ACSIJ Advances in Computer Science: an International Journal, Vol. 5, Issue 1, No.19 , January 2016
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

Digital Image Encryption Based On Multiple Chaotic Maps

Amirhoushang Arab Avval[1], Jila ayubi[2] and Farangiz Arab[3]

[1] Department of Research and Development Ports and Maritime Organization
Chabahar, Sistan and Baluchestan, Iran
amirhoushang.arab@gmail.com

[2] Department of Electrical engineering Meraaj Higher Education Institue
Salmas, West Azarbayjan, Iran
Jila.ayubi@gmail.com

[3] Department of Gaedi Health Center, Isfahan Medical Sciences University
Isfahan, Isfahan, Iran
Dr.f.arab@gmail.com

Abstract

A novel and robust chaos-based digital image encryption is proposed. The present paper presents a cipher block image encryption using multiple chaotic maps to lead increased security. An image block is encrypted by the block-based permutation process and cipher block encryption process. In the proposed scheme, secret key includes nineteen control and initial conditions parameter of the four chaotic maps and the calculated key space is 2^{883}. The effectiveness and security of the proposed encryption scheme has been performed using the histograms, correlation coefficients, information entropy, differential analysis, key space analysis, etc. It can be concluded that the proposed image encryption technique is a suitable choice for practical applications.

Keywords: *Image Encryption; Chaos; Chaotic Maps; High Security.*

1. Introduction

With the rapid growth in digital image processing and network technology, more information and multimedia files has been transmitted over the computer networks and internet. Protection of digital information against illegal access and distribution has become extremely important. Therefore, techniques are required to provide security functionalities like privacy, integrity, or authentication especially suited for these data types of multimedia. A few applications of these techniques for providing privacy and confidentiality of visual data are in the areas of telemedicine, videoconferencing, military surveillance, and video-on-demand, pay TV etc. However, visual data such as image and video is different from text, conventional algorithms such as DES, IDEA, AES and most other methods are not suitable for image and video encryption.

Chaos theory has been established since 1970s in many practical applications to the real world, including synchronization, control, neural network, communication, etc [1-4]. Many researchers have noticed that there exists a close relationship between chaos and cryptography [5], [6]; many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems.

Chaotic systems have several significant advantage in establish secure communications, such as ergodicity, sensitivity to initial condition, control parameters and random like behavior [7], [8]. A lot of image encryption schemes based on chaotic map have been already presented [9-12]. In the digital world nowadays, the security of digital images and performance speed has become more important since the communications of digital information over network occur more and more frequently.

In this paper, a new design of a class of chaotic cryptosystems is suggested to overcome the aforementioned drawbacks. Experimental results and security analysis indicate that the encryption algorithm based on multiple chaotic maps is advantageous from the point of view of large key space and high security.

The rest of the Letter is organized as follows. Section 2 describes used chaotic maps in proposed algorithm. An image encryption and decryption procedure is shown in Section 3. Also, the selected example and simulation results are discussed in Section 4. Section 5 is the conclusion.

2. Chaotic maps

2.1 Jacobian Elliptic Maps

In the past twenty year's dynamical systems, particularly one-dimensional iterative maps have attracted much attention and have become an important area of research activity [13]. This is also true in the case of so-called elliptic maps [14,15]. One-parameter families of jacobian elliptic rational maps [16] of the interval [0,1] with an invariant measure can be defined as:

$$X_{n+1} = \frac{4\alpha^2 X_n(1-k^2X_n)(1-X_n)}{(1-k^2X_n^2)^2 + 4(\alpha^2-1)X_n(1-k^2X_n)(1-X_n)} \quad (1)$$

Where $X_0 \in [0,1]$, $\alpha \in [0,4]$ and $k \in [0,1]$, k (modulus) represent the parameter of the elliptic functions. Bifurcation diagram of jacobian elliptic map is shown in Fig.1.

2.2 Chaotic Coupled Map

CML (coupled map lattices) based spatiotemporal chaotic systems have drawn initial attention in chaotic cryptography in recent years due to their excellent chaotic dynamical properties [17], [18] and [19].

