MedWell Online
Journal of Engineering and Applied Sciences 1(4): 316-322, 2006
© Medwell Online, 2006

Developing a High Level of Image Encryption Using Wavelet and Cipher Block Chaining (CBC)

Yas A. Alsultanny
Graduate College of Computing Studies-Amman Arab University for
Graduate Studies Amman 11953, Jordan P.O.Box : 2234

Abstract: The study present a new technique to image encryption, by partitioning the images to 4*4 and 8*8 blocks, the proposed technique of block replacement introduced by dividing the security key to four segment and one bit from the mod of the segment is selected with it's complement. The diagonal mappings of the blocks are used to reduce the regularity that can be occur through the blocks mapping process. The wavelet used as a tool to deform the image histogram by converting the histogram of the image to two regions of black and white, in order to remove the information from the image. The last stage of the proposed technique is to apply the Cipher Block Chaining (CBC), which create fictitious information to the image histogram. The correlation of two adjacent pixels is used to measure the degree of image adjacencies. The results showed that the original image have adjacency about 90%, by the proposed technique of the image encryption of the adjacency reduced to about 2%. The new technique applied to different sources and sizes of images and it gave good results.

Key words: Image encryption, wavelet, Cipher Block Chaining (CBC), mapping

INTRODUCTION

The security of the digital images becomes important since images can be attached through the transmission over networks or Internet. Algorithms that are good for textual data might not be suitable for multimedia data and, primarily due to the relatively huge size of the images and the nature of the image data itself.

Data redundancy and relationships between pixels are two main problems when dealing with image encryption. There are several relationships between pixels especially between a pixel and its neighbors. Connectivity between pixels is an important concept used in establishing boundaries arias of objects and components of regions in an image[1]. The value of any given pixel can be reasonably predicted from the values of their neighbors. If there are some visible edges, then it can be used in object recognition and scene interpretation.

It is well-known that symmetric cipher systems have some advantages for bulky encryption application[2,3]. One of the most important modes used with block ciphering is the Cipher Block Chaining (CBC). It has some favorable features for image encryption: (i) its suitable for file encryption, (ii) the same block is encrypted to different ciphered block, (iii) it achieves a high level of security. The wavelet and a new method of mapping are used in this study to increase the level of the image encryption.

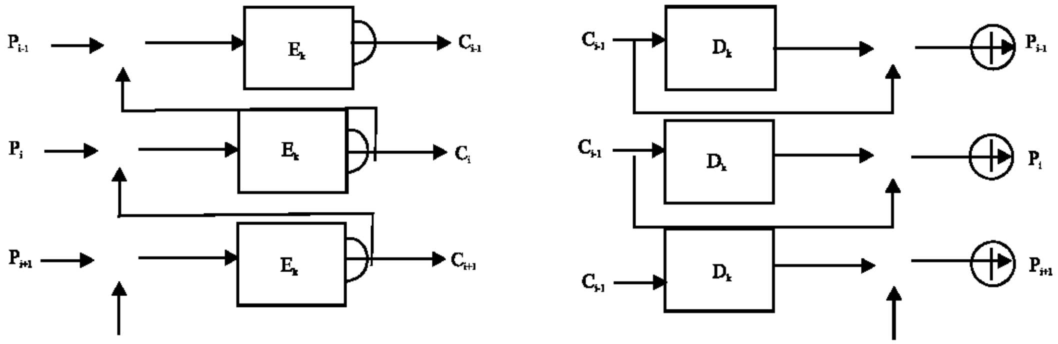
Cipher Block Chaining Mode (CBC): There are several ways of classifying cryptographic algorithms. One of these is the Secret Key Cryptography: A single key is used for both encryption and decryption. There are several secret key cryptography schemes and they are generally categorized as either stream ciphers or block ciphers. Block ciphers can operate in one of the several modes. One of the most important modes is the Cipher Block Chaining (CBC) mode. This mode adds a feedback mechanism to the encryption scheme: The previous encrypted blocks are fed back into the encryption of the current block. Mathematically, this looks like:

$$C_i=E_k(P_i \oplus C_{i+1}) \qquad (1)$$

Decryption is done in the reverse order as follows:

