Journal of KerbalaUniversity , Vol. 11 No.1 Scientific . 2013

A Selective Image Encryption Based on Chaos Algorithm

Asst. Prof: Dr. Abeer Matti Yousif
College of Science,
Al -Nahrain University
Abeermatti@yahoo.com

Manaf Mohammed Ali
M.Sc Student
Informatics Institute For
Postgraduate Studies

Abstract

Selective encryption is a new trend in image and video content protection. It's aim to reduce the amount of data to protect while preserving a sufficient level of security by connected with chaotic theory. Due to their features of ergodicity, sensitivity to initial conditions, pseudo randomly, chaotic maps have good potential for information encryption. In this work, selective image encryption based on chaos algorithm has suggested, This technique adopted two main operations one to decorrelate the relationship between adjacent pixels of plain image which is based on 2D Chaotic Standard map and the other to decorrelate the relationship between the plain image and encrypted image which is based on 4D Chaotic Map. Experimental results show that the proposed scheme is computationally secure, it withstands different types of attacks such as brute force attack, differential attack, chosen-plaintext and chosen-ciphertext attacks. Also, Experimental results show that the proposed scheme is suitable for multimedia application with real time operation. Where the average execution time is (1 second) when the encryption ratio is equal to (6.25 %).

Keywords: Selective encryption of images, Partial encryption, Chaotic map, Discrete cosine transform

الخلاصة

التشفير الانتقائي هو توجه جديد في حماية محتوى الصور والفيديو .فهو يهدف إلى تقليل من كمية البيانات المخصصة للتشفير مع الحفاظ على مستوى كافي من الأمان من خلال الترابط مع نظرية التشويش. نظرا لما تمتلكه من خصائص مثل (ergodicity), الحساسية للظروف الأولية, ظهورها بشكل أشبه بالعشوائي, نظرية التشويش تنطوي على إمكانية جيدة في تشفير المعلومات. في هذا البحث, أقترح تشفير الصورة الانتقائي بالاعتماد على خوارزمية التشويش, هذه التقنية تبنت عمليتين أساسيتين واحدة لتفكيك العلاقة بين نقاط الصورة المتجاورة للصورة المراد تشفيرها والتي تقوم على أساس معادلة التشويش القياسية ثنائية البعد والأخرى لتفكيك العلاقة بين الصورة الأصلية والصورة المشفرة والتي اعتمدت على معادلة التشويش رباعية البعد. وقد أظهرت النتائج أن المنظومة المقترحة هي (computationally secure), فإنها تقاوم أنواع مختلفة من الهجمات مثل هجوم القوة, الهجوم التفاضلي, هجمات الصورة المختارة والمشفرة المختارة. كذلك أظهرت النتائج أن المنظومة المقترحة ملائمة لتطبيقات الوسائط المتعددة مع نظام الوقت الحقيقي. حيث معدل وقت التنفيذ هو(ا ثانية) عندما تكون نسبة التشفير تساوي(6.25%).

I . Introduction

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content fulfill the security requirements for particular multimedia application. To make use of the communication networks already developed and to keep the secrecy simultaneously, cryptographic techniques need to be applied. Traditional symmetric ciphers such as Data Encryption Standard (DES) are designed with good confusion and diffusion properties, however they are not suitable in the case of multimedia information. This is because the intrinsic properties of visual information such as bulk data capacity, strong pixel correlation and high redundancy, will lower the encryption performance [1].

Many methods have been devoted to investigate better solutions for multimedia content encryption such as chaotic image encryption, selective image encryption. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore,

chaotic cryptosystems have more useful and practical applications [2]. Selective image encryption schemes are often designed not to encrypt the entire images completely, but a portion only. The key point is to encrypt only a small part of the bit stream to obtain a fast method[3]. The following issues have to be taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts [4]:

1. Tradeoff between bulky data and slow speed: Digital images and videos are generally bulky data of large sizes, even if they are efficiently compressed. Since the encryption speed of some traditional ciphers is not sufficiently fast, especially for large – sized bulky data.
2. Tradeoff between encryption and decryption and compression: if encryption is applied before compression, the randomness of cipher texts will dramatically reduces the compression efficiency. Thus, one has to apply encryption after compression, but the special and various image/video structures make if difficult to embed an encryption algorithm in to the integrated system.
3. Visual degradation (VD): Measures the perceptual distortion (preferably configurable) of the cipher image with respect to the plain image.
4. Encryption ratio (ER): This criterion measures the ratio between the size of the encryption part and the whole data size. It is one of the main expected features of selective encryption.

In response to the aforementioned challenges in protecting multimedia content, the objective of the proposed scheme in this paper is specially oriented towards designing and implementing a secure, fast image encryption and tunable for different applications like real time systems based on combination of selective encryption and chaos schemes.

The organization of this paper is as follows. In section 2, we explain the discrete cosine transform. Section 3 review the previous research findings. Section 4 introduces the present work. Finally, section 5 shows the experimental results and conclusions of this study are given in section 6.

II . Discrete Cosine Transform

The discrete cosine transform is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain. Many digital image and video compression schemes use a block-based DCT, because this algorithm minimizes the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images. The most important visual characteristics of the image are placed in the low frequencies while the details are situated in the higher frequencies. The Human Visual System(HVS) is most sensitive to lower frequencies than to higher ones [5].

The top left corner of the DCT matrix contains a value that is always of a very great magnitude and low frequency called the DC coefficient. All of others represent increase in higher vertical and horizontal frequencies, called AC coefficient and become lower magnitude as they move from the left to right or from up to down. It means that by performing the DCT on an image in spatial domain, the representation will concentrate in the upper left corner of the DCT matrix, with the lower right coefficients containing less useful information [6].

DCT is considered an optimal transform among the other transform techniques, It is considered as a member of many sinusoidal transformations that have been more preferable, it preserves relatively high compacting of energy in small number of transform coefficients.