Coupled map lattices are arrays of states whose values are continuous, usually within the unit interval, or discrete space and time [20]. The pair-coupled map with ergodic behavior can be considered as a one-dimensional dynamical map defined as:

$$X_{n+1} = [(1-\varepsilon) f_1(X_n)^P + \varepsilon f_2(X_n)^P]^{\frac{1}{P}} \quad (2)$$

Where, in general, P is an arbitrary parameter, ε the strength of the coupling, and the functions $f_1(X_n)$, $f_1(X_n)$ are two arbitrary one-dimensional maps. Obviously, by choosing $P = 1$, we get ordinary linearly coupled maps. $f_1(X_n)$, $f_1(X_n)$ defined as:

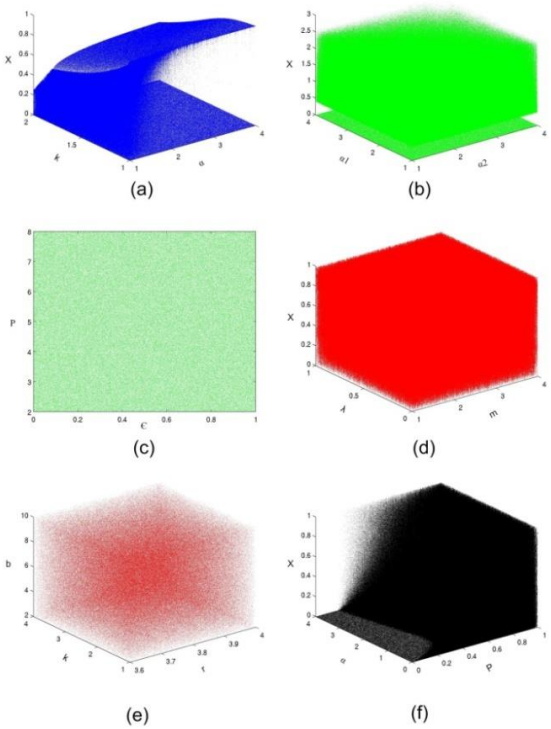

Fig. 1 Bifurcation diagram of (a) Jacobian elliptic map (b-c) Chaotic coupled map (d-e) Quantum map (f) piecewise nonlinear map.

$$f_1(X_n) = \frac{1}{\alpha_1^2} \tan(|\ N \times \arctan(|\ X_n\ |))$$
$$f_2(X_n) = \frac{1}{\alpha_2^2} \cot(|\ N \times \arctan(|\ X_n\ |)) \quad (3)$$

Where $X_0 \in [0,1]$, $\alpha_1 \in [0,4]$, $\alpha_2 \in [0,4]$, $\varepsilon \in [0,1]$ and $P \in [2,10]$.Fig.1(b-c) show the bifurcation plot of chaotic coupled map.

2.3 Quantum Map

The quantum rotators model has been widely used to study the dynamics of classically chaotic quantum systems and is specified in a simple form by:

$$X_{n+1} = r(X_n - X_n^2)\cos^k(-\lambda \frac{e^{-mb}}{b}) \quad (4)$$

Where $X_0 \in [0,1]$, $r \in [3.6,4]$, $\lambda \in [0,1]$, $m \in [1,4]$, $b \in [1,4]$ and $k \in [2,10]$.Bifurcation diagram of quantum map are shown in Fig.1(d-e).

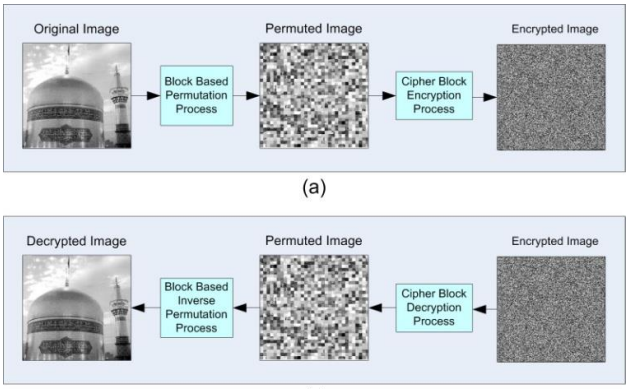

Fig. 2 Block Diagram Of (a) Encryption Process (b) Decryption Process

2.4 Piecewise nonlinear chaotic Map

A brief review of one-parameter families of piecewise nonlinear chaotic maps with an invariant measure is presented in [7]. These maps can be defined as:

$$X_{n+1} = \frac{\alpha^2 F}{1 + (\alpha^2 - 1)F} \quad (5)$$

Where

$$F = \begin{cases} \dfrac{X_n}{P} & 0 \le X \le P \\ \dfrac{X_n - P}{1 - P} & P < X \le 1 \end{cases} \quad (6)$$

