{In the second part, press the image at the second level LL2 and divide into thirty-two any part of the picture in the third level LL3 as in Figure (7) and also apply the RC4 encryption algorithm and this algorithm has been explained in detail above, where the image is encrypted based on the length of the key used to encrypt the image and the key system used to be binary number (0,1)}.

Step6: initial {the same A, B , C, D picture}

Step7: Encryption Process Level three:

For x= 0 to Ni-1

For j= 0 to Nj-1

Ars (y) = far (x, y)

Step8: Applied the key on the picture in RC4 algorithm:

j=0

For i= 0 to Nj-1

j=Abs ((j+Ars (i) + (i modlen (txtkey.Text))))modNj-1)

Step9: Swap in RC4 algorithm:

Temp= Ars (i)

Ars (i) = Ars (j)

Ars (j) = Temp

For y= 0 to Nj-1

Sf (x, y) = Ars (y)

Step10: Result (Put the result of encrypted picture in F).

End.

As the image increases as the encryption key length in the second level and third level LL2 and LL3 Encryption and more to the picture when it is sent over the Internet landscape is not lost because it is compressed based on partial encryption when it is sent over the Internet and network possible for the recipient to open the code and get the picture.

The more compact than the picture whenever the encryption process faster and less time in the process of sending the picture through the networks.

In the following figure (4-a, b, c) shown the block diagram for decomposed three level.

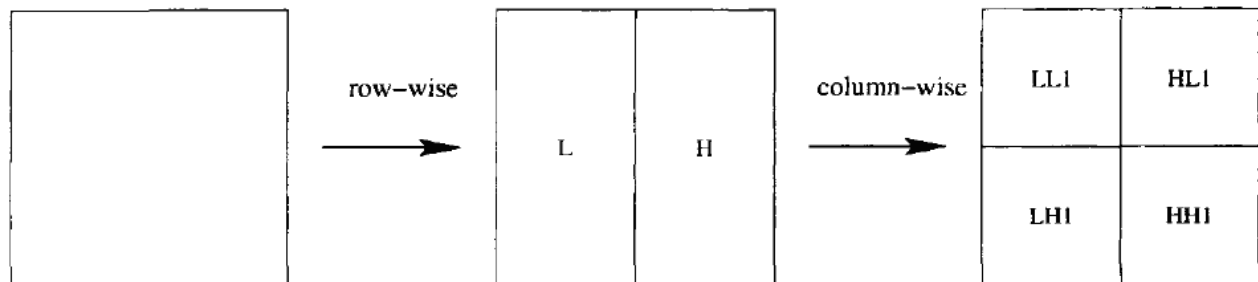


Figure (4-a) First Level Decomposed

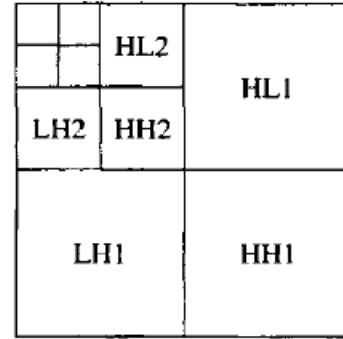
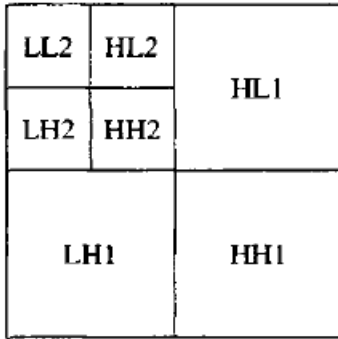


Figure (4-b) Two Level Decomposed

Figure (4-c) Three Level Decomposed

Implementation:

In this section executed the proposed algorithm and the selected image is size (255) and shown in the result of the selected image in three levels.

In the following shown in figures (5, 6,7) the executed the algorithm.