$$P_i=C_{i-1} \oplus D_k(C_{i-1}) \qquad (2)$$

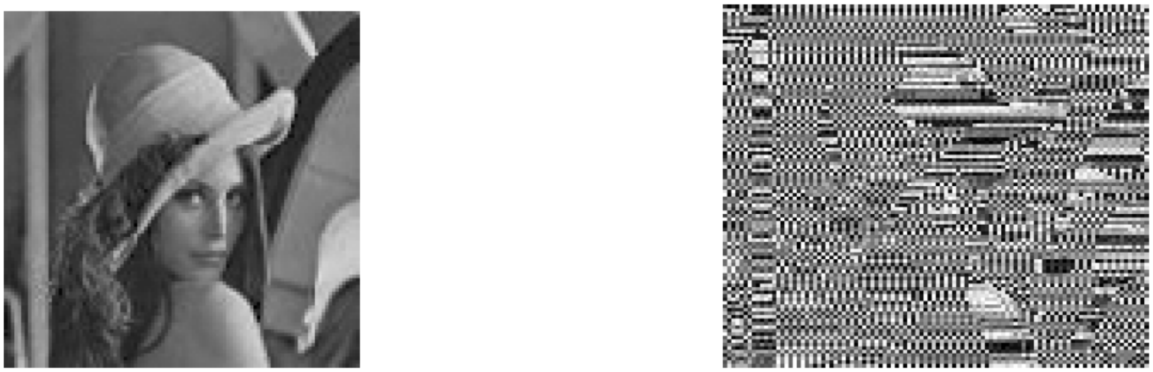
Where;
C_i and P_i; are the encryption and decryption of image blocks.
E_k and D_k; are the encryption and decryption functions
Fig. 1 shows the (CBC) encryption and decryption block diagrams. One of the most characteristics of this mode is that it allows identical blocks to be encrypted to different ciphered block. CBC is the best for encrypting files or



a: CBC encryption

b: CBC decryption

Fig. 1: Cipher Block Chaining (CBC)



a: Original image

b: Ciphered image by CBC mode

Fig. 2: Lena image and its encryption

messages of length greater than 64 bits. Because of its use to achieve confidentiality, it can be used for authentication. The main drawback of this mode comes from it's error propagation. An error in a plain block will affect the corresponding ciphered block and all subsequent ciphered block. In addition, the encryption of each ciphered block depends on its corresponding plain block and all it's subsequent blocks[4].

Figure 2 shows the result of image encryption using the CBC, the result of encryption of this mode is very weak due to the residual information from the original image. Where there are some visible edges, these enable the attacker to recognize the image. The new technique will be applied by using wavelet and image block mapping will increase the level of encryption as will be shown in the study.

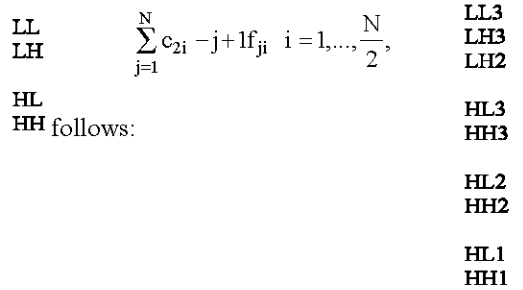
Wavelets: A wavelet is a small wave, which has its energy concentrated in time. It is an orthogonal function which can be applied to a finite set of data in order to separate parts of a signal that overlaps in both time and frequency[5]. It has the ability to split a signal into two components. One of these components, named H for smooth or low-pass band, contains useful and large scale of information and gives more useful information about the desired signal (looks like the original signal). The other component, named G for detail or high-pass band, contains the local noise or undesired signals which will be zero or almost zero[6].

There are many wavelets defined on rows of samples. For image processing we use a wavelet works on the two dimensional grid. The Mallat algorithm is a computationally efficient method of implementing the wavelet transforms[7]. The one-dimensional wavelet transform can be viewed as an application of pair of filters H and G. Each filter creates an output matrix of a half length of the original one. The low-pass band is produced by the H filter function by computing the average of every two samples as follows:

Whereas the high-pass band is produced by the G filter by computing the difference of every two samples asWhere c are the coefficients, f is the input function

$$\sum_{j=1}^{N} c_{2i} - j + 1 f_{ji} \quad i = 1, \ldots, \frac{N}{2}, \qquad \ldots(3)$$

follows:



a: The four output bands of wavelet filters

b: The hierarchy of wavelet bands

Fig. 3: The wavelet level bands

$$b_i = \frac{1}{2} \sum_{j=1}^{N} (-1)^{j+1} c_{j+2-2i} f_j, \ i = \qquad (4)$$

a and b are the output functions. It's expected that the output of G filter contains less information than that of H filter. To reconstruct the original matrix, the inverse low-pass filter is applied to the low-pass band as follows:

$$f_j^{\ L} = \sum_{i=1}^{N/2} c_{2i-j} a_i, \ j = 1 \qquad (5)$$

Whereas the inverse high-pass filter is applied to the high-pass band as follows:

$$f_j^{\ H} = \sum_{j=1}^{N/2} (-1)^{j+1} c_{j+1-2i} b_i, \ j \qquad (6)$$

The original matrix is reconstructed by the sum of inverse low-pass and inverse high-pass outputs:

$$F = f^L + j, \qquad (7)$$

The two-dimensional wavelet transform of an image can be performed by the one-dimensional transform on the columns, followed by the one-dimensional transform on the rows[8]. Each implementation of the filters creates four bands labeled by: LL, LH, HL and HH as shown in the Fig 3a. Because the smooth signal (LL band) is again a continuous signal, it's possible to repeat the whole work again and again until its dimensions are smaller than some threshold, resulting in a hierarchy of bands as shown in Fig. 3b. Applying this transform for the first time is called level 1. Applying it again on LL band is called level 2 and so on.

Block mapping algorithm: The encrypted image looses its logical context and object edges. In other words, there is no possibility to obtain some useful information about the plain image by only observing the ciphered image, to increase the degree of encryption, the developed algorithm will be implemented by the following steps (as shown in Fig. 4);

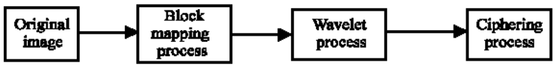


Fig. 4: The main steps of the proposed algorithm

1. Block mapping process
2. Wavelet process
3. Encryption process

Block mapping process: The main purpose of this step is to break down the existing relations and connectivity between pixels as much as possible, in order to reduce the relationship between the pixels adjacencies. The main idea of this process is to divide an image into K of blocks ($K=2^{m}*2^{m}$, where m = 1, 2, 3 ...). These blocks are rearranged in a way that will be depended on the used key to keep a new block distribution. Using different keys will result in different arrangements. This process consists from the following steps:

1- Divide the used key into a set of divisions (D_1, D_2, D_3, ...); From each division D_i, a bit is selected where D_i consists of l_i of bits, we need to select a number of bits from the key to label a number of blocks (k). For example: if the used key is (11110101 11010111 10110011 10101001) and the image will be divided to 16 blocks, then 4 bits will generate the 16 label to each block. Hence, the key is divided into 4 parts of 8 bit each. A bit will be selected from the following: D_1=10101001, D_2=10110011, D_3=11010111 and D_4=11110101 where l_i =8 bits.

2- Select the j'th bit b_i from D_i; the bit selected by;

$$j\text{-}1 = \text{decimal number of}(D_i) \bmod l_i \qquad (8)$$

The complement of each selected bit is computed. The first element of the vector V_i is the selected bit b_i, whereas, the second element is it's complement b_i. For example: in the case of D_1= $(10101001)_2$=$(169)_{10}$ and (169 mod 8)=1. This means that the first element of V_1 is the 2nd bit of the division D_1 which is 0, whereas, the second bit of the vector V_1 is the complement which is (1). In other words, V_1=[0,1]. By the same procedure, we will get the V_2=[0,1], V_3=[1,0] and V_4=[1,0]. This illustrated in Fig. 5.

3-Construct K different numbers; from all combinations of the elements of each vector V_i, a

Key = 11110101 11010111 10110011 10101001			
D_4 = 11110101	D_3 = 11010111	D_2 = 10110011	D_1 = 10101001
$(11110101)_2 = (245)_{10}$	$(11010111)_2 = (215)_{10}$	$(10110011)_2 = (179)_{10}$	$(10101001)_2 = (169)_{10}$
245 mod 8=5	215 mod 8=7	179 mod 8=3	169 mod 8=1
77 6 5 4 3 2 1 0 1 1 1 1 0 1 0 1	7 6 5 4 3 2 1 0 1 1 0 1 0 1 1 1	77 6 5 4 3 2 1 0 1 0 1 1 0 0 1 1	77 6 5 4 3 2 1 0 1 0 1 0 1 0 0 1
$V_4[0]= 1, \bar{V}_4[1]=0$	$V_3[0]= 1, \bar{V}_3[1]=0$	$V_2[0]= 0, \bar{V}_2[1]=1$	$V_1[0]= 0, \bar{V}_1[1]=1$