Assuming an 8x8 (image block) the forward (2-D) discrete cosine transforms equation is given by the following equation [7]:

$$G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} p_{xy} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \quad \ldots.(1)$$

where $C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0, \\ 1, & f > 0, \end{cases}$ and $0 \le i, j \le 7.$ ….(2)

where C_f is C_i, C_j and P_{xy} are the values of image component $i,j = 0,1,...,7$, $x,y = 0,1,\ldots,7$.

III . Previous works

Several selective encryption methods have been proposed for DCT compressed images. Droogenbroeck and Benedett [8] selected AC coefficients from compressed images for encryption. In their method the DC coefficients are not ciphered because they carry important visible information and they are highly predictable. The compression and encryption stages are separated in this approach and this requires an additional operating cost. Roueida Mohammed Yass [9] her work focuses on Image security integrating encryption with multimedia compression systems. Three approaches for integrating encryption with image compression system are proposed, Color Plane Permutation, Discrete Cosine Transform (DCT) coefficients confusion, and sign encryption of DCT coefficients. The proposed approaches are motivated by selective encryption, were a portion of the coefficients from either the final results or intermediate steps of a compression system are enciphered with a cryptographic cipher. These methods provides a certain level of confidentiality and slow cipher. Ge Xin and *et al.'s*. [10] proposed an image encryption algorithm based on spatiotemporal chaos in DCT domain To solve the drawbacks of some chaotic image encryption schemes, The image after DCT transformation and quantization is encrypted block by block. Propagating cipher-block chaining mode (PCBC) is adopted in the scheme, and it's from analysis and experiments that the scheme can resist chosen plaintext and ciphertext attacks without influence on the compression efficiency. Ping Xu, Jianjun Zhao and Dihua Wang [11] proposed A selective image encryption algorithm based on hyper-chaos. The plain image is first divided into blocks, and the coefficient blocks are obtained by performing DCT transformation and quantization on the blocks. Then encrypted part of blocks by 4D Chen's system. Analysis and experimental results show that the encryption algorithm is acceptable and secure.

IV The Proposed Scheme

The main objective of this work is to design and implement a new fast and highly secure selective image encryption scheme for confidentiality purpose which can be applied in real time systems and to solve the drawbacks of some previous chaotic image encryption schemes. In addition to abovementioned goal, the proposed encryption scheme intended to be integrated with JPEG compression scheme as one complete suit so does not cause any changes in compression ratio. Two different approaches will be studied then well implemented to reach the aim, those approaches are Selective encryption and Chaotic encryption.

As shown in figure (1); the main involved steps are: **color transformation** to transforming RGB format into YUV color space format, **Discrete cosine transform** to transforming each 8*8 blocks from spatial to frequency domain. The majority of the DCT energy is concentrated on low frequencies like DC or the first AC coefficients, **quantization** by Quantizing DCT coefficients to the nearest integer value, **diffusion process** (change value of pixels) where the proposed selective encryption approach is applied on DC and the first three AC coefficients. Those coefficients are selected from each block and then encrypted using 4D chaotic system as given in equations:

$$\begin{aligned} X_1 &= a(x_2 - x_1) + x_2 x_3 x_4, \\ X_2 &= b(x_1 + x_2) - x_1 x_3 x_4 \\ X_3 &= -cx_3 + x_1 x_2 x_4, \\ X_4 &= -dx_4 + x_1 x_2 x_3 \end{aligned} \qquad \ldots.(1)$$

Here, x_1, x_2, x_3, x_4 are system trajectories and *a,b,c,d* are system parameters. When a=30, b=10, c=1, d=10, the system is hyper – chaotic[12].

Confusion process (change the position of pixel) based on 2D chaotic standard map as given in equations:

$$x_{k+1} = \left(x_k + y_k + r_x + r_y\right) \bmod \ (n)$$

$$y_{k+1} = \left[y_k + r_y + k_c \sin\left(\frac{2\Pi \ x_{k+1}}{n} \right) \right] \bmod (n) \qquad \ldots.(2)$$

Where (x_k , y_k) and (x_{k+1} , y_{k+1}) is the original and the permuted pixel position of an N × N image respectively. Where n is the image width and height, (r_x , r_y) is a random scan couple, and standard map parameter K_c is a positive integer[13].

