AL-Qadisiya Journal for science Vol. 15 No. 2 year 2010

Anew algorithm for Encryption based on Application the Chaotic Key (EACK)

Mais'a Abdul Karim Nasir and Sahera Obaid Sead
Computer Dept/ Science College/ . Basrah University

Abstract:-

Encryption is designed to provide confidentiality, privacy and encryption images play an important role at the present time for use in modern data communication and transfer of images across the network between the sender and the recipient and storing images in databases and are confused by the encryption of information in special ways, if any person is able Decoding this information then we have we fail to achieve this goal. Current research presents a proposed technique for coding images for the production of encrypted image is completely different from the original image, the current method relies on the symmetric key encryption-based picture of the transfers from the matrix during the preparation of the private key used to encrypt the image and then transfers the application of sports, and use this key once again to disengage encrypted image

The aim of the current research is to present a proposal for the encryption technology of color pictures to get an encrypted totally different from the original image using the key to El Chaotic Key symmetrical key pad matrix transfers and lifting the encryption to encrypt the image. In this research was the use of Matlab language was in the implementation and designs the program.

1. Introduction

The fascinating developments in digital image processing and network communication during the past decade have created a great demand for real-time secure image transmission over the internet and through wireless networks. To meet this challenge, a variety of encryption schemes have been proposed [7].
Unfortunately, in many applications, conventional encryption algorithms(such as AES) are not suitable for image and video encryption. some video encryption algorithms are applicable to still images as well as videos[1,4].
The image encryption methods based on chaotic maps attract considerable attention recently due to their potential for digital multimedia encryption [2].
Proposed a Chaotic Key –Based Algorithm (CKBA) for image encryption .the security claims for CKBA have been vastly overestimated. not only is the complexity

of a cipher text-only attack against CKBA far lower than originally claimed, but chosen/known-plaintext attacks [9].

We proposed a novel image encryption algorithm, called EACK, based on the previously proposed method by Han Shuihua & Yang Shuangyuan[8].Our approach it is shown how to adapt certain matrix transformation to create a novel asymmetric block encryption. the main process in that system ,include six stages and each stage depends on the results of the previous phase are as follows: --

First: - Keyword is a read password and convert it to vector is then applied to the image.

Second: - the creation of the key analog and has the technology used in the key of Chaotic Key.

Third: - the application of the key on the image through the work of a logical match between the Key values and the values of the image.

Fourth: - the application of the separate Pocket (Discrete Cosine Transform)DCT conversion
on the image produced.

Fifth: - a process of silencing Quantization of the values of the image resulting from the conversion Pocket separate.

Sixth: - Conduct a survey crooked Zigzag Scan the values of the image resulting after silencing.

2. RELATED IMAGE CRYPTOSY &COMPRESSION

C-C Chang(2001) ,proposed a fast image encryption algorithm based on vector quantization(VQ),cryptography and number theorems in VQ,the image was first decomposed into vectors and the sequentially encoded vector by vector. Then traditional cryptosystem form commercial applications was used, for enhancing security and reducing the computational complexity of encryption/decryption, some number theorems were applied .VQ is an efficient approach to low bit-rate image compression THEREFORE SPEEDS UP the encryption process and achieve high security

J .Zhang(2006),image encryption methods can't meet the demands of encryption, S-DES system can encrypt the input binary flow of image ,but the fixed system structure and few keys will still bring some risks. dual image encryption algorithm based on S-DES and logistic map is proposed. The encryption speed of one image doesn't exceed one second. compared to traditional methods, it has some merits such as easy to understand, rapid encryption speed, large keys and sensitivity to initial value

Ercan Solak(2006),An encryption algorithm we demonstrate that a recently proposed chaotic encryption system is not invertible under double precision arithmetic. We also show that the algorithm incorrectly for some inputs

SAHRA&MAISA(2008),The research aims to proceed the process of encryption and the digital images by using a suggested method which uses the Discrete Cosine Transform and Some logical functions and programmatic applications. The rapid development of the communication network through the Internet and development of the electronic trade with spread of the digital media such as (images, audio, video) which can be got easily, copied, and distributed with another persons names. All these led to the needs of the authentication or copyright.. The suggested technique of transforming the desperate cosine is regarded as one of the important transforming methods and is wide spread, recently in the analytic field and treatment of the digital pictures.

It is another main process in that system, where it includes similar operations for encryptions of the interlude image but it begins and these operations proceed in reverse direction of the previous operations,
Proposed method has the advantages of several of them: simplicity, high secrecy, speed and accuracy. Has been reviewed several examples of normal and color photographs to demonstrate the technical performance of the proposed and the results were very good.
A new approach is suggested in this paper for fast and secure image encryption

3. Proposal Method

The first part of the encryption technology : -The process of image encryption Color image is encrypted by the proposed method the analysis of the image into three levels depending on the colors which results in the three matrices (a matrix of red and a matrix of green and blue matrix) and applying each stage of the three matrices are regular pictures directly to the application of stages as follows: -

First phase: keyword call Exchanger Transposed Keyword Mixed
This phase includes the process of encryption using a keyword (password) encrypted image, encryption which is the initial and the first stage in the integrated image encryption system and is done through the following steps: --

(1) The preparation of a keyword and that by reading a series of symbols or characters for example,
the following password: - S = 'My Keyword'
(2) Transform this series to correct matrix numbers by converting each character code (ASCII
CODE)
And its storage in the matrix U as follows: --
S = 'my keyword'

U = 109 121 32 107 101 121 119 111 114 100 ... .

Then we incorporate these values to get the correct matrix numbers as follows: --

U1 = 1 0 9 1 2 1 3 2 1 0 7 1 0 1 1 2 1 ... ...

(3) Be a new U2 matrix containing the numbers in the U1, but without repetition of any element (ie,

Neglecting the duplicate numbers in the U1) becomes U2 as follows: --

U2 = 1 0 9 2 3 7 4

(4) Assume that U1 is a matrix of numbers (0-9) compare the array with the U1 and U2 are

the Addition of the elements in the U1 and U2 are in the matrix at the end of U2 to get in the end, U2 matrix containing all the numbers (0-9) arranged given as follows: --

U1 = [0 1 2 3 4 5 6 7 8 9]

U2 = [1 0 9 3 2 7 4 5 6 8]

After the preparation of the key or a series of key figures, the next step will be the key to the Application of the image file to be encrypted through the following steps: --

(5) Read the image file regular or color (RGB) and stored in a matrix Xm×n, and we scaling image File size [128 ×128].