Fig. 5: Generating the vector V_i from D_i

Generated number (Block number in the original order)	12	4	8	0	14	6	10	2	13	5	9	1	15	7	11	3
sequence number (Block number in the new order)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Fig. 6: The mapping between the generated number and it's sequence number

new number is generated using the following algorithm:

```
for i = $V_1[0]$ to $V_1[1]$
    for j = $V_2[0]$ to $V_2[1]$
        for m = $V_3[0]$ to $V_3[1]$
            for n = $V_4[0]$ to $V_4[1]$
```

Compute the decimal number from the evaluation of (n || m || j || i)

The generated numbers represents the label order of each block in the original order of the image. The sequence in which these numbers are generated is important and must be kept. It represents the new locations to which block of the original order will be mapped. This is shown in Fig. 6.

4-Block Mapping; This is done according to the order derived in step 3. If the mapping are labeled horizontally as shown in Fig. 7a, then there will be some regularity after moving blocks according to the mapping order declared in Fig. 6. For example: as shown in Fig. 7b, each address number in the column i is greater than the address number in the column i+2 by 4 (for the same row). Also, each address number in row j is greater than the address number in row j+2 by 1 (for the same column).

To remove this kind of regularity, locations in the original data file are numbered diagonally as shown in Fig. 8.

Fig. 9a shows the results of mapping, when this approach is applied to Lena image when, K = 16 (4x4) segments, Fig. 9b shows the image when, K = 64 (8x8) segments.

Applying wavelet transform: The main purpose of using wavelet transform is to use it's ability to separate image data into two parts: low-pass band and high-pass band. This feature can be used as a means of encryption which will deform the histogram of the image. The main defect of using this transform is that the low-pass band contains useful and large scale of information and gives more

12	13	14	15
8	9	10	11
10	1	5	8
0	1	2	3

After mapping

15	7	11	3
13	5	9	1
12	6	10	2
12	4	8	0

a: Block labels to the image data horizontally

b: The new order according to Fig. 6

Fig. 7: Regularity of blocks mapping

15	14	12	3
13	11	9	6
10	1	5	8
0	4	7	9

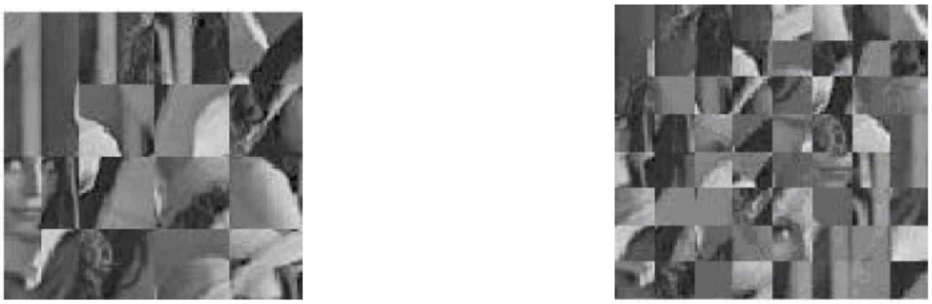
After mapping

3	11	15	0
7	1	8	10
9	4	6	13
12	14	2	5

a: Block labels to the image data diagonally

b: The new order with out regularity

Fig. 8: Block labeling without regularity



a: Lena image divided into 16 (4x4) segments

b- Lena image divided into 64 (8x8) segments

Fig. 9: Image mapping

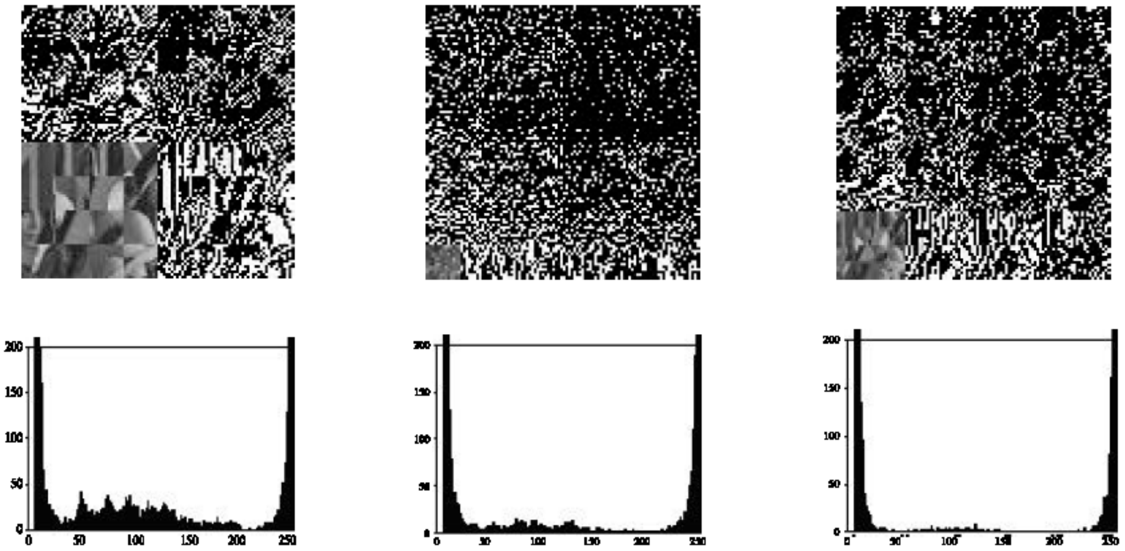
useful information about the desired signal (looks like the original signal).