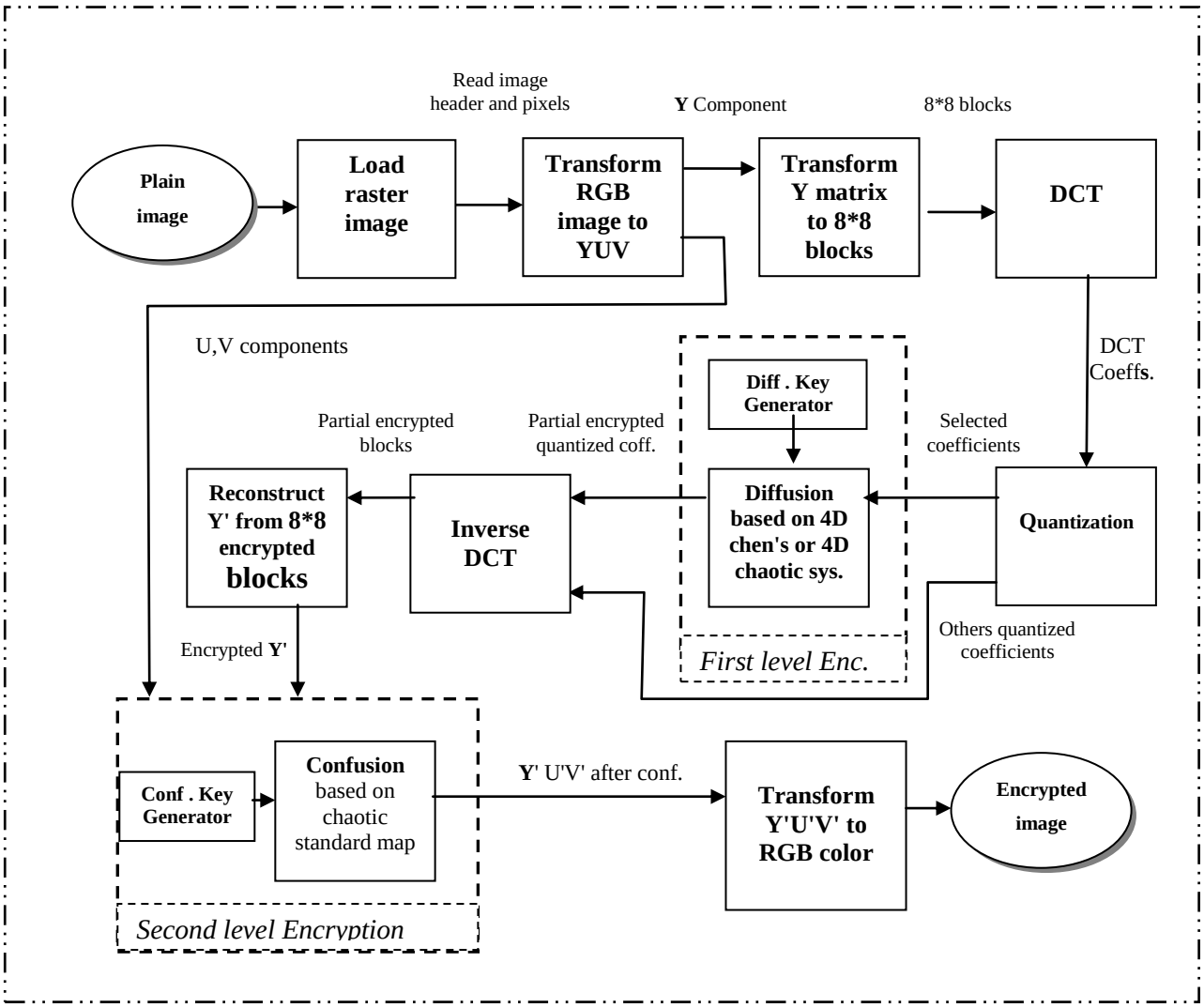


Figure (1) Encryption Module of Proposed Scheme

From these operations, can be conclude two levels of security one to decorrelate the relationship between adjacent pixels of plain image which is based on 2D Chaotic Standard map (confusion) and the other to decorrelate the relationship between the plain image and encrypted image which is based on 4D Chaotic Map (diffusion).

The diffusion process is decided to be performed on sensitive parts first, Then confusion is done later. The reason for such a decision is the majority of the DCT energy (sensitivity) is concentrated on low frequencies which is represented by the first DCT coefficients. Diffusing those sensitive parts will produce a sufficient and satisfactory level of security, while performing confusion later will produce an extra level of security according to the type of application.

V Experiment Results

In this work, many test sets have been conducted and the evaluation can be viewed from two aspects: General image encryption criteria and partial image encryption criteria. General encryption methods criteria are: Correlation coefficient, key space analysis, encryption quality, processing time, diffusion characteristics. While partial encryption methods criteria could be: tunability, encryption ratio, compression friendliness, error tolerance. These parameters can be tested as following below:

First- General Criteria Parameters

The standard images was taken as test images sample. And the important image encryption criteria are**:**

A - Correlation Coefficient

is a useful measure to judge encryption quality of any cryptosystem. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated.

Three functions are need to computes correlation coefficient these are[14] respectively, as

$$D(x) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))^2, \qquad \ldots\ldots(3)$$

$$E(x) = \frac{1}{N}\sum_{i=0}^{N}x_i, \qquad \ldots\ldots (4)$$

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=0}^{N}(x_i - E(x))(y_i - E(y)), \qquad \ldots\ldots (5)$$

From both the plain-image and the cipher image. The correlation coefficient of the pixel pair is then calculated as equation (6)

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}}, \qquad \ldots\ldots (6)$$

where x and y represent gray-scale values of two adjacent pixels in the image.

Tables (1) and (2) present correlation coefficient for both plain file and the cipher file of five standard images.

Table (1) Correlation coefficient for plain image.

IMAGES 256*256	VERTICAL	HORIZONTAL	DIAGONAL
Airplane	0.9221	0.9353	0.8832
Baboon	0.7830	0.8434	0.8297
Cameraman	0.9728	0.9498	0.8925
Lena	0.9643	0.9506	0.9353
Pepper	0.9676	0.9636	0.8935

Table (2) Correlation coefficient for cipher image.

IMAGES 256*256	VERTICAL	HORIZONTAL	DIAGONAL
Airplane	0.00759	-0.01275	0.0234
Baboon	0.01492	-0.03932	0.0262
Cameraman	0.00581	-0.00864	0.0114
Lena	0.00955	-0.01711	0.0231
Pepper	-0.0098	0.01966	0.0292

Obviously from the result of table (2), the values of correlation coefficient are encouraged. The reason is that chaotic algorithm offers features such as nonlinear, pseudo randomly and ergodicity.

In this scheme, the chaotic maps confusion property is in close relation with the security against statistical attack. if this chaotic map can confuse images to the one with random distribution, then it is difficult for statistical attack.

B- **Key Space Analysis**

A strong ciphering system depends on the strength of ciphering keys. Strength of keys depends on the key space. On the other hand the relationship between the encryption key and the cipher text should be as complex as possible so any change of one bit of the key will produce a total different cipher text.

To evaluate the strength of ciphering key, two kinds of tests are needed which are exhaustive key search test and key sensitivity test.

1-Exhaustive Key Search Test: An encryption scheme is considered secure if its key space is large enough. In this work, two layers of ciphering are applied which perform two processes : diffusion and confusion consequently.