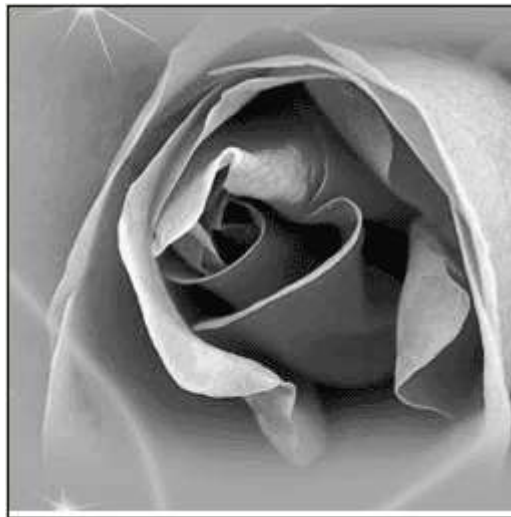


Image original

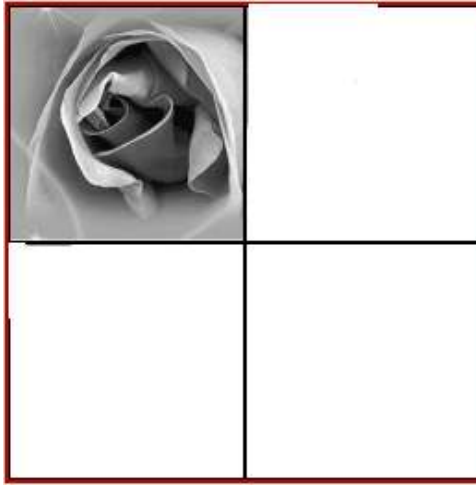


Figure (5) Image Four parts first Level

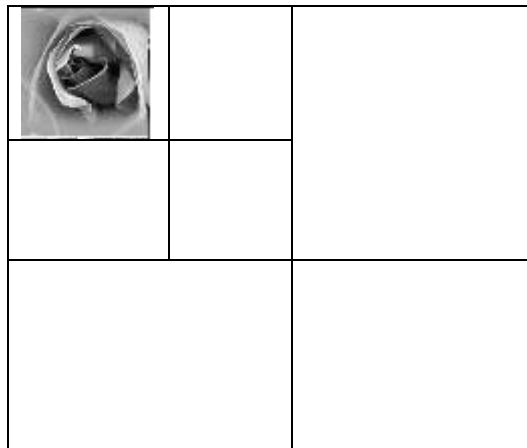


Figure (6) Image Sixteen parts second Level

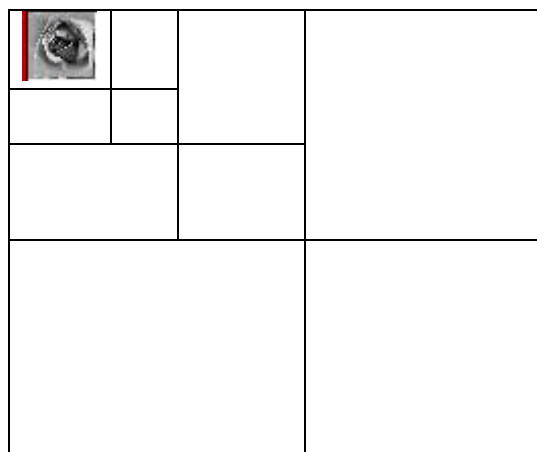


Figure (7) Image Thirty –two parts three Levels

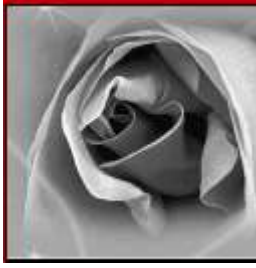


Image Four part



Image sixteen part



Image thirty-two

Test the results:

In this section execute two more tests the cipher image, shown in figure (8) and figure (9).


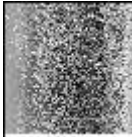




Length of Key	Level	Encrypted picture
One byte	2	
Two byte	2	
Three byte	2	
Four byte	2	
Five byte	2	
Six byte	2	

Figure (8) Test one

According from the result that obtained form encryption process for the image show that when increase the key length size reach to image with good cipher that cancel all the information.







Length of Key	Level	Encrypted picture
One byte	3	
Two byte	3	
Three byte	3	
Four byte	3	
Five byte	3	
Six byte	3	

Figure (9) Test two

According to the measurement test illustrated that in section (6) implementation the measure on the cipher image.

In the following shown the result for test on all image with three levels in table (1)

According to the result in table (1)

From the results of the measures that were used to test the ciphered images, we can obtain the following:-

- 1- The large results of MSE means the proposed algorithm is succeeded to conceal pure image information (i.e. there are large errors in ciphered image caused by the use of the proposed algorithm.).
- 2- The small results of SNR and PSNR means the proposed algorithm caused large noise (i.e. small, a result implies better image concealment of original image.).