When applying level1 of this transform for a first time (Fig. 10a, the signal is separated into two bands and the image is divided into 4 divisions. By applying the same transform on each previous division for a next time (Fig. 10b, the scale between the two bands increases and most of the gray level values concentrated at the end points. When applying the transform for a third time on each of the previous divisions, the two bands are extremely separated (Fig. 10c. It looks like that the image consists only from black and white data.

Encryption using cbc mode: The image now is ready to be encrypted using CBC mode. For simplicity, the XOR algorithm is used in the encryption algorithm.. When using this mode, the same plain blocks are encoded to different ciphered blocks using the same key. But, it may be noted that the difference between the ciphered blocks is too small. This means that they are almost have the same gray level.

It's important that the encrypted image looses its logical context and edges that corresponded with object borders which are very important for object recognition and scene interpretation. In other words, there is no possibility to obtain any useful information about the plain image, by only observing the ciphered image. Fig. 11b shows the encrypted image when applying the CBC to the image of 4x4 segments and Fig. 11c shows the encryption to the 8x8 segments. The histogram of the encrypted image show that there are a fictitious object generated to this image, this will give a high level of encryption, where the hacker sense that there are some objects in the image, but this is not true.

Security analysis: The experimental results showed that the proposed algorithm has a good effect on security level in a way that it does not contain any useful information about the plane image. The proposed scheme has very good confusion and diffusion properties. The mapping step plays a main role in doing diffusion, whereas, wavelet transform plays a main role in doing confusion. Since

