Fast And Secure Image Encryption System For Real Time Applications And Mobile Communications

نظام تشفير الصور سريع وآمن لتطبيقات الوقت الحقيقي واتصالات المحمول

Assistant Lecturer : Manaf Mohammed Ali
Karbala University

Abstract

The strength of image encryption systems are depending on confusion (change the pixel position) and diffusion(change the pixel value) and most of researchers separate these operations and perform these in cascading form with different algorithms, so there are some drawbacks in this cryptosystem and may be cryptanalyzed soon. In this paper proposed image encryption system based on chaotic map due to special properties of chaotic theory, such as pseudo-randomness, no periodicity and sensitivity to initial conditions. The two operations confusion-diffusion are processed in same loop based on two dimension chaotic standard map with different secret keys. Experimental results show that the proposed scheme has high security and computationally secure , it withstands different types of attacks such as statistical attack, differential attack and brute force attack and the processing time of encryption is high (0.29 second) which is suitable for mobile communication and real time applications

Keywords: *image encryption, Chaotic map, YUV color space , histogram*

الخلاصة

المتانة في انظمة تشفير الصورة تعتمد على التشويش (تغيير موقع عناصر الصورة) والنشر (تغيير قيمة عناصر الصورة) وأغلب الباحثين قد فصلوا بين هذه العمليات من خلال تنفيذها بشكل متتابع مع استخدام خوارزميات مختلفة ، لذا هنالك بعض نقاط الضعف في نظام التشفير أعلاه وممكن قد يكسر هذا النظام. في هذا البحث تم فرض نظام تشفير يعتمد على معادلة الفوضى وذلك للخصائص الخاصة في نظرية الفوضى مثل العشوائية وعدم التكرار والحساسية للظروف الاولية .لقد تم دمج العمليتين (التشويش- النشر) في نفس الدورة بالاعتماد على معادلة التشويش ثنائية البعد ولكن بمفاتيح سرية مختلفة. النتائج المختبرية اظهرت أن النظام المفترض يملك امنية عالية و (computationally secure) ويقاوم مختلف الهجمات مثل الهجوم الإحصائي و الهجوم التفاضلي وهجوم القوة المحكمة ،أن وقت التنفيذ للتشفير هو سريع جدا(0.29 ثانية) والذي يكون ملائما لتطبيقات الاتصالات الخلوية وتطبيقات الزمن الحقيقي .

i. Introduction

In recent years, the transfer of data by the use of communication media is drastically increases, data contains information in the form of text, image, and video. So the need of the protection of data is also increases, but this matter becomes important when the transmission media transfers high confidential data like military data, medical data and video conferencing etc.[1].

Digital images have been widely used for different applications, such as business، health service and military affairs. All the significant data should be encrypted before transmission to avoid eavesdropping. However, bulk data size, the correlations between adjacent pixels and high redundancy among the raw pixels of a digital image make the traditional encryption algorithms, such as DES, IDEA, AES, not able to be operated efficiently[2]. Therefore, designing another and specialized encryption algorithms for digital images has attracted much research effort. The field of chaotic cryptography has undergone tremendous growth over the past few decades. The primary motivation of employing chaotic systems is its simplicity in form and complexity in dynamics.

The intrinsic properties of chaotic systems, such as ergodicity, sensitive to the initial conditions and control parameters, are analogous to the permutation(confusion) and diffusion properties specified by Shannon[3]. Thus makes it natural to employ chaotic systems in image encryption algorithms [4]. Therefore, chaotic cryptosystems have more useful and practical applications

The confusion–diffusion structure becomes the basis of many chaotic image encryption schemes since Fridrich developed a chaos-based image encryption scheme of this structure in 1998[5].

In response to the aforementioned challenges in protecting image content, the aim of the proposed scheme in this paper is specially oriented towards designing and implementing a secure, fast image encryption and suitable for different applications like online applications and mobile communication.

ii. Previous Works

Different methods have been proposed in image encryption based on chaotic map, Musheer Ahmad [6] proposed algorithm of Encryption of Images Using Chaotic Mapping, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map After that the shuffled image is encrypted using chaotic by one-dimensional Logistic map, in spite of the cryptosystem is secure and the correlation is very low, one of the weakness points are used cat map which has the periodicity problem(eventually the pixel positions will return to their original positions after number of iterations) and the key space is not enough.