(6) We take each and every element of the matrix for the image, which is a number, composed of Three grades to a maximum, and then we figure to the derogation to orders get three numbers For Each element in the matrix for example: --

	a1	a2	a3
X(i,j)=254	2	5	4

(7) each and every one of these figures will be index of the matrix U2 that we obtained from Step 4, we extract the corresponding index for each of the matrix U2 as follows: --

b1=U2(a1)*100 b1=U2(2)*100 b1=0

b2=U2(a2)*10 b2=U2(5)*10 b2=20

b3=U2(a3)*1 b3=U2(4)*1 b3=3

Combine the three values to get the number b, which represents the matrix element of the new :

b=b1+b2+b3 , b=0+20+3 , b=023

(8) We alter the picture derived component X (i, j) with the number b, which we have received and Store the result in matrix RES and this is the final step in this stage.

After this stage, if we have now introduced the resulting image will note some of the image

Distortion and this distortion is the encryption of the initial image. It is noted that

Increasing the proportion of encryption at this point where the password composed of symbols Is more complex, leading to the complete disappearance of the features of the image was Selected word (password) for example

, (\,. / As; \ [ui]-=_+ bbbbbbbbbmmmmmpoiu =-+_., 123456)

Second phase: the creation of asymmetric key Will adopt at this stage, the key to the Chaotic Key [11] and we will make it to the image file a second step in the stages of encoding the image.

The preparation of the key steps of Chaotic Key:-

(1) Take the values of the primary variable X_0, Let $X_0 = 0.95$.

(2) We read the two keys Key1 and Key2, Let: - key1 = 113, key2 = 233

And read the values of α, a primary α = 3.9.

(3) Generate the matrix X, which represents the values that will get it from the application of

equation (1) as follows: --

$$X(i) = \alpha * X(i-1) * (1-X(i-1)) \quad \text{- - - - - - - - - - ---------- - --(1)}$$

Where: i=1...36

(4) The establishment of a new matrix(y), representing the private key Chaotic Key, by

Comparing the value of X with the value 0.5 on the basis of which the key is created in the

Matrix of the single 0 and 1 as follows: --

If X(i)>0.5

y(i)=0

else

y(i)=1

Thus, each element of X, thus ending the stage of preparation for the key

Third phase: the key to the application of the Chaotic Key

At this stage is to split the image file(P ×P) (8 ×8) blocks as follows: --

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) \text{ - - - - - - - } & f(0,7) \text{ - - - - - - - - - - } & f(0,m-1) \\ f(1,0) & f(1,1) \text{ - - - - - - - - } & f(1,7) \text{ - - - - - - - - - - } & f(1,m-1) \\ . & . & . & . \\ . & . & . & . \\ f(7,0) & f(7,1) \text{ - - - - - - - - } & f(7,7) \text{ - - - - - - - - - } & f(7,m-1) \\ . & . & . & . \\ f(N-1,0) & f(N-1,1) \text{ - - - } & f(n-1,7) \text{ - - - - - - - } & f(N-1,M-1) \end{bmatrix}$$

Fig. (1) the division of the picture to the matrix blocks (8 ×8)

Then we take the masses, each the size of the front (K ×K) (6 × 6) and store the matrix S and we are applying the private key, which Chaotic Key Houdini in the second phase of mass (K ×K) values for each image.

Bitxor (key,s (i,j))

When the key value of zero do conform to a logical XOR component of the image with the first key (key1), but if the job was the work of one matching logical XOR component image with the second key(key2), then the bloc to re-image and thus to keep all the values of the image.

Fourth Phase : the application of the conversion muddy Pocket separate (DCT) Pocket is a separate technology transfer and one of the most important techniques used in digital image processing, where the image is cut into equal-sized blocks N ×N (8 ×8) and each block is converted from the spatial to the frequency domain using the conversion equation Pocket separate dimensions of 2D-DCT and which represents the following equation(2): --

$$F(u,v) = 1/4\, C(u)\, C(v) \left[\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \cos((2x+1)v\pi/2n \cos((2y+1)v\pi/2n)\right] \quad \text{.....(2)}$$

Where

$$C(Z) = \begin{cases} 1/\sqrt{2} & \text{if } Z=0 \\ 1 & \text{if } Z \neq 0 \end{cases}$$

Where z is either u or v

x, y= 1,2 , ……,N-1

Implemented at the call of this equation approach DCT2 (S),Do any of the application of DCT on each block NxN where we note an increase in the presentation of the image distortion of the image.

Quantization stage

Quantization the process of being transferred to the data to convert data to a digital format or values closer to zero Detection. Where after the application of the DCT process on the image data for the image you'll need to convert them into digital format so we can deal with it in the rest of encryption. One of the objectives of this phase to have the additional compression to reduce the ratio of the number of gray levels required to represent the values of transactions in addition to an increase in

transactions and the elimination of zero-information that is not necessary for vision. And this operation is carried out using a special scale called quantization table , which is a matrix (8 ×8) Where the image is divided into blocks (8×8), and is divided by the values of the mass of the image on the values of the quantization table(1).

Table(1)Quantization Table

16	*11*	*10*	*16*	*24*	*40*	*51*	*61*
12	*12*	*14*	*19*	*26*	*58*	*60*	*55*
14	*13*	*16*	*24*	*40*	*57*	*69*	*56*
14	*17*	*22*	*29*	*51*	*87*	*80*	*62*
18	*22*	*37*	*56*	*68*	*109*	*103*	*77*
24	*35*	*55*	*64*	*81*	*104*	*113*	*92*
49	*64*	*78*	*87*	*103*	*121*	*120*	*101*
72	*92*	*95*	*98*	*112*	*100*	*103*	*99*

Fifth Phase : meandering muddy survey Zigzag Scan

Conducted the survey to all the crooked dealings of the image blocks, and the effect the order of the survey in the coding process as it takes the transaction frequency and low-lying, most of which are not zeros before the high frequency and, as in the figure(2).