8- Conclusion:

In this research can be detected three conclusion:

- 1- Image Encryption plays an important role in the image sent through the local and international networks in order to maintain the structure of the picture, especially when the image is compressed where the encryption part of the picture.
- 2- Image has been way RC4 encryption to maintain the structure of the image and based on the length of the key to this method as the key length increases as becoming stronger as the compressed image encryption possible and return to the original image when received.
- 3- Without loss any information according to the results from the tests.

References:

- 1- William Stalling, (2005), "Cryptography and network Security Principles and Practices" Four Edition ,.
- 2- Schaefer E. D., (1999) . "An introduction to Gryptography", Santa Clara University.
- 3- David Salomon, (2004), "Data Compression", Third edition.
- 4- Qiang wu, Fatima Merchant, Kenneth R. Cattleman, (2008) "Microscope Image Processing".
- 5- Ed. K. R. Rao and P. C. Yip. , (2001), "The Transform and Data Compression Handbook", Boca Raton, CRC Press LLC.
- 6- Schneir B., (1997). "Applied Cryptography", Second Edition.
- 7- Raghad Z. Y. Al-Macdici and Dr.Muzhir S. M. Al-Ani, (2001). "Modified Large-Scal Randomization Key-Stream Generator fo Digital Image Encryption" , Second National Conference on Computer , Communication and Control Engineering.
- 8- Scotte E. U., (1998). "Computer Vision and Image Processing :Practical Approach Using CVIp Tools", Prentice-Hall ,Inc.
- 9- Ayad A. Salam. (2005). "Visual Partial Encryption Using Wavelet and Clock-Controlled Random Algorithm", PhD. Thesis, Ministry of Higher Education and Scientific Research in Computer Sciences.
- 10- Ikhlas Khalaf Alsaadi, (2005). "Lossless Wavelet Based Image ComparessionWith Hybird 2D Decomposition", M.Sc. Thesis, University of Technology at Computer Science.

Table (1)

Image cipher	MAE			MSE			RMSE			PSNR			SNR		
	R	G	B	R	G	B	R	G	B	R	G	B	R	G	B
1 B LL2	1.6402366	0.527337	0.567337	5305.794586	5868.168553	1199.4525511	72.840885	76.60397	34.633113	2.921886	2.771864	5	6.101560	5.547700	8.371344
2 B LL2	1.6402366	3.274082	0.746982	5305.79458	6322.128083	1178.710539	72.840885	79.51181	34.332354	2.921886	2.663124	5	6.101560	5.343778	8.452341
3 B LL2	-11.15978	-6.71641	1.295873	8528.46991	8256.961124	1552.167727	92.349715	90.86782	39.397559	2.2443097	2.288233	5	3.712783	3.856638	7.233072
4 B LL2	-13.07023	-7.96795	2.086698	8367.322409	8229.39966	1511.139851	91.473069	90.71604	38.873382	2.2701700	2.292791	5	3.795629	3.871159	7.349412
5 B LL2	-14.67207	-11.7036	0.567596	7941.34857	7870.905791	1164.417893	89.114244	88.71812	34.123568	2.341566	2.353823	5	3.959150	4.001192	8.466099
6 B LL2	-13.83452	-12.3969	-0.95349	7657.25297	7522.23588	1120.388476	87.505731	86.73083	33.472204	2.3918380	2.416536	5	4.117363	4.197969	8.633501
1 B LL3	7.944489	9.342040	17.228571	7113.694690	7928.481628	3820.224487	84.342721	89.04202	61.807964	2.494707	2.343795	3	4.842803	4.438934	5.024882
2 B LL3	11.691270	7.950793	3.727777	6357.43580	6702.09533	1261.603985	79.733529	81.86633	35.519065	2.655071	2.579235	5	5.340165	4.692629	7.313609
3 B LL3	7.808642	0.951388	-3.408179	8494.98617	7751.851138	2348.395850	92.168249	88.04459	48.460250	2.249633	2.237484	4	4.088066	4.080373	4.609909
4 B LL3	-0.993243	-0.35060	-3.433934	8857.75321	8313.35830	2358.75681	94.115637	91.17762	48.567034	2.193275	2.27896	4	3.911709	3.793957	4.626051
5 B LL3	-0.882645	6.509246	6.0753911	8398.760226	7372.56037	1238.261722	91.644750	85.86362	35.1889431	2.2650775	2.444558	5	4.121680	4.314219	7.485401
6 B LL3	-0.704125	-0.45234	2.753200	9866.428063	8137.369760	1775.229711	99.329895	90.20737	42.1334749	2.0502944	2.308144	4	3.422230	3.885562	5.917119