Ge Xin et al.'s. [7] proposed an image encryption algorithm based on spatiotemporal chaos in DCT(discrete cosine transform) domain to pass the problems 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, from analysis and experiments that the scheme can resist chosen plaintext and cipher text attacks but the main drawbacks are a loss in date and the decryption image is not similarity to encryption image because DCT and quantization which loss in data and the speed of encryption is slow because the delay time required to convert image from spatial domain to frequency domain by DCT.

Kamlesh Gupta and Sanjary Silakari [8] proposed a technique for color image encryption using chaotic map instead of traditional technique which provides operations like confusion, diffusion by using cascading 3D standard and 3D cat map finally the image is encrypted by performing XOR operation on the shuffled image and diffusion template, this system is secure and immunity to different attacks like statistical attack and brute force attack, this cryptosystem is computationally complex and the weakness in the periodicity of cat map .

Jean kapkop and Joseph Effa [9] proposed chaotic image encryption scheme based on the generation of large permutation and diffusion keys, logistic map chaotic to shuffle the pixel positions without changing the pixel values and at diffusion shuffled image is split in n sub-images and the combination of PWLCM (piecewise linear chaotic map) shuffled image is split in n sub-images and the combination of PWLCM (piecewise linear chaotic map) with solutions of LDE (linear Diophantine equation) are generated to mask the pixels in each sub-image, the experimental results appeared the algorithm has a satisfactory security level and sensitive to initial key parameters.

To overcome for some mentioned problems, the suggestion scheme processed these problems based on 2D chaotic standard map which has more special features like large key space, without periodicity problem and solve the first value of image or 2D matrix for image by using random scan couple(r_x , r_y) which cannot solve in other maps, it has more key parameters than cat map or logistic map. The system is high sensitive to key parameters specially the value and the position of pixels are change in parallel or in the same loop, furthermore the simplicity design with less hardware requirements.

iii. Introduction To Chaos Theory

Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudo-random property and non-periodicity as the chaotic signals usually noise-like, etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. The characteristics of chaotic signals make chaos system an excellent and robust cryptosystem against any statistical attacks. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods. In present years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques to meet the demand for real-time image transmission over the communication channels. Therefore, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic systems have been proposed [10].

Two general principles which guide the design of practical algorithms are diffusion and confusion. Diffusion means spreading out of the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this idea is to spread the influence of a single key digit over many digits of ciphertext. Confusion means use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext[11].

iv. YUV Color Space

The color sensitive area in the Human Visual System (HVS) consists of three different sets of cones and each set is sensitive to the light of one of the three primary colors: red, green, and blue. Consequently, any color sensed by the HVS can be considered as a particular linear combination of the three primary colors. In RGB color representation system, a color is produced by adding three primary colors: red, green, and blue (RGB) **[**12**]**.

The RGB model is used mainly in color image acquisition and display. In color signal processing including image and video compression and encryption, however, the luminance – chrominance color systems (like YUV or YCbCr) are more efficient and, hence, widely used. This has something to do with the color perception of the HVS.

YUV representation, describes luminance and chrominance components of an image. The luminance component(Y) provides a gray scale version of the image, while two chrominance components(U,V) give additional information that converts the gray scale image to a color image**[**12**]**.

The reason for using the YUV system is that the human visual system (HVS) is less sensitive to chrominance or color information than to the luminance information, where Y contains more than 90% of the information of data. The chrominance signals can therefore be represented by a lower resolution than the luminance without significantly affecting the visual quality [13].

For the above reasons, In this paper we used diffusion operation (changes the value of image pixels) for Y component because it contain majority of image information and used confusion operation (changes and shuffle the position of the image pixels) for all components(YUV). The exact transformation from RGB to YUV representation, specified by the CCIT 601 standard, is given by the following equations:

$\mathbf{Y = 0.299R + 0.587G + 0.114B}$ **….. (1)**

$\mathbf{U = 0.564(B - Y)}$ **…. (2)**

$\mathbf{Y = 0.713(R - Y)}$ **…..(3)**

v. The Proposed Scheme

The important criteria for any cryptosystem are the security for this system which can immunity for different types of attacks like statistical, differential attacks and the speed for this system .The main objective of this work is to design and implement fast and secure image encryption scheme for confidentiality purpose which can be applied in real time systems and to solve the weakness, drawbacks of some previous chaotic image encryption schemes. Two different operations will be studied then well implemented to reach this aim. ***firstly*** to decorrelate the relations between the adjacent image pixels(confusion)which applied for (Y,U,V) components and ***secondly*** to decorrelate the relations among the plain image and cipher image(diffusion)which be applied for(Y) Component .In this work ,the permutation-diffusion operation occurred at the same time or in the same loop to minimized the time for encryption , reduce the hardware requirements.