Diffusion key space : is consist of 4 initial parameters (4- sub keys).The key space of each one is equal 256 bit, The attacker needs $4*2^{256}$ operations to find the exact key. If the attacker employs a 1000 million instructions per second (MIPS) computer to guess the key by brute force attack, the computational load in year is:

$$\frac{4\times 2^{256}}{1000\times 10^{6}\times 60\times 60\times 24\times 365} \rangle\ 1.2634583\times 10^{61}\ years$$

Which is considered very long time and computationally infeasible.

***Confusion key space*:** Consider an image of size N × N, The key space (use same keys for different iterations (*n*)) of chaotic standard map. Then the key space = **$[(N^2)!]$.**

Suppose the image size (256*256), then the computational load in year will be:

$$\frac{\left[(256^2)!\right]}{1000\times 10^{6}\times 60\times 60\times 24\times 365} \rangle\rangle\ 1.2634583\times 10^{61}\ years$$

The resultant key space is equal to the diffusion key space plus confusion key space. Then the security of the proposed scheme is capable of withstanding *brute force* attacks using today's computer.

2- Key Sensitivity Test: Another test with respect to secret key is the key sensitivity test that indicates how much an encrypted image is sensitive towards the change in the key. For a secure cryptosystem, a decryption algorithm will not decrypt cipher text image correctly. if there is a one bit difference between encryption key and decryption key.

Attacker tries to find out relationship between the plain-image and the cipher-image, by studying how differences in an input can affect the resultant difference at the output in an attempt to derive the key. Trying to make a slight change such as modifying one pixel of the encrypted images, attacker observes the changes of the plain-image.

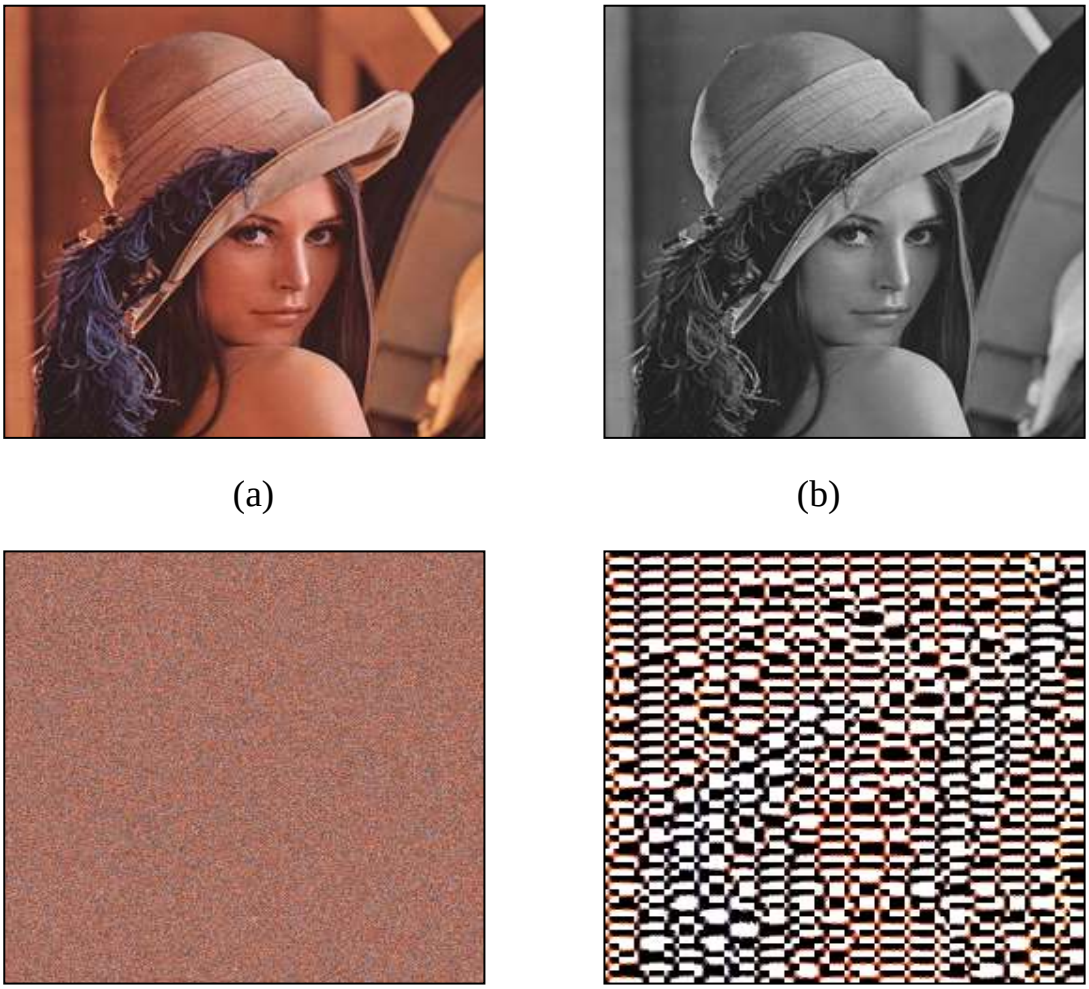
It means that ***large key sensitivity*** is required for highly secure cryptosystems. An ideal image encryption should be sensitive with respect to the secret key such that a single bit change in the key should produce a completely different encrypted image.

Key sensitivity of the proposed scheme is measured for diffusion and confusion keys by:

- **Sensitivity of diffusion key**

To evaluate the sensitivity of diffusion key " lena.bmp " image is tested giving the following parameters values :

Encryption key (in diffusion process) is: x_1 =0.5, x_2 =-0.3, x_3 =1.4, x_4=1.3, number of rounds(n) =30 and decryption key is the same as encryption key except for x_1=0.500005. The results are shown in figure (2).