Then, the probability parameter of the piecewise nonlinear chaotic maps p is generated by using the results of iteration of the trigonometric map can be defined as:

$$Y_{n+1} = \frac{1}{\beta^2} \tan^2(N \times \arctan(\sqrt{X_n}) \quad (7)$$

Therefore

$$P=\begin{Bmatrix} Y_{n+1} & 0\le Y_{n+1}\le 1 \\ \dfrac{1}{Y_{n+1}} & Y_{n+1}>1 \end{Bmatrix} \quad (8)$$

Where $X_0 \in [0,1]$, $\alpha \in [0,4]$, $\beta \in [0,4]$, $Y_0 \in [0,1]$, $b \in [1,4]$ and $P \in [0,1]$. Bifurcation diagram of quantum map is shown in Fig.1(f).

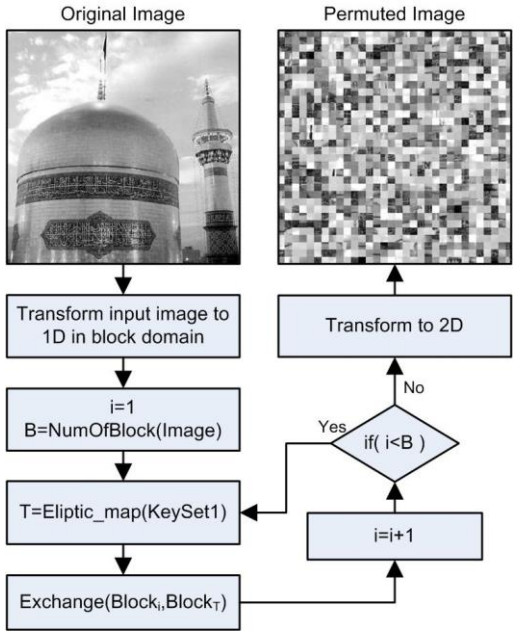

Fig. 3 Flowchart of Permutation Process.

3. THE ENCRYPTION AND DECRYPTION PROCEDURES

The proposed cryptosystem is a stream cipher algorithm based on multiple chaotic Maps. The block diagram of the proposed algorithm is presented in Fig.2 .This algorithm consists of the following major parts:

3.1 Permutation Process

Permutation procedure algorithm on each block is as follows:

- Step 1: Transform the input image from 1D to 2D in block domain.
- Step 2: Let size of image blocks in B and initialize $i=1$.
- Step 3: Generate chaotic pseudo-random number by jacobian elliptic map and set in T. ($T \in [1, B]$)
- Step 4: Exchange i-th block of image with T-th block.
- Step 5: Let $i=i+1$.
- Step 6: Repeat steps 3 to 5 until you reach the last block.
- Step 7: To display obtained image, transform the blocks from 1D to 2D.

3.2 Cipher Block Encryption Process

Cipher block encryption procedure is as follows:

- Step 1: Initialize $i=1$.
- Step 2: Generate chaotic pseudo-random number by jacobian elliptic map and set in T_1 . $T_1 \in \{1,2,3\}$)
- Step 3: Apply bit XOR operator :
- $Block_i = Block_i \oplus Block_{i-1}$

Flowchart of permutation process is shown in Fig.3.