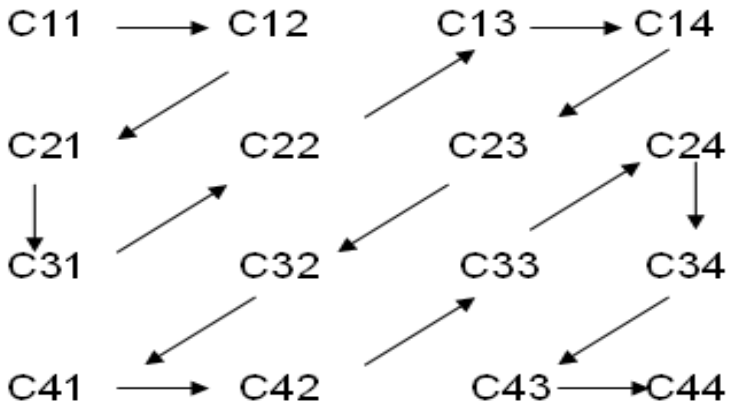


Fig. (2): Zigzag Scan

For the production of one-dimensional array and stored in the matrix product (D) as follows:--

D = [C11 C12 C21 C31 C22 C13 C14 C23 C32 C41 C42 C33 C24 C34 C43 C44]

The process of meandering through the Survey division of the picture to the 8x8 blocks and then call crooked approach to the survey:--

x=zigzag(s)

The second part of the encryption technology : The process of Decoding image Description

After the survey, which is a crooked last stage in the process of encoding the image and the encryption process to complete the full picture We will now stages decoding of the image, reversing the sequence of action steps to be negative as follows: --

1 - Survey phase reverse Altar c

Where we recall a crooked inverse function of the survey from which we get the picture before The survey, pictures post quantization a digital data: --

x = zig zag_inv (s);

2 - Contrary to a silencing

Stage in the application of reverse quantization will get the picture after the conversion process to get any Pocket image data transferred, not digital.

3 - Pocket reverse phase transformation

At this stage is the application of the transfer function of retrieval Pocket encryption and

Disengage the previous phase, a phase quantization to get to the stage prior to the silencing

Phase of the application of chaotic key, this stage is to call and call IDCT2 approach is applied to reverse the conversion.

d = idct2 (s)

4 - Contrary to the key stage of the application of Chaotic Key

At this stage, the key to cancel the application of the Chaotic Key and logical that the work of Matching between the key again and the image matrix.

Bitxor (key, res (i, j))

5 - Contrary to the application stage floor keyword

Are the values of the division of the image matrix from the previous step and the replacement of these values are the values of their positions in the matrix of the floor keyword U2, and thus cancel the impact of the floor on the image keyword. Following the completion of this step, the former will get the original image, i.e., we have decoded image encoded.

4. Test Result

For the purpose of testing the efficiency of proposed method we apply it to a set of color images has been used as a measure correlation to measure the compatibility of the image retrieved from the encryption process with the original image and the Peak Signal to Noise Ratio (PSNR) measure for calculating the difference between the original images and recovered.

5.Correlation

Measure the similarity between the association and the original image file recovered. The objective is to obtain the value of correlation approach to the one, Association known as the equation (3) the following: --

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

Where:

$I_1(r,c)$: is the value of the screen points in the (r, c) of the image described. While $I_1(r, c)$ is a valuable component of the image in (r, c) of the original image is defined as follows:

$$\bar{I}_1 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_1(r,c) \quad \text{... ...……..... (4)}$$

Where:

I_2 (r, c): is the value of the screen points in the (r, c) of the image described. I_2: is the rate of the retrieved image as:

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_2(r,c) \quad \text{.... .... …… (5)}$$

Where:

M: Height the Image

N: width the image

c, r: the number of rows and the number of columns.

For the color image must be retrieved for the three-color images taken in the calculation of the correlation . And the correlation calculated for each of the color image is due to the re-installation. The rate of these three correlations is used to generate the image associated with the re-installation of RGB. That the equation of the link to the image color is:

$$Corr_{RGB} = \frac{Corr_{red} + Corr_{green} + Corr_{blue}}{3} \quad \text{..... ...} \quad (6)$$

Where Corr red and Corr green and Corr blue (red link and link and link green blue),

respectively, are the correlations for each color layer and the correlation calculated by equation (3) above.

6. Scale of PSNR

Is, in fact, the method for calculating the amount of the difference between the original image and recovered image, as the picture element is the component of the recovered image is the original amount of the added noise, which is one of the most common standard And the calculation of the value of PSNR is as follows:

$$PSNR = 10 \log_{10} \frac{(255)^2}{MSE} \quad \text{.....(7)}$$

Where the rate of square error (MSE) is: --

$$MSE = \frac{1}{NXM} \sum_{X=0}^{N-1} \sum_{Y=0}^{M-1} [g(x,y) - f(x,y)]^2 \quad \text{.....(8)}$$

The measured PSNR of the unit (dB) decibels.

Where: --

f (x, y): is the original image.

g (x, y): the image is recovered.

Also for the color image must be a three-color image retrieval taken at the expense of the PSNR. And the value will be calculated for each of the color image is due to the re-installation. The rate of these three values is used to generate a margin of error for the image re-installation of RGB. The equation of the PSNR of the image color is: --

$$PSNR_{RGB} = \frac{PSNR_{red} + PSNR_{green} + PSNR_{blue}}{3} \quad \text{.....(9)}$$

Since the PSNR red and PSNR green and PSNR blue, respectively, is the rate of error for each color layer and calculated by the equation of PSNR above. The following table summarizes the results of the application of the current method of twelve pictures (Four of four BMP and JPG and four gray Correlations between the image and the original image encoded between the original images and recovered the difference between the original image and the encoded PSNR

Table (2) the results of applying the proposed method on regular and colored pictures

difference between the original image and encoded PSNR	Correlation between *the original image* and *image recovered*	Correlation between *the original image* and *image decoded*	Name image	Type image
28.6823	0.94239	0.010697	Allah	*JPG*
24.7982	0.95778	0.036758	Baby	
24.2841	0.98256	0.030936	Taj-Mahal	
27.7867	0.9733	0.036652	Girl	
28.5714	0.98934	0.031757	Allah Wa Akbar	*BMP*
28.4844	0.98225	0.01817	Red_baby	
24.7215	0.97651	0.036758	Malak	
27.5452	0.96838	0.024122	lena	
27.3497	0.93984	0.041915	Maka	GRAY SCALE
26.5446	0.9659	0.029077	Birds	
23.6139	0.93975	0.037466	Aqsaa	
23.6667	0.93587	0.01962	House	