(a) (b)

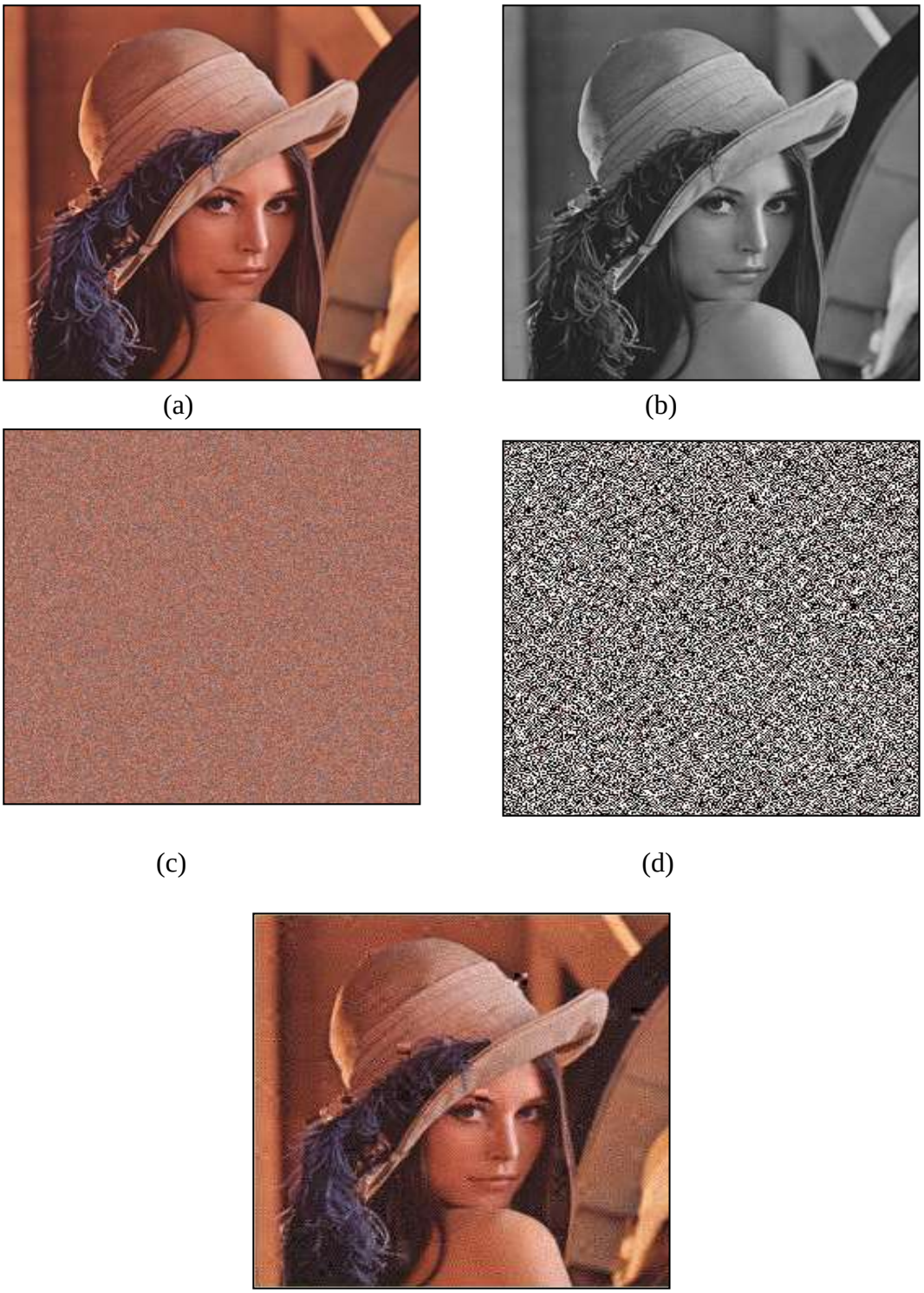
(c) (d)

Figure(2) (a) Plain image "lena.bmp", (b) gray scale "lena" image, (c) cipher images and (d) decryption image with only one bit is differ in x_1=0.500005.

obviously the test shows the cryptosystem is sensitive to any change in the key. besides it is sensitive to the any change in number of rounds or any initial values.

- **Sensitivity of confusion key**

Confusion key sensitivity is evaluated by setting the encryption key, for example. K_c =1000, the random scan couple(r_x =1, r_y=5), decryption keys are the same as encryption keys except for K_c = 1001, the number of rounds(m)=20. Inputting the same image " lena.bmp " the results will be as shown in figure (3)



(a) (b)

(c) (d)

(e)

Figure(3) (a) Plain image " lena.bmp "; (b) gray scale "lena" image; (c) cipher images and (d) decryption image with only one bit is differ in standard map parameter K_c = 1001;(e) decryption image with standard map parameter K_c = 1000

From above presentation, one concludes the proposed cipher scheme has an ***enough large key space*** and ***sensitive to a slight change of the key*** which make it impossible to obtain the plain image from decrypted one if any slight changes are occurred generate a completely different in decryption results and can't get the correct plain image.

C- **Processing Time**

Processing time for encryption and decryption is also an important issue in real-time multimedia application. To estimate the execution time of the proposed encryption scheme, different tests are performed on PC with 2.2 GB dual core processor and 3 GB RAM. Those tests choose different diffusion round (R_d) and confusion round values (R_c). Tests results of encryption time is shown in table (3) while table (4) presents decryption time calculation.