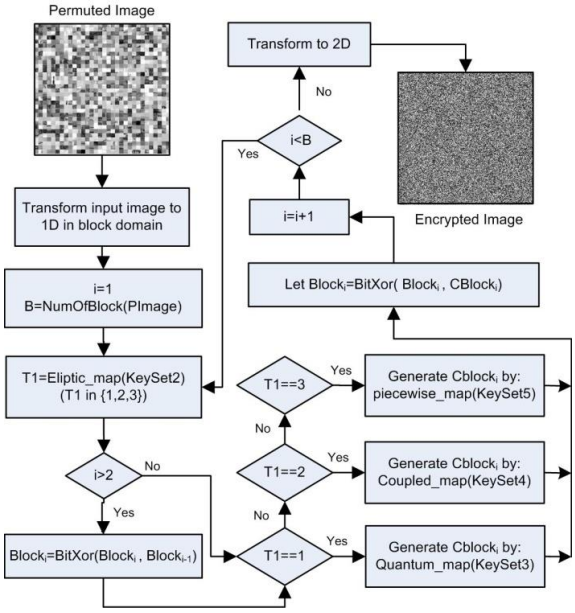

Fig. 4 Flowchart of Cipher Block Encryption Process.

- Step 4: if $T_1 = 1$ then, generate chaotic pseudo-random number by chaotic coupled map and set in $CBlock_i$. (Each elements in $CBlock_i \in [0,255]$).
- Step 5: if $T_1 = 1$ then, Generate chaotic pseudo-random number by quantum map and set in $CBlock_i$. (Each elements in $CBlock_i \in [0,255]$).
- Step 6: if $T_1 = 3$ then, generate chaotic pseudo-random number by piecewise map and set in $CBlock_i$. (Each elements in $CBlock_i \in [0,255]$).
- Step 7: Apply bit XOR operator :

$$Block_i = Block_i \oplus CBlock_i$$

- Step 8: Let $i = i + 1$.
- Step 9: Repeat steps 2 to 8 until you reach the last block.
- Step 10: To display obtained image, transform the blocks from 1D to 2D.

Flowchart of Cipher Blocked Encryption process is shown in Fig. 4. Since both decryption and encryption procedures have similar structure, they essentially have the same algorithmic complexity and time consumption.

4. EXPERIMENTAL RESULTS

In order to test the efficiency of the proposed chaotic cryptographic scheme a gray scale image "Mashhad" with the size 512×512 pixels is used (Fig. 5(a)). The results of the encryption are presented in Fig. 5(b-c). As can be seen from the figures there is no patterns or shadows visible in the corresponding cipher text. The test has been carried out in other familiar images as well (see Fig. 5).

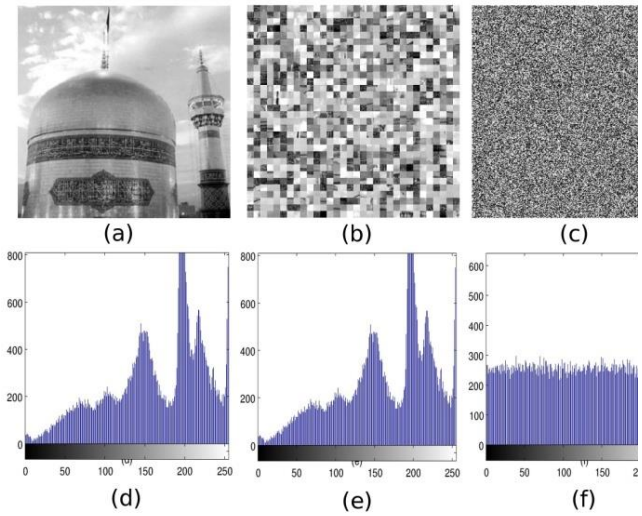

Fig. 5 Encryption and Decryption of Mashhad image. (a) Original Image (b) Permuted Image (c) Cipher text Image (d) Histogram of Plaintext (e) Histogram of Permuted Image Cipher text.

4.1 SECURITY ANALYSIS

When a new cryptosystem is proposed, it should always be accompanied by some security analysis. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analysis has been performed on the proposed scheme like key space analysis, statistical analysis, etc. The security analysis demonstrated a high security level of the new scheme as demonstrated through following test methods.

4.1.1 Histogram analysis

An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels. By taking a (512×512) sized "Mashhad" image as a plaintext, the histogram of the plaintext and permutated image and corresponding cipher text are shown in Fig. 6(d-f). As it was shown, the histograms of the original image and hence it does not provide any clue to employ any statistical analysis attack on the encryption image [7], [21].