In other side, the secret keys for chaotic map which used for pixels permutation also can be used for diffusion but in different values therefore the key space is large for this reason.

As shown in figure (1); the main involved steps are: color transformation to transforming RGB color space into YUV color space format and then applying encryption techniques (**diffusion and confusion**) based on 2D chaotic standard map

as given in equations:

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

$$\mathrm{y}_{k+1} = \left[\mathrm{y}_k + \mathrm{r}_\mathrm{y} + \mathrm{k}_c \sin\left(\frac{2\Pi \quad \mathrm{x}_{k+1}}{\mathrm{n}} \right) \right] \bmod (n) \qquad \text{….(4)}$$

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[14].

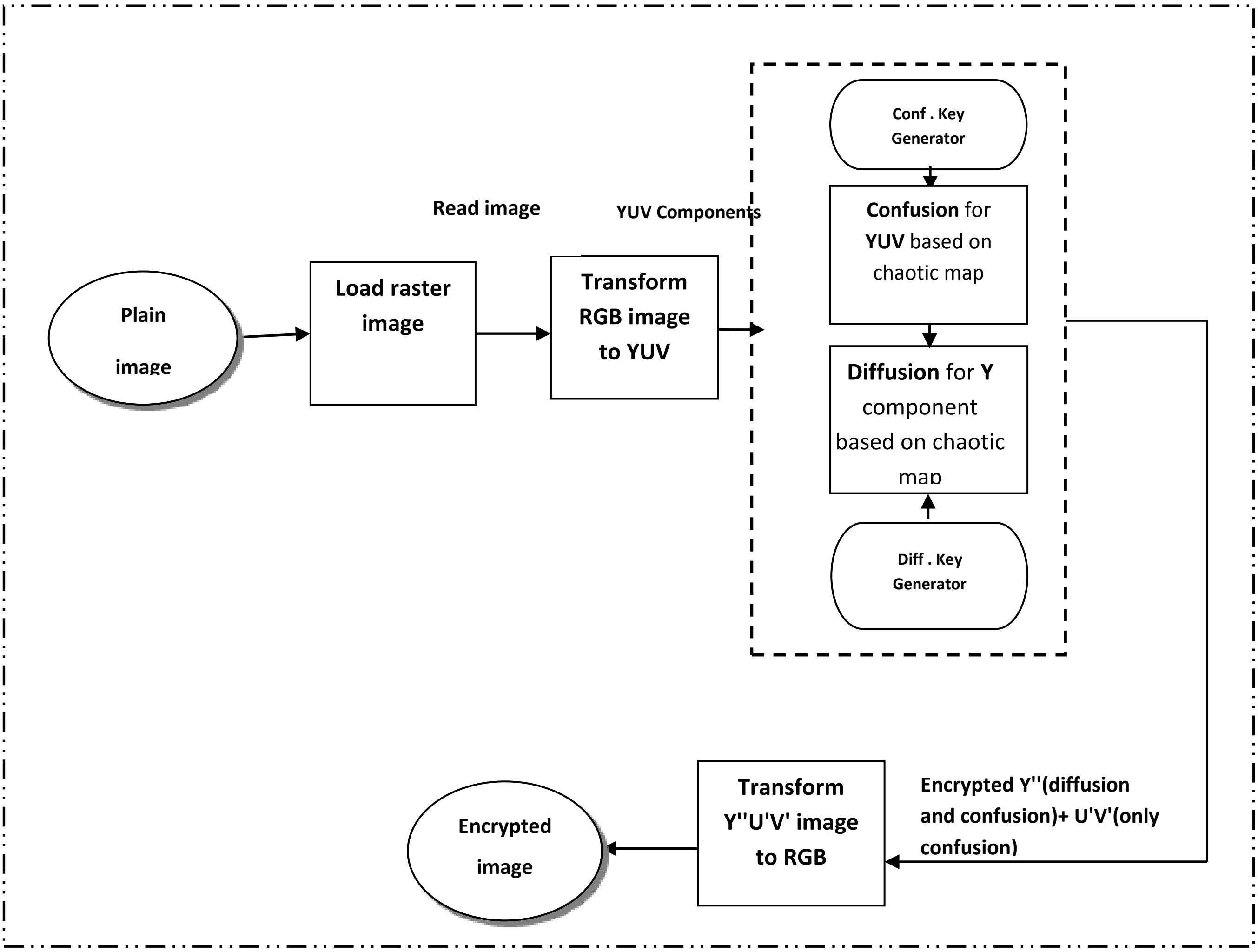

Plain image
Read image
Load raster image
YUV Components
Transform RGB image to YUV
Conf . Key Generator
Confusion for YUV based on chaotic map
Diffusion for Y component based on chaotic map
Diff . Key Generator
Encrypted Y''(diffusion and confusion)+ U'V'(only confusion)
Transform Y''U'V' image to RGB
Encrypted image

Figure **(1)** Encryption Module of Proposed Scheme

vi. **Experiment Results**

The encryption algorithms are implemented under visual basic 2008 and different images (Cameraman, Lena, Airplane) are taken as an example in the experiments. Many test sets have been conducted and the evaluation can be viewed as General image encryption criteria. General encryption methods criteria are: Correlation coefficient, key space analysis, processing time, encryption quality.

A- Correlation Coefficient

A correlation determines the relationship between two variables. In other words, correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem[15]. Any image cryptosystem is said to be good, if encryption algorithm conceals all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated.

If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero.

The correlation coefficient of the pixel pair is then calculated as in equations

$$D(x)=\tfrac{1}{N}\sum_{i=0}^{N}(x_i-E(x))^2,\quad E(x)=\tfrac{1}{N}\sum_{i=0}^{N}x_i, \qquad \text{...... (5)}$$