Table (3) Encryption speed test for different rounds of size 256 *256

IMAGE 256*256	ENCRYPTION TIME(SEC)					
	R_d=30	R_c= 4	R_d=30	R_c= 10	R_d=30	R_c= 32
Airplane	0.921		1.156		1.953	
Baboon	0.937		1.140		1.984	
Lena	0.906		1.140		1.968	
Pepper	0.906		1.156		1.968	
Cameraman	0.906		1.125		0.859	

Table (4) Decryption speed test for different rounds of size 256 *256

IMAGE 256*256	DECRYPTION TIME(SEC)					
	R_d=30	R_c= 4	R_d=30	R_c= 10	R_d=30	R_c= 32
Airplane	1.120		1.453		2.593	
Baboon	1.125		1.421		2.593	
Lena	1.109		1.421		2.593	
Pepper	1.109		1.421		2.593	
Cameraman	1.093		1.421		2.593	

Comparing the results of table (3) with (4), one can notice generally encryption and decryption time is suitable for real time application and the decryption execution time is greater than encryption time rate equal to (0.3 sec). The reason of such increasing because there is need to ultra operations to calculate the locations of each pixel which is (x, y) for each iteration before finding the original location of the same pixel in previous iteration.

From above results we conclude the proposed encryption scheme is of a ***high speed*** and ***flexible*** to different application especially real time systems.

D - Diffusion Characteristics of a Cryptosystem

Diffusion characteristics of an image encryption algorithm means that the output pixels of ciphertext image should depend on the input pixels of plaintext image in a very complex way. Diffusion characteristics can be evaluated by the following parameters:

1- Avalanche Effect

A small change in key or plaintext image should cause significant change in the corresponding ciphertext image. This property of scheme is known as avalanche effect.

Mean Square Error (MSE) is the cumulative squared error between two digital images and can be used to check the avalanche effect [15]. Let C1 and C2 be two ciphertext images whose corresponding keys are differ by one bit, then MSE can be calculated as :

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \left[C_1(i, j) - C_2(i, j) \right]^2 \qquad \text{.....(7)}$$

Where M, N is the width and height of digital images and C1(i, j) is gray scale value of pixel at grid (i, j) in cipher image C1 and C2(i, j) is gray scale value of pixel at grid(i, j) in cipher image C2. If the value obtained using equation (7) for MSE is > 30 dB, quality difference between two images is evident. Table(5), shows the results of MSE for the proposed cryptosystem.

Table (5) : Avalanche Effect(MSE results).

IMAGES	MSE
Airplane	42.24 dB
Baboon	42.35 dB
Cameraman	42.36 dB
Lena	42.36 dB
Pepper	42.37 dB

2-Number of Pixel Change Rate and Unified Average Change Intensity

For any encryption algorithm, it is desirable property that a small change in plaintext image should cause a significant change in the ciphertext image.

Two common measures are used to check the influence of a one pixel change on the overall image. These two measures are Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) [16].

NPCR can be represented in equation (8).

$$NPCR = \frac{\sum_{i,j}^{N,M} D(i,j)}{W \times H} \times 100\% \qquad (8)$$

The first measure NPCR finds percentage of different pixel numbers between the plaintext image and the ciphertext image can be calculated.

The second measure is Unified Average Change Intensity (UACI) determines the average intensity of differences between the two images. Mathematically UACI can defined as:

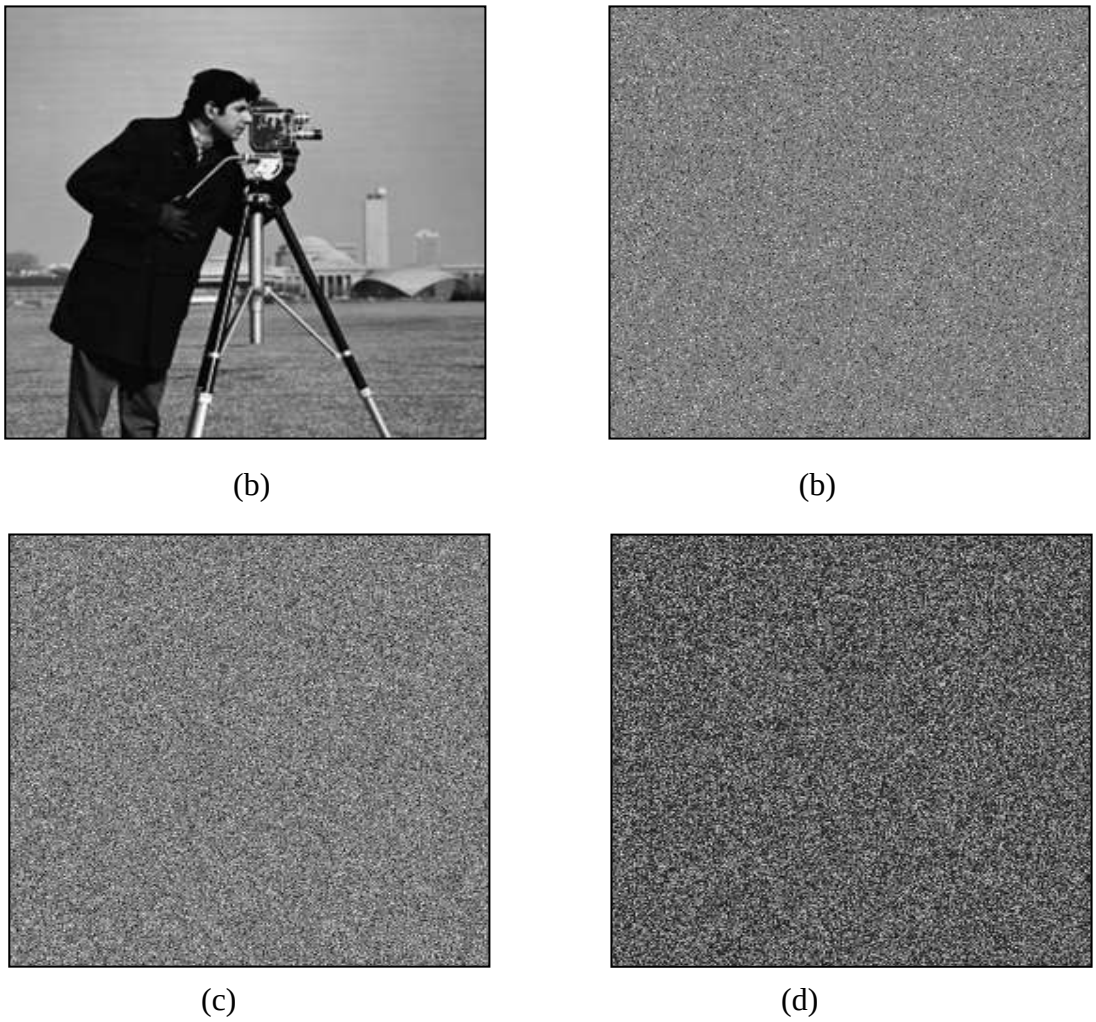
$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \qquad (9)$$