4.1.2 Information Entropy

The entropy (such as KS-entropy, information entropy,) is the most outstanding feature of the randomness [22]. Information theory is a mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon. To calculate the entropy $H(s)$ of a source s, we have:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} \qquad (9)$$

Where $P(s_i)$ represents the probability of symbol s_i. Actually, given that a real information source seldom transmits random messages, in general, the entropy value of the source is smaller than the ideal one. However, when these messages are encrypted, their entropy should ideally be 8.If the output of such a cipher emits symbols with entropy of less than 8, Then there exists a predictability which threatens its security. For the introduced encrypted image (Fig. 5(c)) and standard test images (Fig. 7-9), we have calculated the information entropy and the result have been presented in Table 1. The obtained values are very close to the theoretical value 8.

Apparently, comparing it with the other existing algorithms, the proposed algorithm is much closer to the ideal situation. That is, the information leakage in the encryption process is negligible, and so the encryption system is secure against the entropy attack.

4.2 Correlation of two adjacent pixels:

We have also analyzed the correlation between two vertical, two horizontal, and two diagonally adjacent pixels in "Mashhad" cipher image. To analyze the correlation of the adjacent pixels the following relation has been used [9]:

$$C_r = \frac{(N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j)}{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_i)^2)(N\sum_{j=1}^{N} y_j^2 - \sum_{j=1}^{N} y_i)^2)} \qquad (10)$$

Where x_i and y_j are the values of the adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation. We have chosen randomly5000 image pixels in the plain image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in diagonal, horizontal

and vertical direction (See Table 2). The same result for ciphered image presented in Table 3. It demonstrates that the encryption algorithm has covered up all the characters of the plain image showing a good performance of balanced 0 - 1 ratio. The correlation of the plaintext and cipher text is shown in Fig. (6).

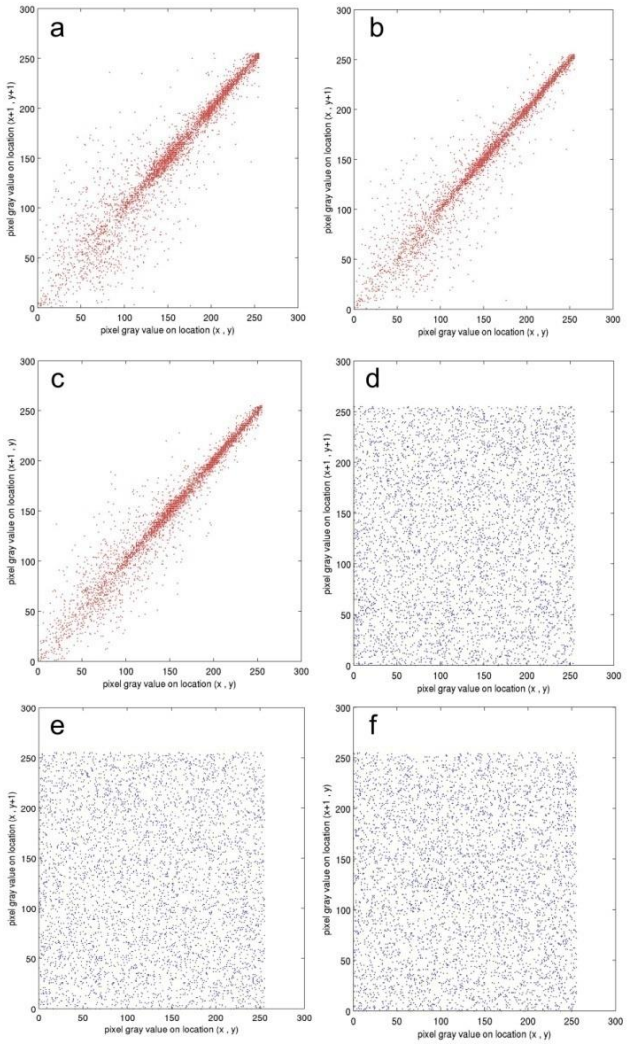

Fig. 6 Correlations of two diagonal, horizontal and vertical adjacent pixels in the plain-image and in the cipher-image: (a-c) Correlation analysis of plain-image. (d-f) Correlation analysis of cipher-image.