$$\operatorname{cov}(x,y)=\tfrac{1}{N}\sum_{i=0}^{N}(x_i-E(x))(y_i\ -E(y)), \qquad \text{...... (6)}$$

$$r_{xy}\ =\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}, \qquad \text{.......(7)}$$

Where x and y represent gray-scale values of two pixels in the same place in the plaintext and cipher text images. D(x) is variance at pixel value x in the plaintext image and Cov(x,y) is covariance at pixels x and y for both the plain-image and the cipher image. Tables (1) and (2) present correlation coefficient for both plain image and the cipher image of four 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

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

From the above tables (1,2), the large and clearly difference between two tables. The values of correlation coefficient in the cipher image is low and approach to zero which mean the encryption scheme conceals all attributes of a plaintext image and appear to random image. When the value of correlation is close to zero then the chaotic map can confuse images and hidden all attributes of this image and change it to random distribution, then actually it is difficult against statistical attacks because this attack depend on correlation of adjacent pixels of image.

B- Key space analysis

Any encryption system depends on the strength of keys generator or key parameters and the strength of keys depends of key space, therefore the relationship among the encryption key and the encryption text should be as difficult as possible so any change of encryption keys will produce a total different cipher text.

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

1) **Exhaustive Key Search Test:**

The encryption system is considered secure if its key space is large enough, two levels of ciphering are applied which perform two processes : confusion and diffusion which occurred at the same loop.

❖ **Confusion and diffusion 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. Where these operations have same map(standard map with different parameters)Then the security of the proposed cryptosystem is capable of withstanding brute force attacks using today’s computer.