The higher value of NPCR and UACI, the better the algorithm is, as shown in table (6) .All tested images have NPCR near to 100 %.

Table(6): Shown the value of NPCR and UACI for proposed scheme.

IMAGES	NPCR %	UACI %
Airplane	99.991	51.40
Baboon	99.993	52.36
Cameraman	99.994	51.94
Lena	99.997	55.70
Pepper	99.996	54.14

As an example to clarify the effect of NPCR. Figure (4) shows the difference between two cipher images C_1 and C_2 whose plain images have a pixel difference at their lower right corner.



(b) (b)

(c) (d)

Figure(4) (a) Plain image, (b) and (c) cipher images whose corresponding plain images have one pixel difference only, (d) difference between cipher images shown in (b) and (c).

Second- Evaluation Criteria of Selective Encryption

Since the proposed scheme is designed to be compatible with compression technique so there is a need to add more specific criteria for this purpose. the following are explain this target.

- **Tunability**

It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Selective encryption algorithms based on static encryption parameters do not allow tunability. Tunability is a desirable property especially for content protection systems targeting different applications with requirements in terms of security, computational power, real time systems.

For these reasons the cipher scheme in this work is designed to be ***tunable***. In the design phase, two aspects are taken into consideration regard tunability. These were :

1. Designing multi layers of secrecy by satisfying first confusion or/and second diffusion properties.
2. According to the above point different ranges of values have been suggested to each input parameter of coding algorithm, depending on the need of the applied application parameter like number of iterations, positive integer (k_c), random scan couple, etc.

- **Encryption Ratio**

This criterion measures the ratio between the size of the encrypted part to the whole plain data size. Encryption ratio has to be minimized when selective encryption is applied. At the same time it should preserve a significant level of security[17].

In this work, the encryption ratio of cryptosystem equal to **(6.25%)** because only one DC coefficient and three AC coefficients are encrypted from each block (64 coefficients).

- **Compression Friendliness**

An encryption scheme is considered compression friendly if it has no or very little impact on data compression efficiency. Some encryption schemes impact data compressibility or introduce additional data that is necessary for decryption. It is desirable that size of encrypted data should not increase [18]. In this work, all steps required for compression are performed because they all needed to execute partial encryption process except compression coding like Huffman coding. The last one could be added without affecting the scheme.

usually steps required for compression / are :

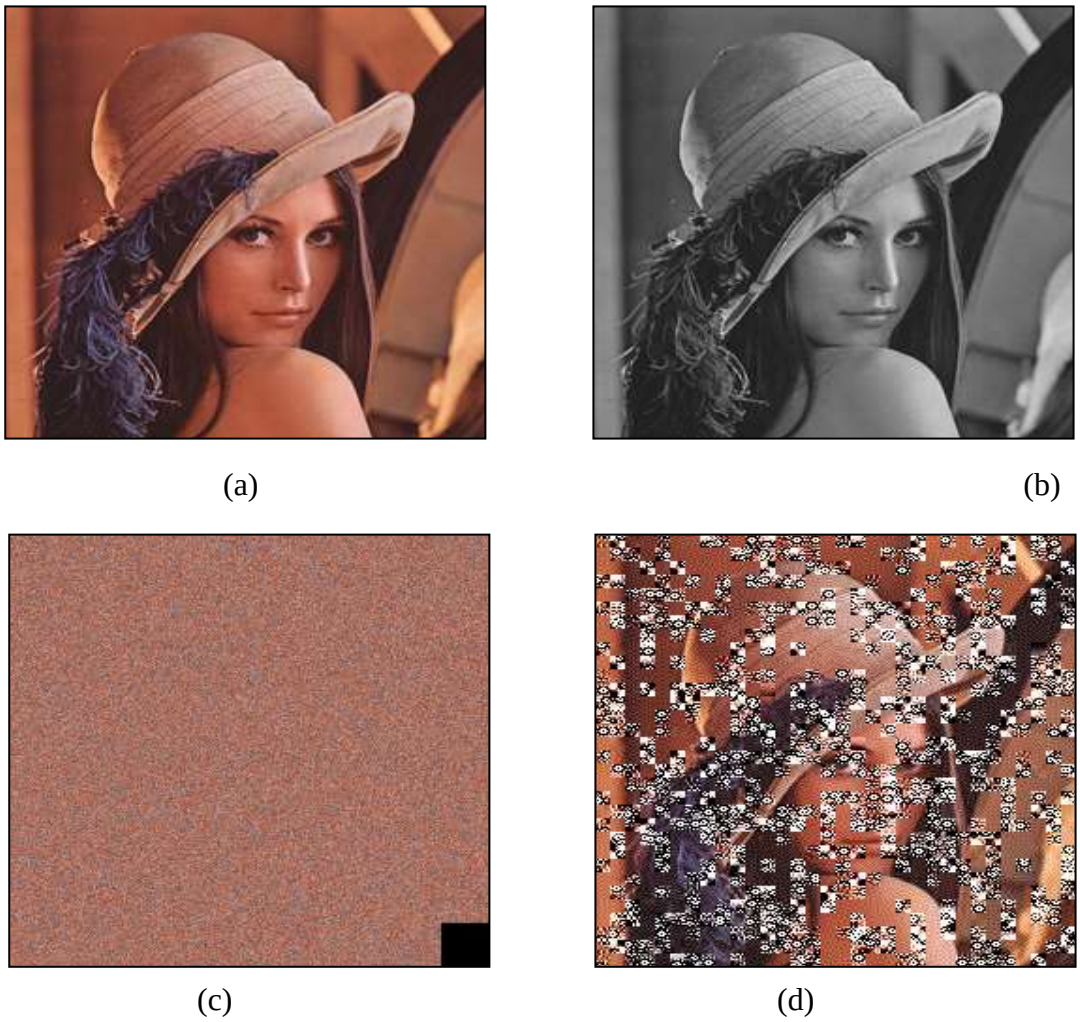
1. Read plain image.
2. Convert RGB color scheme to YUV scheme.
3. Decomposing Y component into 8*8 blocks.
4. Transforming each block to frequency domain by adopting DCT.
5. Quantizing DCT coefficients to the nearest integer value
6. Implement zigzag and Huffman coding.