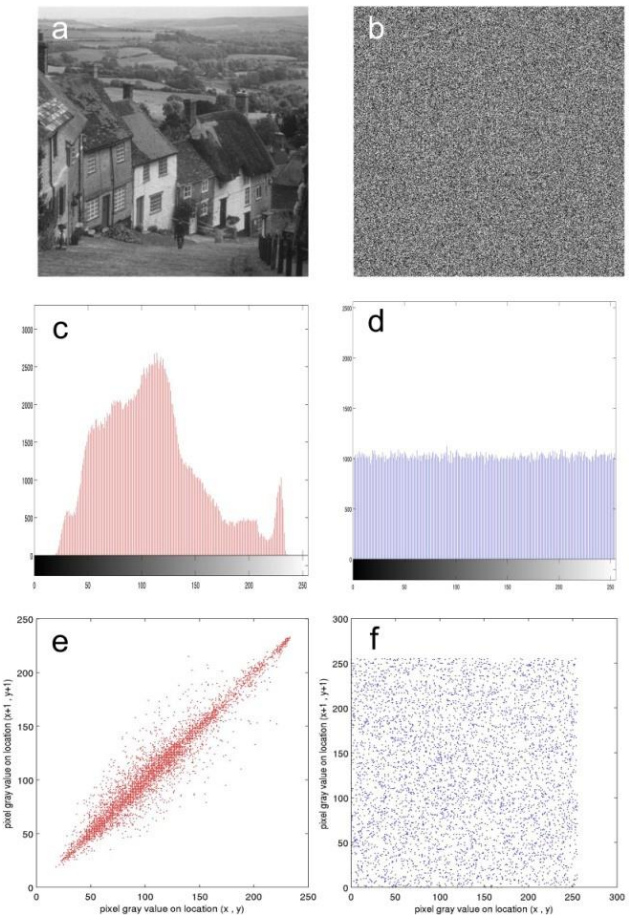

Fig. 7 (a) Original Hill image (b) encrypted image (c) histogram of original image (d) histogram of encrypted image (e-f) Correlations of two diagonal adjacent pixels in original and encrypted image.

4.3 Plaintext sensitivity analysis (Differential analysis):

In order to resist differential attack, a minor alternation in the plain-image should cause a substantial change in the cipher-image. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, two common measures were used: NPCR and UACI [23]. NPCR represents the change rate of the ciphered image provided that only one pixel of plain image changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image. For calculation of NPCR and UACI, let us assume two ciphered images C_1 and C_2 whose corresponding plain images have only one-pixel difference. Label the grey-scale values of the pixels at grid (i, j) of C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$, respectively. Define a bipolar array, D, with the same size as image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$, namely, if $C_1(i, j) = C_2(i, j)$ then

$D(i,j)=1$; otherwise, $D(i,j)=0$. NPCR and UACI are defined by the following formulas [24]:

$$UACI=\frac{1}{W\times H}[\frac{|C_1(i,j)-C_2(i,j)|}{255}]\times 100\% \quad (11)$$

$$NPCR=\frac{\sum_{i,j}D(i,j)}{W\times H}\times 100\% \quad (12)$$

Where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme by considering the one-pixel change influence on a 256 grayscale image of size 512×512. The obtained result presented in Table 4. The calculated value of UACI and NPCR for the proposed algorithm is compared with other chaos-based image encryption algorithm and comparison results is shown in Table 5. The table shows that the proposed algorithm is so sensitive to the plaintext.