The results of applying the system to color pictures JPG :-

Fig. (3) The results of applying the rules of the Taj-Mahal Photo

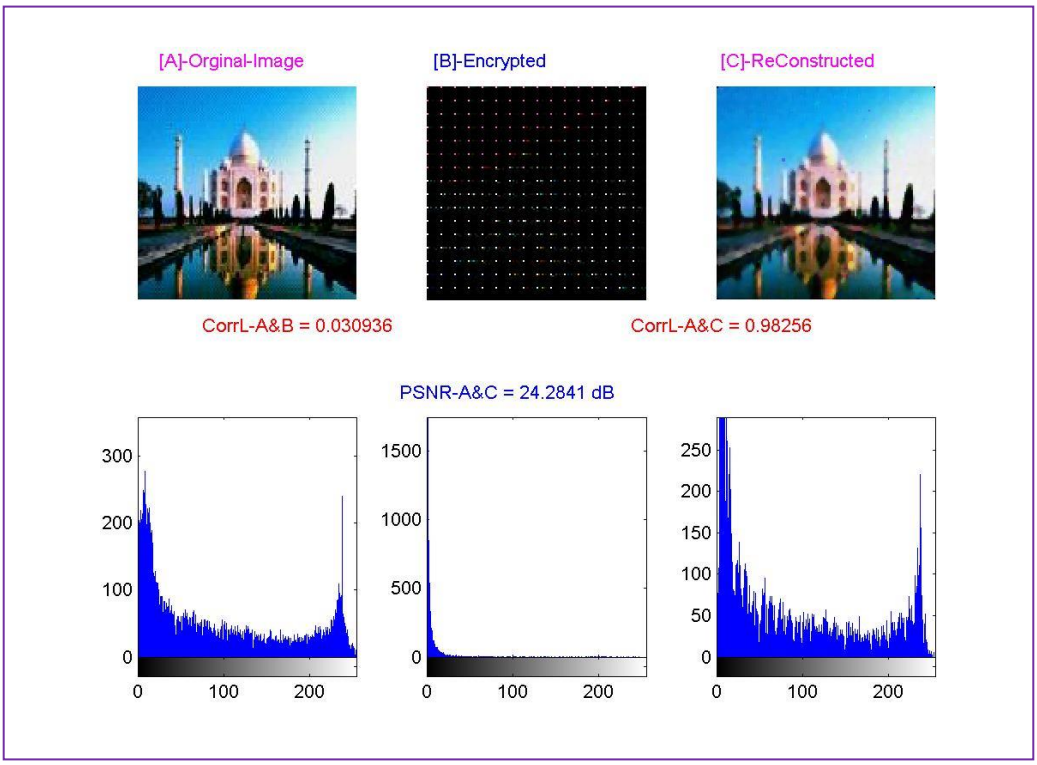
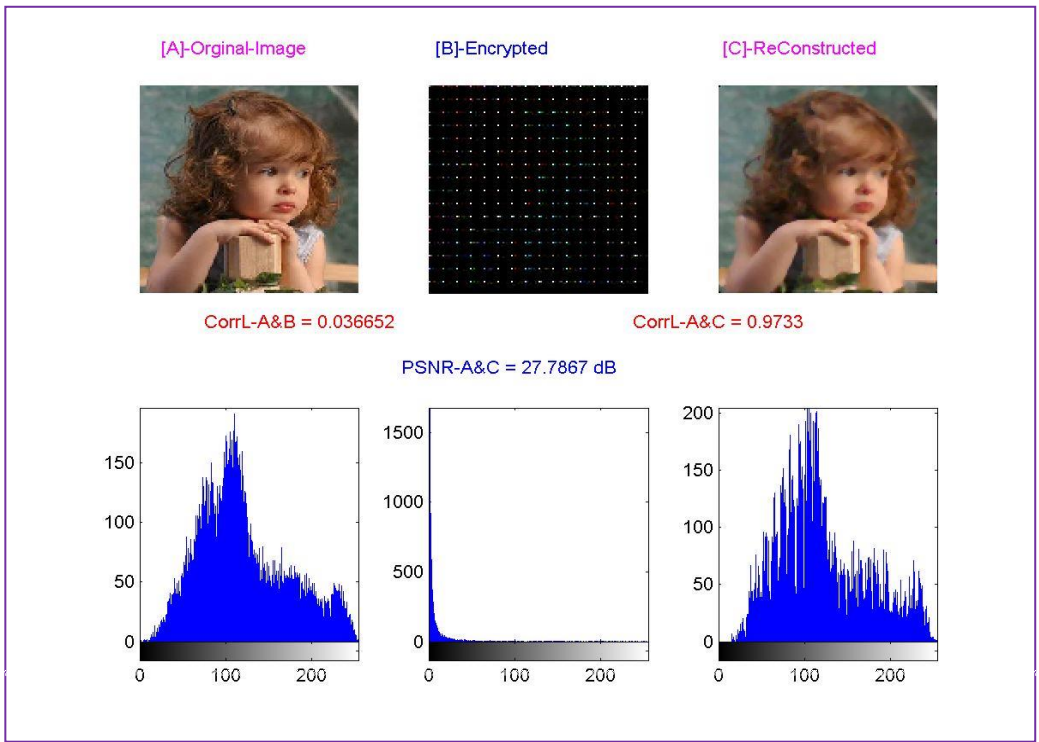