Concluding, the proposed scheme has no impact on compression efficiency and the size of encrypted image not increase.

- **Error Tolerance**

A main challenge in selective encryption algorithms is to design secure schemes that are error tolerant.A single bit error that occurs in the encryption bit stream during transmission will propagate many other bits after decryption. This causes decoding failure or important distortion to the plain data at the receiver side[17].

As an example to clarify the effect of spot error in the encryption image during transmission and the result of decryption image show figure (5)



(a) (b)

(c) (d)

Figure (5) (a) Plain image, (b) gray scale " lena " image, (c) cipher images have spot error during transmission, (d) the result of decryption image.

From the above figure, due to diffusion property of the proposed scheme which has high avalanche properties (MSE > 42 dB) and according to the properties of chaotic systems with confusion and diffusion then the scheme is poor error tolerance

VI Conclusion

In this paper, The implementation of the proposed scheme based on chaotic algorithm has two operations, **diffusion** to decorrelate the relationship between adjacent pixels of plain image which is based on 2D Chaotic Standard map and the other **confusion** to decorrelate the relationship between the plain image and encrypted image which is based on 4D Chaotic Map. The proposed scheme provide high security, high speed, high visual degradation (VD), encryption ratio (ER) is equal to (6.25 %), compatible with compression and tunability where is tunable for set of applications like real time systems by tuned the parameters of confusion and diffusion. The experimental results show that the proposed scheme is computationally secure and it withstands different types of attacks such as brute force attack, differential attack, chosen-plaintext and chosen-ciphertext attacks.

References

[1] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law "A Fast Image Encryption Scheme based on Chaotic Standard Map" Internet Paper, Department of Electronic Engineering, City University of Hong Kong,2007.

[2] K.Sakthidasan @ Sankaran and B.V.Santhosh Krishna "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images" International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[3] Fonteneau C.,Motsch J., Babel M., and D'eforges O., "A hierachical selective encryption technique in a scalable image codec ", International conferences in communication, Bucharest, Romania 2008.

[4] B. Furht and D.Kirovski, editor, " Multimedia security handbook". CRC press, Boca Raton, Florida, 2005.

[5] K. Lala, B. Sami, A. Thawar, S. Zyad " Image Encryption Using DCT and Stream Cipher"; European Journal of Scientific Research; ISSN 1450-216X Vol.32 No.1, pp.47-57(2009)

[6] Latha Pillai, "Video Compression Using DCT", Available at www.xilinx.com, Xilinx, Inc, 2007.

[7] R. C. Gonzalez and R. E. Woods, "Digital Image Processing", published by Addison Wesley Longman, Delhi, 2001.

[8] M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," in Proceedings of Advanced Conceptsfor Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, Sept. 2002.

[**9**] Roueida Mohammed Yass, "A Cryptographic Scheme for color Images "; M.Sc. Thesis; Iraqi Commission for Computers & Informatic, Informatics Institute For Postgraduate Studies; 2006

[**10]** Ge Xin, Liu Fen-lin, Lu Bin, Wang, C " An Image Encryption Algorithm Based on Spatiotemporal Chaos in DCT Domain" Internet paper; Zhengzhou Information Science and technology Institute; Zhengzhou; China; IEEE 2010.

[11] Ping Xu, Jianjun Zhao, Dihua Wang " A selective image encryption algorithm based on hyper-chaos" Internet paper; Zhengzhou Information Science and technology Institute; Zhengzhou, China; IEEE 2011.

[12] Yun Cao, Runhe Qiu, Yuzhe Fu "Color Image Encryption based on Hyper-Chaos" information and Technology Department; Donghua University;Shanghai, China; IEEE 2009.

[13] J. Fridrich "Symmetric Ciphers Based on Two-dimensional Chaotic Maps" Int. J. Bifurcat. Chaos 8(6), pp. 1259-1284, 1998.

[**14**] Jawad Ahmad, Fawad Ahmad; "Effiiciency analysis and security evaluation of image encryption schemes"; published by International journal of video & image processing and network security;2012

[15] A.mohamed, G.Zaibi, and A. Kachouri, " Implementation of rc5 and rc6 block ciphers on digital images," in systems, singles and devices (SSD), 2011 8th international multi –conference on. IEEE.2011.

[16] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry, " Efficiency and Security of Some Image Encryption Algorithms" Proceedings of the World Congress on Engineering, London, U.K 2008.

[17] A.Massoudi, F.lefebvre, C.DeVlesschouwer, Bamako, " Overview on selective encryption of image and video :challenges and perspectives", EURASIP Journal on information security,2008.

[18] Jolly Shah and Vias Saxena, " Performance study on image encryption schemes", department of cs &IT, jaypee institute of information technology, Uttar Pradesh, India, IJCSI, July 2011.