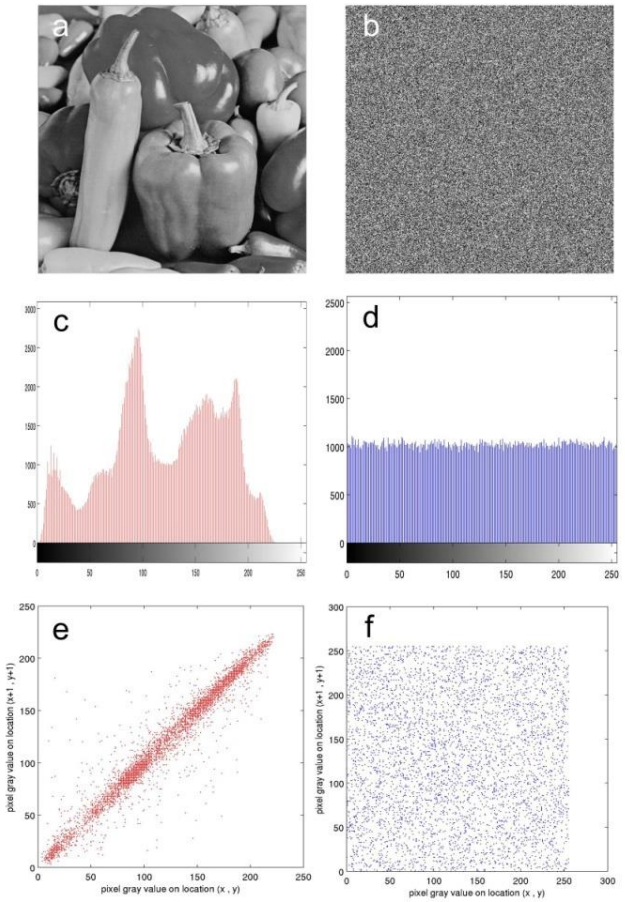

Fig. 8 (a) Original peppers image (b) encrypted image (c) histogram of original image (d) histogram of encrypted image (e-f) Correlations of two diagonal adjacent pixels in original and encrypted image.

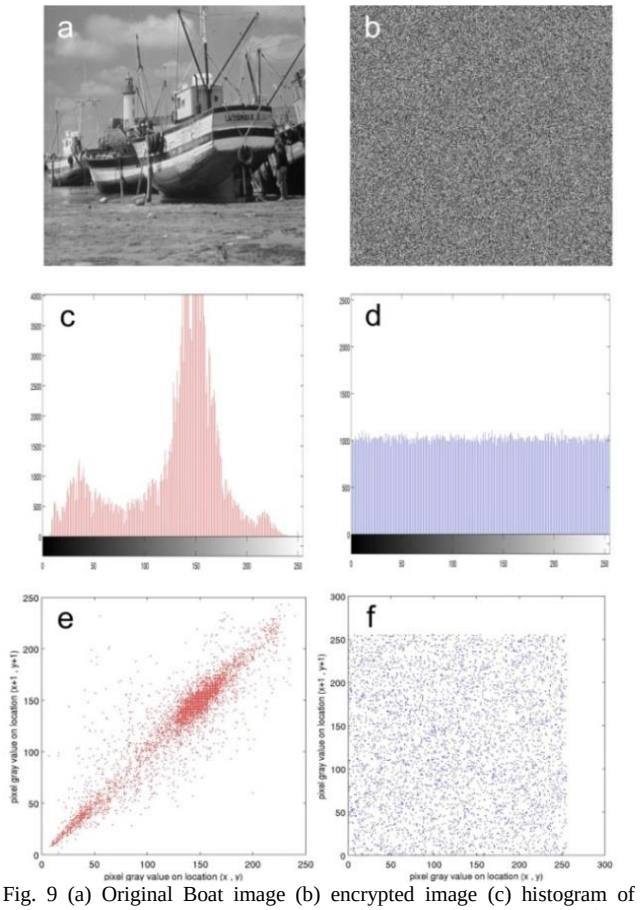

Fig. 9 (a) Original Boat image (b) encrypted image (c) histogram of original image (d) histogram of encrypted image (e-f) Correlations of two diagonal adjacent pixels in original and encrypted image.

5. Key Space

The key is the fundamental aspect of every cryptosystem. An algorithm is as secure as its key. No matter how strong and well designed the algorithm might be, if the key is poorly chosen or the key space is small enough, the cryptosystem will be broken. The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system.