Fig. (4) The result



s of the application system on the photo Girl

Results of the application of the rules of the color images BMP :-

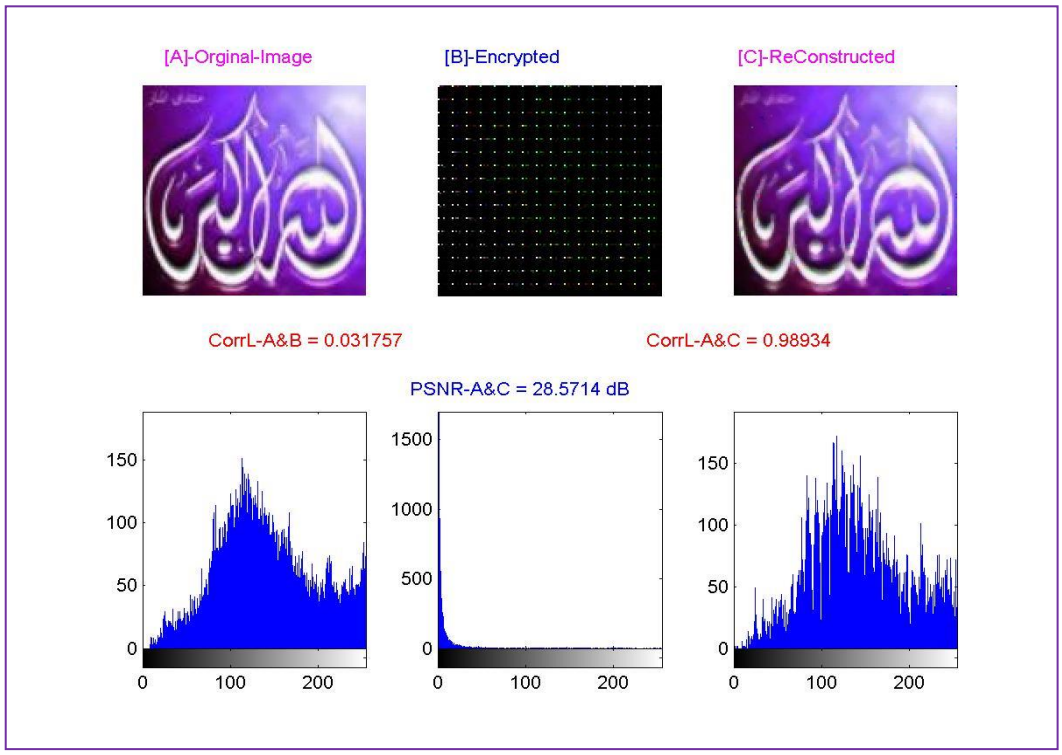


Fig. (5) The results of the application system on the image Allah Wa Akbar

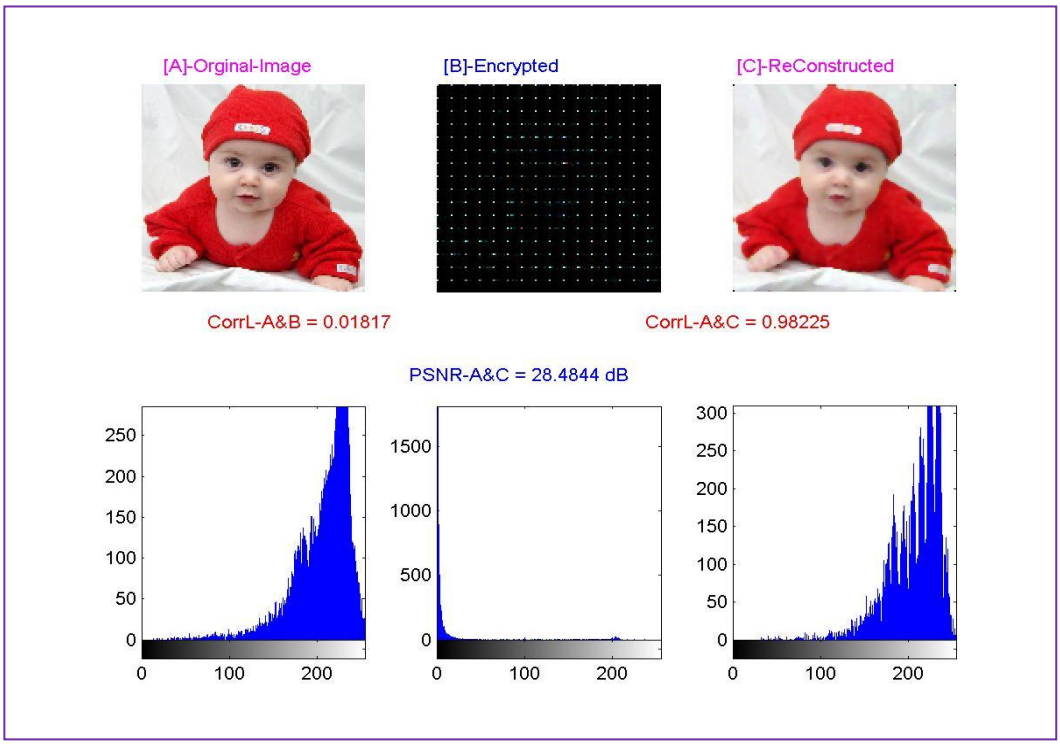


Fig. (6) The results of the application system on the image Red_baby

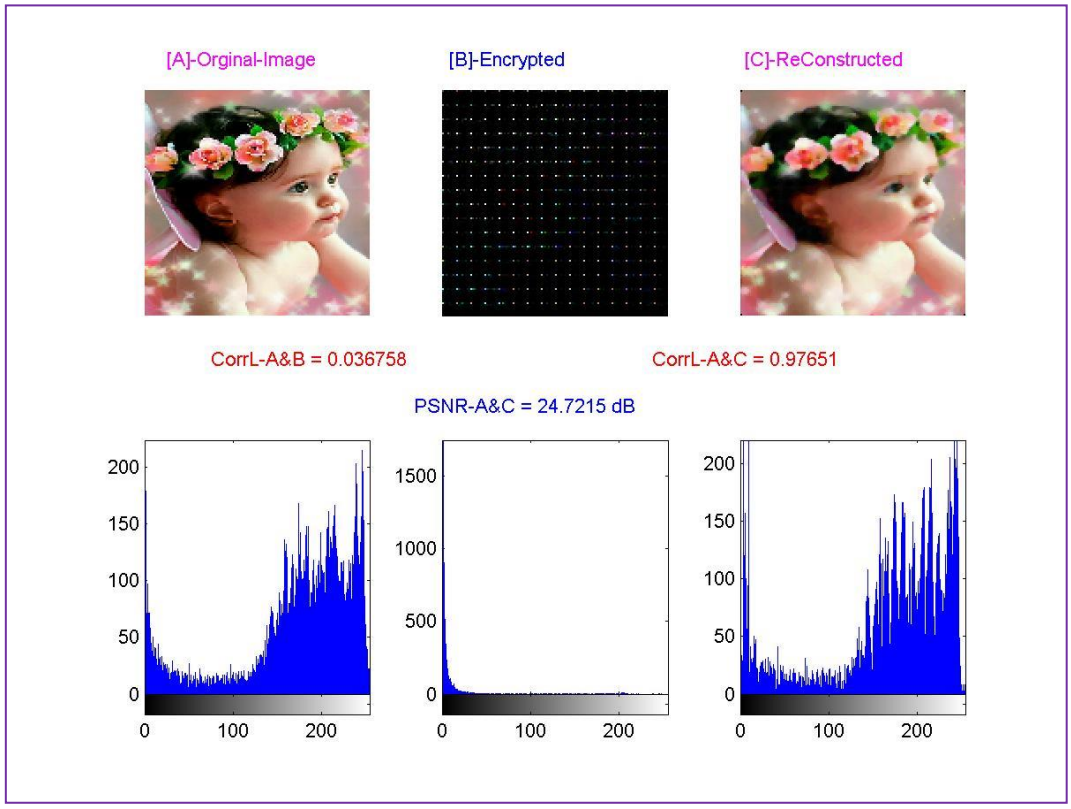


Fig. (7) The results of the application system on the image Malak

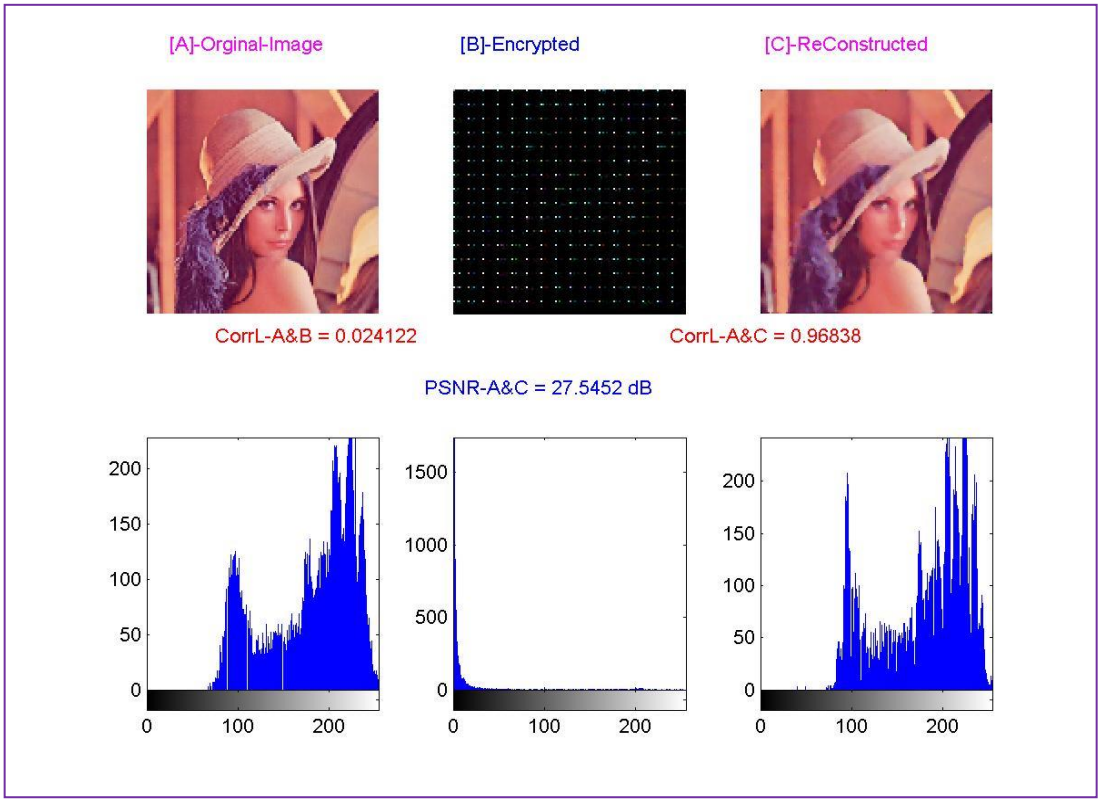


Fig. (8) The results of the application system on the image Lena

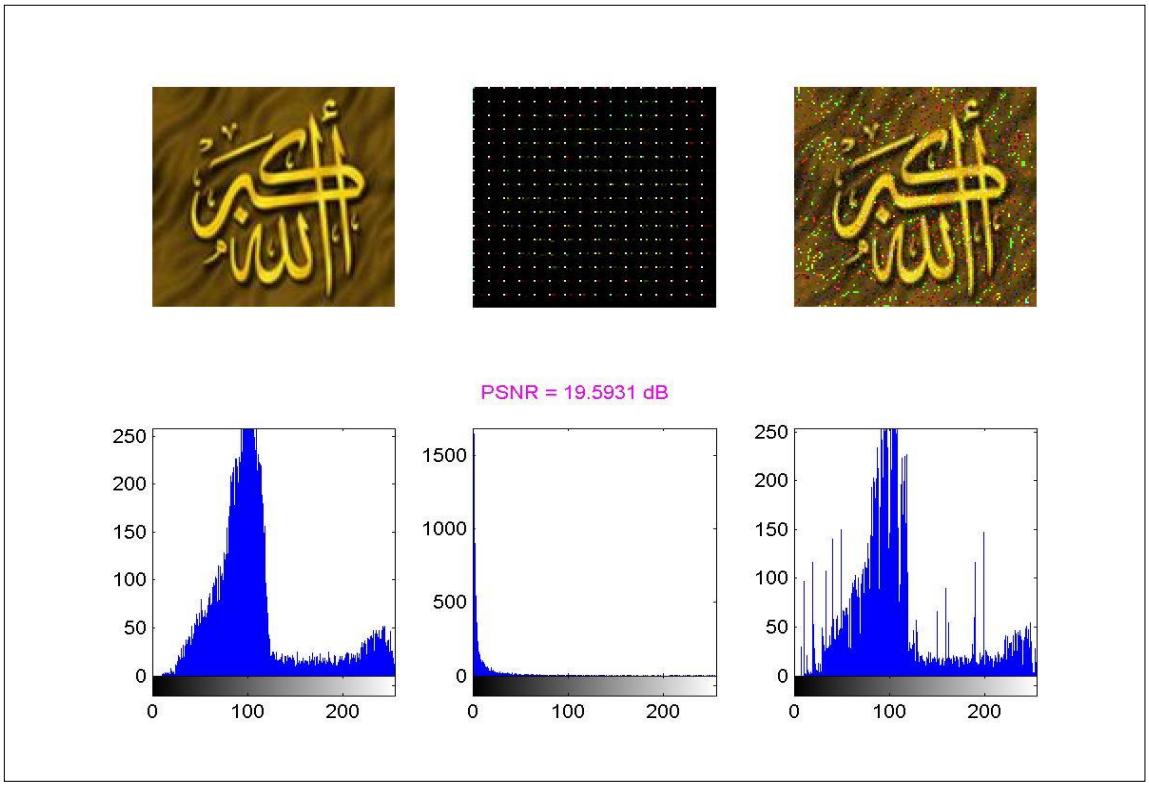


Fig (9) the results of the application system on the image Allah

Results of the application of the rules of the regular Photo Gray Scale :-

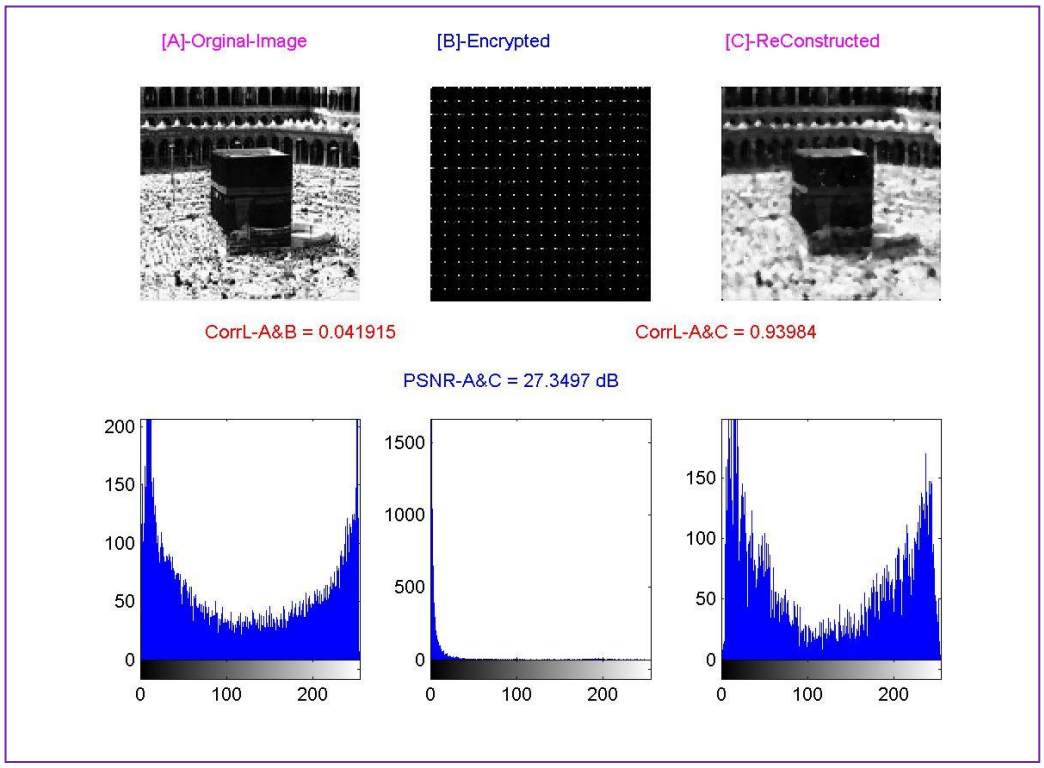


Fig (10) the results of the application system on the image maka

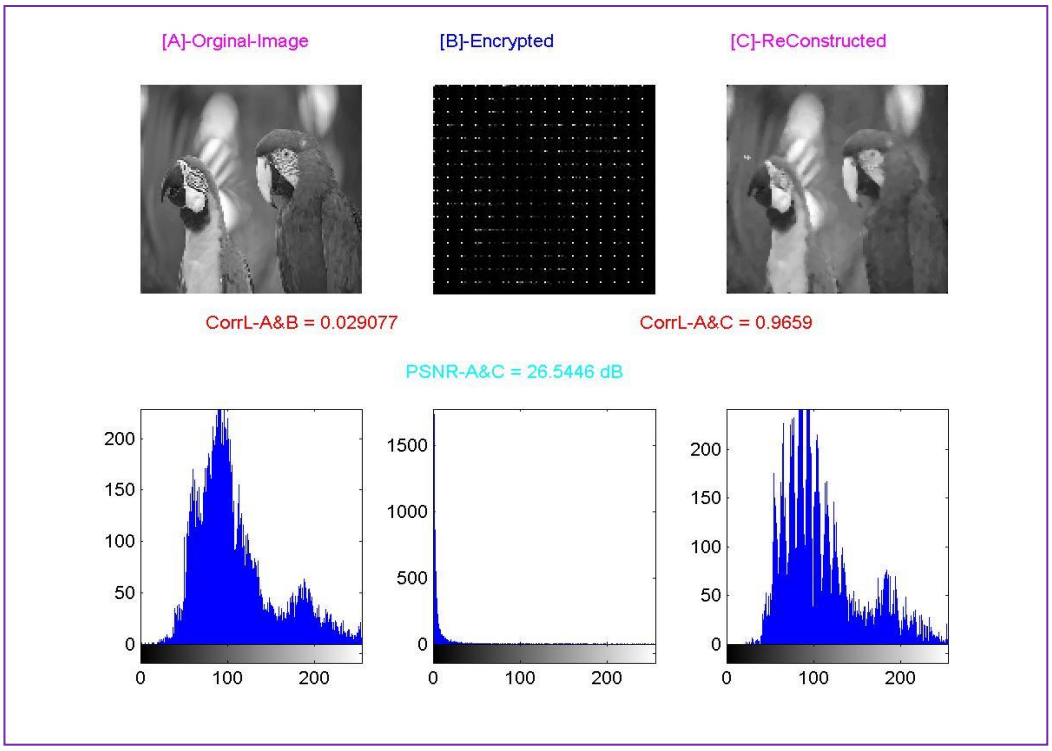


Fig (11) the results of the application system on the image Birds

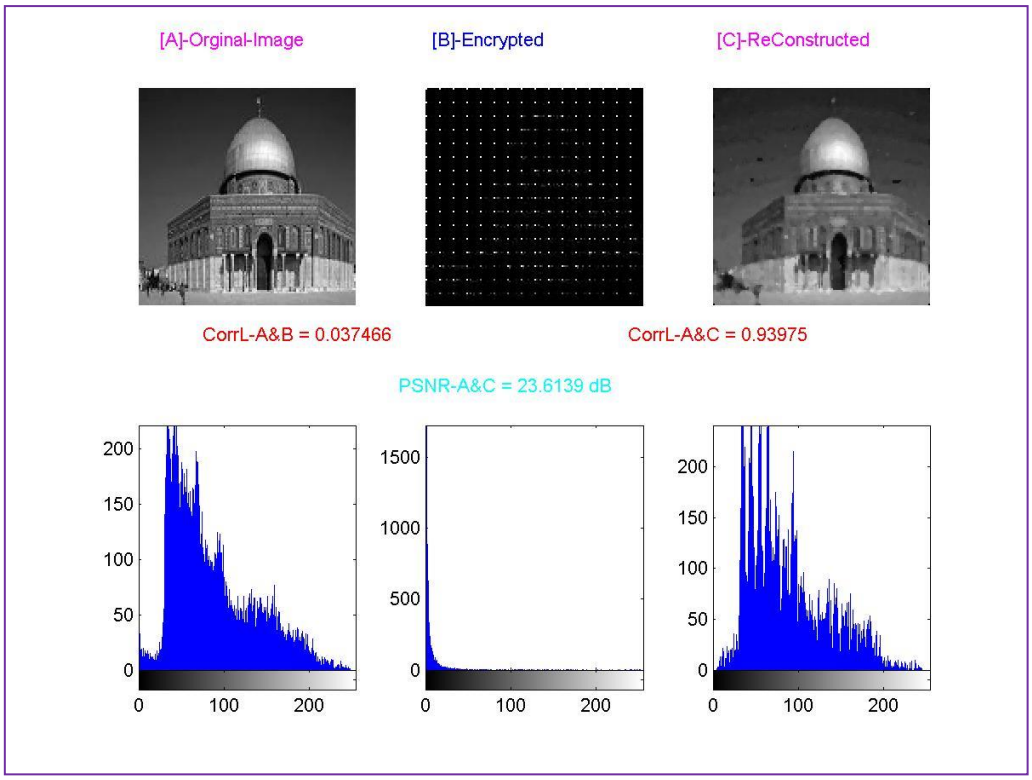


Fig (12) the results of the application system on the image Aqsaa

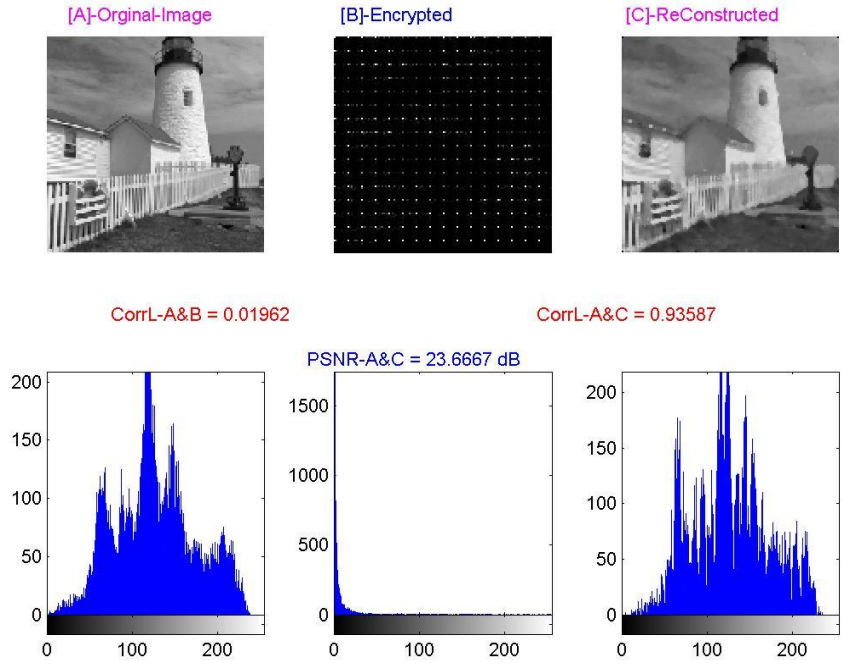


Fig (13) the results of the application system on the image house

7. Conclusion