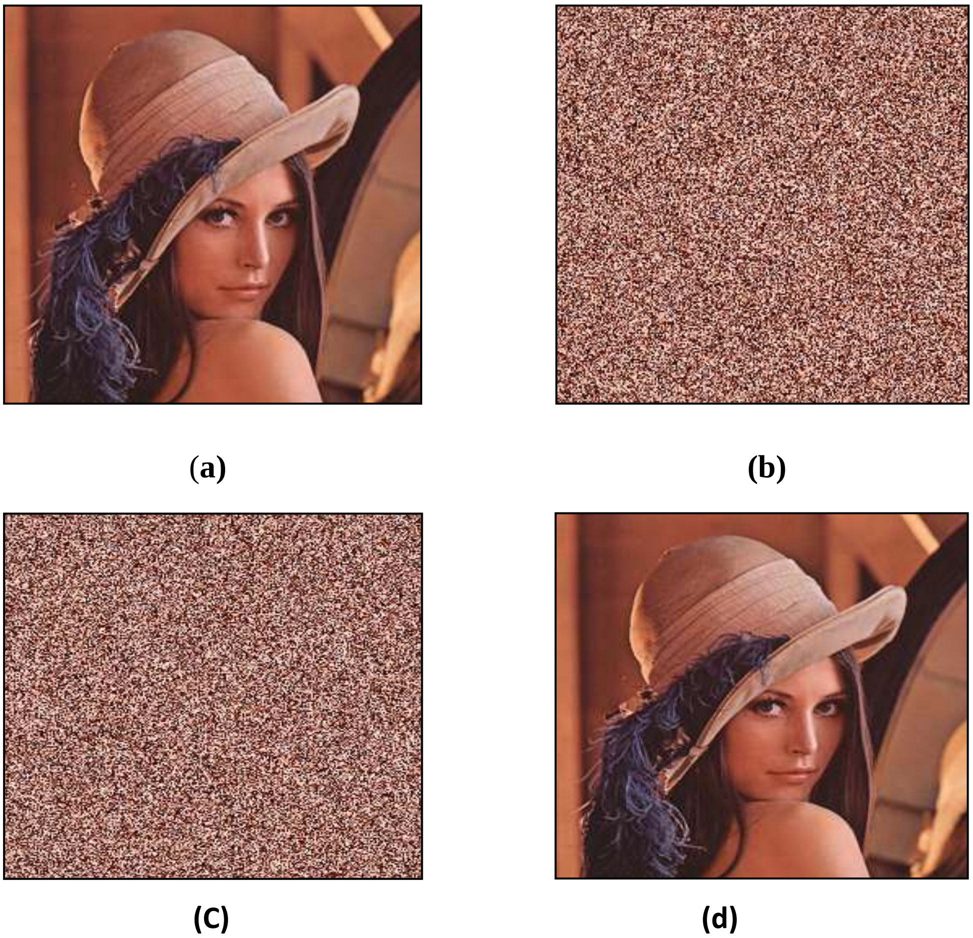
2) **Key Sensitivity Test:**

The sensitivity test means the sensitivity of an encryption keys test. The cipher is good when the slight difference in the keys should cause the great changes in the cipher texts. 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. Perfect 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.

- **Sensitivity of encryption key(diffusion or confusion keys)**

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

Encryption key (in confusion process) is: for example. Kc =999, the random scan couple(r_x =3, r_y=5), decryption keys are the same as encryption keys except for Kc = 1000(the difference is equal = 0.001), the number of iterations =10. Inputting the same image " lena.bmp " the results will be as shown in figure (2)