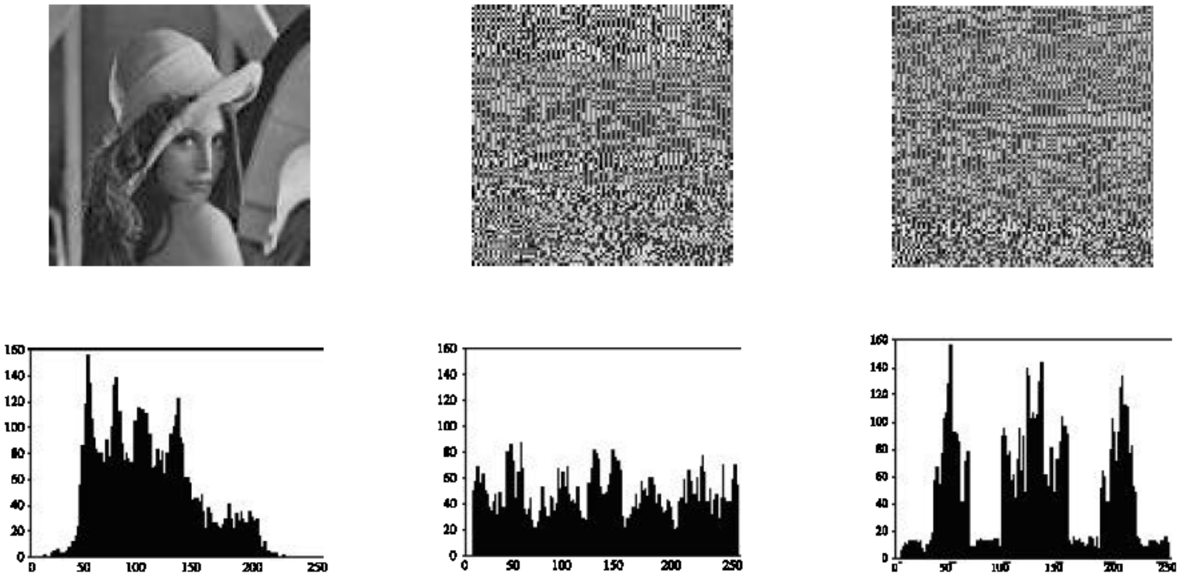


a: Applying wavelet transform time for a first time

b: Applying wavelet transform for a second time

c: Applying wavelet transform for a third

Fig. 10: Applying wavelet to the mapping image in Fig. 9b



a: Lena image before encryption

b: Encryption to 4*4 segmentation image after applying CBC mode

c: Encryption to 8*8 segmentation image after applying CBC mode

Fig. 11: Encryption by applying CBC mode to the different image segments

many kinds of ciphers can be solved or tested by statistical analysis, we use the correlation between adjacent pixels to test the security level of the proposed algorithm.

The Correlation between adjacent pixels; used to measure the strength of the linear relationship between pixels variables X and Y. The linear correlation coefficient, r. is defined by;

$$r = \left| \, S_{xy} \Big/ \sqrt{S_{xx} S_{yy}} \, \right| \qquad \ldots(9)$$

Where;

Table 1: Adjacent correlation results

Image segments	Correlation direction	Percentage (%) of original image correlation	Percentage (%) of image correlation after block mapping	Percentage (%) of image correlation after applying wavelet	Percentage (%) of correlation after image encryption
4x4	Horizontal neighbors	88.3	0.3	5.50	2.14
	Vertical neighbors	95.0	0.2	32.8	0.80
	Diagonal neighbors	86.9	1.9	17.3	0.17
Image segments	Correlation direction	Original image	Image after block mapping	Image after applying wavelet	After image encryption
8x8	Horizontal neighbors	88.3	19.5	1.20	2.03
	Vertical neighbors	95.0	14.4	27.7	2.70
	Diagonal neighbors	86.9	18.0	0.60	2.90

$$S_{xy} = \sum xy - (\sum x)(\sum y)/n,$$

$$S_{xx} = \sum x^2 - (\sum x^2)/n,$$

$$S_{yy} = \sum y^2 - (\sum y)^2/n$$

x and y are gray scale values of two adjacent pixels in the image. The two variables (pixels) can be any two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels. For any pixel A[i][j], the adjacent vertical pixel is A[i][j+1], the adjacent horizontal pixel is A[i+1][j], the adjacent diagonal pixel is A[i+1][j+1] for i and j = 1, 2, …,N-2. Table (1) shows the results of computing horizontal, vertical and diagonal coefficient correlation values before and after applying each step of the proposed algorithm. It's clear that the mapping step plays a main role in decreasing the correlation between pixels. For this point, we could consider the mapping process as a method of image de-correlation. In general, the correlation extremely decreases from approximately 88% for horizontal neighbor pixels, 95% for vertical neighbor pixels and from 87% for diagonal neighbor pixels, to values approximately less than 2%.

CONCLUSION

This study represents a new technique of image encryption by introducing the mapping technique, which is constructed by dividing the image to segments of 4*4 or 16*16 segments, a new method of mapping introduced in order to decrease the adjacency between image pixels, the results showed that the adjacency will be less than 2% after encryption. The wavelet is used to deformation the histogram of the image to separate the information to two bands black and white, which remove all the information. The CBC encryption mode applying to redistributed the image information and creating a factitious objects, which are appear to the hackers as an indication to the hacker as an objects, but really they are false data.

The proposed scheme has very good confusion and diffusion properties such that it will not be possible to obtain some useful information about the plain image by only observing the ciphered image, as well as the technique used have high level of complexity, which is not easy to decrypt by hackers. .

REFERENCES

1. Rafael C. Gonzalez and Richard E. Woods, 2002. Digital Image Processing. Prentice Hall.
2. Bruce Schneier, 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, Inc.
3. Scharinger, J., 1998. Fast Encryption of Image Data using Chaotic Kolmogorov Flow. Electronic Imaging J., 7: 318-325.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1997. Handbook of Applied Cryptography. CRC press.
5. Sidney, C., Ramesh A. Gopinath and Haitao Guo, 1998. Introduction to Wavelets and Wavelet Transforms. Prentice Hall.
6. Sieuwert van Otterloo, 2000. Amazing Wavelet Image Compression. Utrecht.
7. Tim Edwards, 1991. Discrete wavelet transforms: Theory and Implementation. Stanford University.
8. Howard Chi Ho Cheng, 1998. Partial Encryption for Image and Video Communication. University of Alberta.