Research technology to encrypt the Internet and the regular colored images by relying on asymmetric key-based matrix conversions. Presents the current And asymmetric-key encryption a method of encryption where encryption comes encrypted data using the same key and we have adopted this technology in the key . And asymmetric-key encryption is a method of encryption where encryption comes encrypted data using the same key and we have adopted this technology in the key of a key symmetrical, and therefore the conversion application Pocket separate DCT and Quantization and crooked survey on the values of The emerging picture of each stage, respectively.

We have noted from the results during the process resulting from the application of technical practice on a range of regular and colored pictures as follows:

1 - percentage of correspondence between the encrypted image and the original image very few (almost zero) and this ratio is good and shows the efficiency of the proposed method, where the percentage of similarity between original image and coded to be almost non-existent.

2 - percentage of correspondence between the original image is recovered, and 99%, and this percentage is very good that any proposed method can be regarded as a third-discredited methods of data as to maintain the contents of the original image well. Advantage of proposed method of high confidentiality, speed and simplicity compared to the sports complex ways, and the fact that this method is composed of several stages and each stage depends on the outcome of the previous stage, this way we can add new stages of technical development, or the deletion of a certain simplification without affecting the stages of pre-existing This demonstrates the flexibility of the proposed method of adjustment and future development.

8. References :-

[1] Baxes G.A., John Wiley & Sons,(1994), Digital Image Processing :Principles and Appellations , Inc ., USA

[2] Claire Topping, (2003). General Cryptographic Knowledge. "general_cryptographic_knoledge3"

[3] Chang C.C.,Hwang M.S., and Chen T.S.,(2001)"Anew encryption algorithm for image Cryptosystems".

[4] Daniel Socek, Shujun Li, Spyros S.Magliveras & Borko Furht Enhanced 1-D Chaotic Key- Based Algorithm for Image Encryption.

[5] Ercan Solak & Cahit Cokal,(2006)"Encryption and decryption of images with chaotic map lattices",Depatment of Computer Science and Engineering,Isik University,Istanbul TR 34980,Turkey.

[6] J Zhang,H E Ren,G S Xu and X Y Luo,"Chaotic Image Scrambling Algorithm Based on S-DES"College of Measurement-Control Tech&Communications Engineering,HarbinUniversity of Science and Technology,Harbin , 150080, China, Information and Computer Engineering College, Northeast Forestry University,Harbin, 150000,China.

[7] Guanrong chen,Yaobin Mao and Charles K 2004 Asymmetric Image Encryption Scheme Based on 3D chaotic cat maps