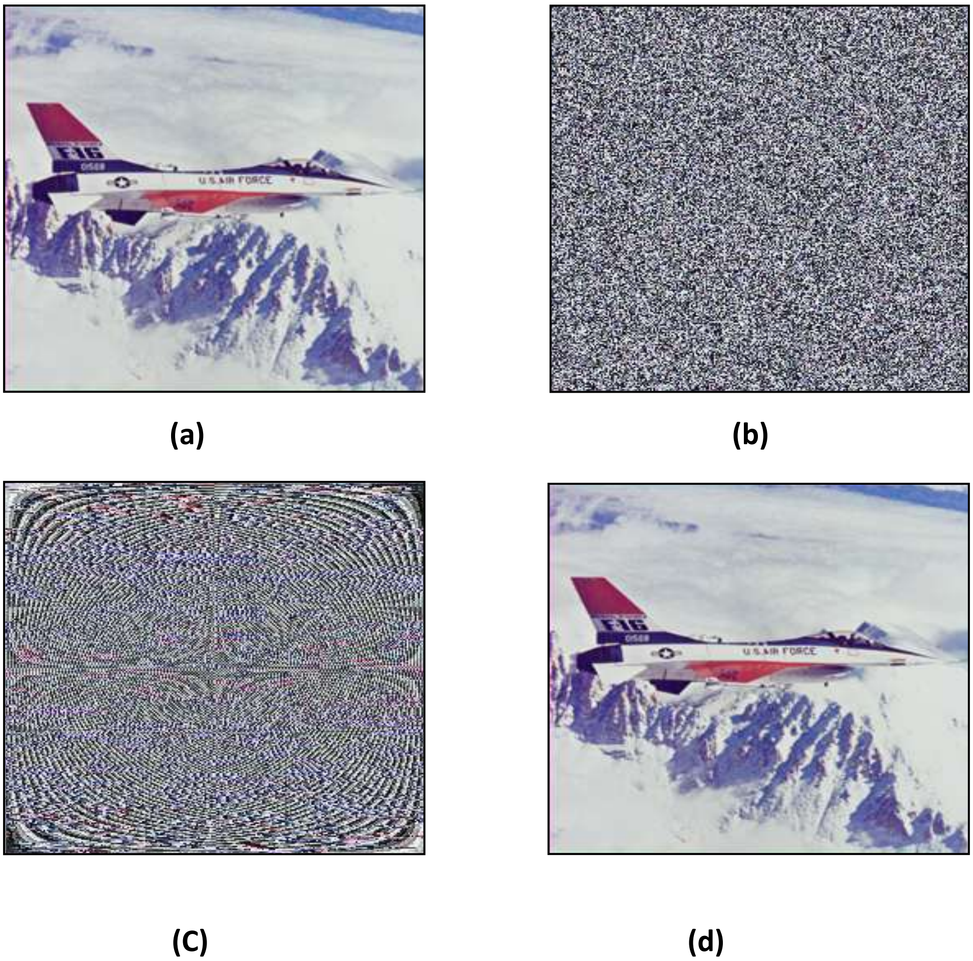


(a) (b)

(C) (d)

Figure(2) (a) Plain image " lena.bmp "; (b) cipher image; (c) decryption image with only one bit is differ in standard map parameter(k_c = 1000) and (d) decryption image with same parameter(k_c=999).

Another sensitivity for number of iterations(same parameters for encryption and decryption but the number of iterations=10 in encryption side and it is equal = 9 in decryption side) as shown in figure(3) , airplane image as an example



(a) (b)

(C) (d)

Figure (3): (a) Plain image " airplane.bmp "; (b) cipher image with no. of iterations=10; (c) decryption image with only one loop is differ=9 and (d) decryption image with same parameter and number of iterations.

Another test for sensitivity can be applied to any parameters encryption key(random scan couple r_x ,r_y) for diffusion or confusion techniques and the result is similar to the above figures, therefore can be conclude the proposed cryptosystem has an enough large key space and sensitive to any change until is a slight change of the key which make it impossible to obtain the plain image from decrypted one, so if any slight changes are occurred generate a completely different in decryption results and can't get or access to the correct plain image.

C- Processing Time

The speed of any cryptosystem is the significant criterion of any system especially in multimedia systems and real time application. To estimate the execution time of the proposed encryption scheme, different tests are applied, the Tests results of encryption time is shown in Table (3)

Table(3) Show the speed of encryption algorithm

IMAGE 256*256	ENCRYPTION TIME(SEC)		
	R=5	R=10	R=20
Airplane	0.192	0.280	0.452
Lena	0.201	0.296	0.405
Cameraman	0.187	0.276	0.452

The results of Table (3) , the execution time of encryption with different rounds is less (1 second) which represent it is faster than many systems and can be say the encryption time is suitable for different applications like real time applications and the encourage results lead to leave and doesn't need the partial or selective encryption techniques to decrease the encryption time to became suitable with real time applications.

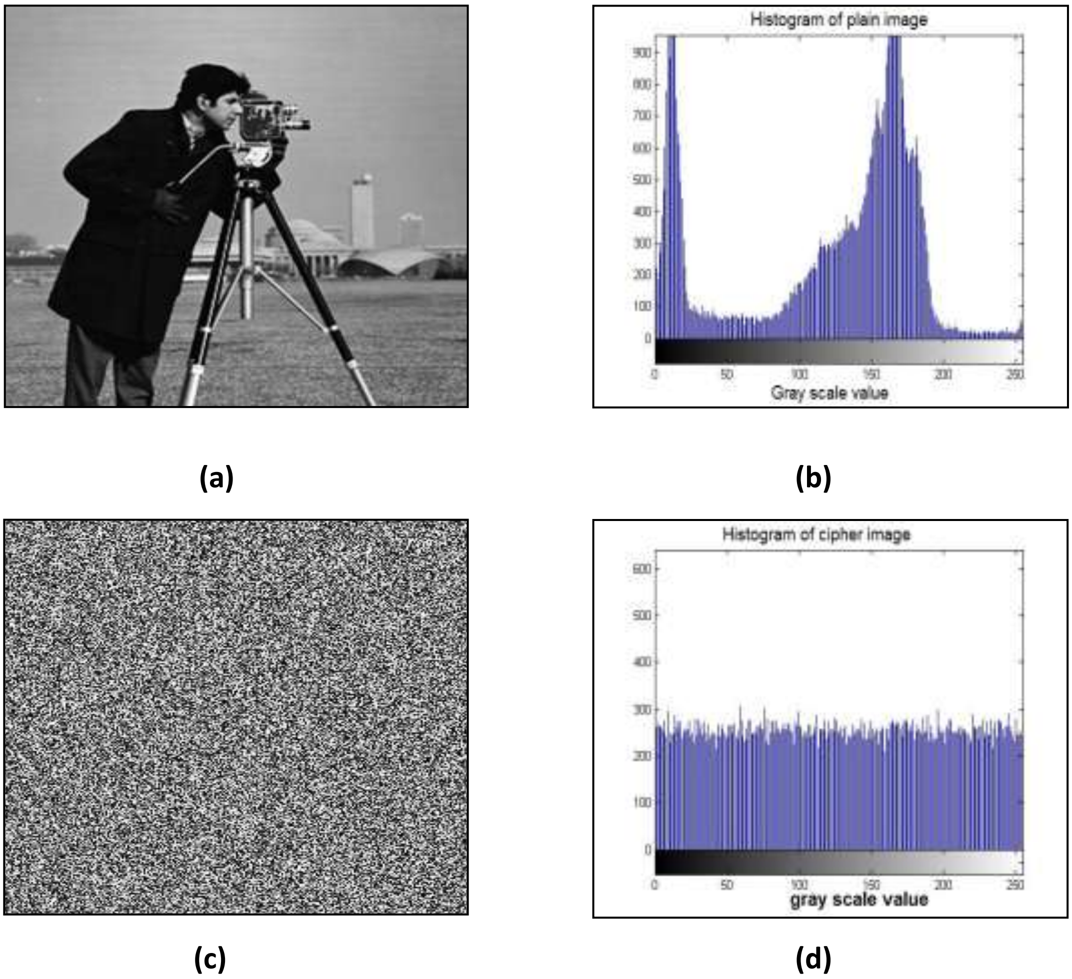
D-Encryption Quality

An important issue in image encryption algorithms is the evaluation of the quality of encryption. An image encryption algorithm is good, if it is able to conceal a large number of image features. Histogram and Peak signal-to noise ratio (PSNR) are good criteria To judge the quality of encryption system.

i. Statistic Characteristic of Images(Histogram)

Image histogram is an important statistic characteristic of images, which can directly reflect the correlation of the gray value and the frequency of the gray value in the image[16]. When The cipher image have a uniform histogram distribution we can be said the cryptosystem is good and conceals all the attributes of the plain image.

As shown in figures (4), the cameraman plain image and its relative corresponding cipher image are presented, their histograms are presented too.



Figure(4): (a) cameraman plain image (b) histogram of plain image (c) cipher image (d) histogram of cameraman cipher image

When comparing figure (4.b) and figure (4.d), the histogram of the cipher image is fairly uniform and it significantly hidden the statistical features of the original image .Therefore the attacker cannot estimate the cipher image because the distribution of pixel values of image are the same and symmetric and doesn't found any difference in these values, then the quality of this scheme is good.

ii. **Peak Signal-to-Noise Ratio (PSNR)**

Peak signal-to noise ratio criterion can be evaluate an image encryption scheme. PSNR reflects the encryption quality. It is a measurement which indicates the changes in pixel values between the plaintext e and the cipher text .
Mathematically: PSNR is [17].

$$PSNR = 10\log_{10}\left[\frac{M \times N \times 255^2}{\sum_{i=0}^{M-1}\sum_{j=o}^{N-1}(P(i,j)-C(i,j))^2}\right] \quad \text{....... (8)}$$

Where M is the width and N is the height of digital image. P(i,j) is pixel value of the plaintext image at grid (i ,j) and C(i,j) is pixel value of the ciphertext image.