[8] Han Shuihua & Yang Shuangyuan (2005) An Asymmetric Image Encryption Based on Matrix Transformation "Ectitransaction on computer And Information Technology", ol.1, no.2, November 2005.

[9] Kirk Job-Sluder (2002), Cryptography: A guide to protecting your files for consultants, educators and researchers. Indiana University

[10] SAHRA&MAISA(2008),"Picture Encryption by Using Discrete Cosine Transform (DCT)"computer dept,Scince College,Basrah University.

[11] X Y Y,J Zhang ,H E Ren ,G S Xu and XY Luo (2006),Chaotic Image Scrambling Algorithm based on S-DES, College of Measurement-Control Tech & Communications Engineering, Harbin University of Science and Technology ,Harbin ,China.

AL-Qadisiya Journal for science Vol. 15 No. 2 year 2010

خوارزمية جديدة لتشفير الصور بالاعتماد على تطبيق المفتاح الفوضوي

ميساء عبد الكريم و ساهرة عبيد
جامعة البصرة/كلية العلوم/قسم علوم الحاسبات

الخلاصة

يهدف التشفير إلى توفير السرية والخصوصية ويلعب تشفير الصور دور مهم في الوقت الحاضر لاستخدامه في اتصالات البيانات الحديث ونقل الصور عبر الشبكات بين المرسل والمستلم وخزن الصور في قواعد البيانات ويتم التشفير بواسطة خلط المعلومات بطرق خاصة فإذا تمكن أي شخص من فك تشفير هذه المعلومات عندئذ نكون قد فشلنا في تحقيق هذا الهدف.

البحث الحالي هو عرض تقنيه مقترحه لتشفير الصور الملونة للحصول على صوره مشفره تختلف تماما عن الصورة الأصلية باستخدام مفتاح(Chaotic key) لتشفير وفك تشفير الصورة.