Table (4) shows the results of calculating PSNR for some images

Table (4) show the values of PSNR of the test images

Images	Lena	Cameraman	Airplane
PSNR(db)	32.12	32.25	32.13

When the PSNR is high and the value of PSNR is greater than (30 db) then the quality of cryptosystem is good. From the above table PSNR > 32db .It means that the quality of the decrypted image is acceptable.

vii. Conclusion

Image encryption system is robust and secure if firstly: the correlation between adjacent pixels become very low (approach to zero), this criterion depend on strength of confusion operation secondly: the correlation or relationship between the plain image and cipher image is low or no relationship, this criterion depend on strength of diffusion operation. Thus in this paper an image encryption based on 2D chaotic map wherever confusion(randomly change of pixels position)and diffusion(randomly change of pixels value) specially these are execute at same loop, Where the value and position pixel are changes randomly and in non-linear behavior based on chaos theory. Experimental analysis show that the proposed image encryption system has high security(large key space, high sensitivity to secret keys, uniform histogram) and high speed (0.25 second) .It suitable for Variety types of applications like the real-time field, mobile communication and protect the image data in the Internet.

References

[1] Zhao L, Adhikari A, Xiao D, Sakurai K. "***On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption".*** Commun Nonlinear Sci Numer Simulat; Vol(17) :3303–27, 2012.

[2] Patidar V, Pareek N, Sud K. " ***Modified substitution–diffusion image cipher using chaotic standard and logistic maps***". Commun Nonlinear Sci Number Simul;Vol.(7) :2755–65, 2010.

[3] Shannon CE. "***Communication theory of secrecy systems***". Bell System Tech, 28(4),656–715, 1949.

[4] ZH. Guan, F. Huang, W. Guan, "***Chaos-based image encryption algorithm***", Physics Letters A , Vol. 346, No. 1-3, pp. 153–157, 2005.

[5] J. Fridrich, ***"Symmetric ciphers based on two dimensional chaotic maps***", International Journal of Bifurcation and Chaos Vol.8 (6) 1259-1284, 1998.

[6] Musheer A, Shamsher A, "***A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping",***International Journal on Computer Science and Engineering, Vol.2(1), 46-50, 2009.

[7] 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; IEEE, Zhengzhou, China;pp.267-270, April 2010.

[8] Kamlesh G and Sanjary S," ***New approach for fast color image encryption using chaotic map*** ", university of engineering and technology, Guna, India, journal of information ssecurity, vol.(2),pp.139-150, july 2011.

[9] Jean N k , Joseph E, Jean F," ***A Fast Image Encryption Algorithm Based on Chaotic Maps and the Linear Diophantine Equation***" Department of Physics, Faculty of Science, University of Ngaoundéré, Ngaoundéré 237, Cameroon, Volume 1, No: 4, pp. 232-243, 2014.

[10] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "***Encryption and decryption of images with chaotic map lattices.***" CHAOS Journal, American Institute of Physics, vol. 16, no. 3, pp. 033118-033118-6, 2006.

[11] Ljupco Kocarev " ***Chaos-Based Cryptography: A Brief Overview"*** IEEE,2001.

[12] Yun Q. Shi, Huifang Sun; "***Image and Video Compression for Multimedia Engineering"***, New Jersey Institute of Technology ,2nd Edition, New Jersey, USA, pp. 49-50, 2008.

[13] Samara A. Halagy, "***Coding of Video Over IP Based Networks***", M.Sc. Thesis, University of Nahrain, 2007**.**

[14] S.G. Lian, J. Sun, Z. Wang**, "A block cipher based on a suitable use of the chaotic standard map",** Chaos, Solitons & Fractals 26 (1) pp. 117-129, 2005**.**

[15] Jawad Ahmad, Fawad Ahmad; "***Efficiency analysis and security evaluation of image encryption schemes***"; International journal of Video & Image Processing and Network Security, Vol(12), No:04, 2012**.**

[16] I. E. Elashry, "***Digital image encryption***, " MS Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2010.

[17] M.El-Iskandarani, S.Darwish and S.Abuguba, ***"A roubust and secure scheme for image transmission over wireless channels***, " in security technology, pp.51-55,.ICCST 2008. IEEE, 2008.