In the proposed scheme, the secret key includes nineteen control and initial conditions parameter of the four chaotic maps. The sensitivity to these initial parameters is shown as follows:

- Jacobian Elliptic Maps: ($X_0\in[0,1]$, $\alpha\in[0,4]$ and $k\in[0,1]$).
- Chaotic Coupled Map: ($X_0\in[0,1]$, $\alpha_1\in[0,4]$, $\alpha_2\in[0,4]$, $\varepsilon\in[0,1]$ and $P\in[2,10]$).
- Quantum Map: ($X_0\in[0,1]$, $r\in[3.6,4]$, $\lambda\in[0,1]$, $m\in[1,4]$, $b\in[1,4]$ and

$k \in [2,10]$).

- Piecewise Nonlinear Chaotic Map:

($X_0 \in [0,1]$, $\alpha \in [0,4]$, $\beta \in [0,4]$, $Y_0 \in [0,1]$, $b \in [1,4]$ and $P \in [0,1]$).

If the precision is 10^{-14} for each of nineteen parameters, the size of key space for initial conditions and control parameters is $2^{883}((10^{-14})^{19})$ .The key space is large enough to resist all kinds of brute-force attacks [24].

6. CONCLUSION

Cryptography is the art of achieving security by encoding messages to make them non- readable. We propose a novel encryption scheme for color image based on multiple chaotic maps. This algorithm tries to address the shortcoming of encryption such as small key space and level of security. Secret key includes nineteen control and initial conditions parameter of the four chaotic maps and the calculated key space is 2^{883} and the key space is large enough to resist all kinds of brute-force attacks. Therefore, it is an effective technique for image encryption. The goal is to realize an encryption method with a private code. Further studies must be started to develop encryption methods with a public key.

TABLE 1: INFORMATION ENTROPY

Image	*Entropy*
Mashhad	7.9994
Hill	7.9994
Peppers	7.9993

TABLE 2: SIMULATION RESULT OF CORRELATION OF TWO ADJACENT PIXELS IN ORIGINAL IMAGE

Image	*Diagonal*	*Horizontal*	*Vertical*
Mashhad	0.9493	0.9725	0.9762
Hill	0.9655	0.9818	0.9820
Peppers	0.9715	0.9822	0.9812
Boat	0.9259	0.9358	0.9728

TABLE 3: SIMULATION RESULT OF CORREATION OF TWO ADJACENT PIXELS IN CIPHER IMAGE

Image	*Diagonal*	*Horizontal*	*Vertical*
Mashhad	-0.0188	0.0015	-0.0038
Hill	0.0029	0.0211	0.0014
Peppers	0.0072	0.0051	0.0092
Boat	0.0027	0.0419	-0.0059

TABLE 4: PLAINTEXT SENSITIVITY ANALYSIS OF PROPOSED ALGORITHM

Image	*UACI*	*NPCR*
Mashhad	0.3345	0.3841
Hill	0.3352	0.3925
Peppers	0.3353	0.3937
Boat	0.3352	0.3979

TABLE 5: COMPARATION RESULT OF PREPOSED ALGORITHM WITH OTHER RELATION CHAOTIC METHOD

Algorithm	*UACI*	*NPCR*
Behnia et al.[7]	0.39	0.46
Akhavan et al.[28]	0.39	0.39
Sun et al.[29]	0.3192	0.40
Rhouma et al.[30]	0.3346	0.389
Tong et al. [31]	0.3356	0.39453
Proposed Algorithm	0.3345	0.3841

References

[1] Ira Aviram, AvinoamRabinovitch, Bifurcation analysis of bacteria and bacteriophage coexistence in the presence of bacterial debris, ommunications in Nonlinear Science and Numerical Simulation, Volume 17, Issue 1, January 2012, Pages 242-254, ISSN 1007-5704, DOI: 10.1016/j.cnsns.2011.04.031.

[2] RongweiGuo, Finite-time stabilization of a class of chaotic systems via adaptive control method, Communications in Nonlinear Science and numerical Simulation, Volume 17, Issue 1, January 2012, Pages 255-262, ISSN 1007-5704, DOI: 10.1016/j.cnsns.2011.05.001.

[3] Li-Guo Yuan, Qi-Gui Yang, Parameter identification and synchronization of fractional-order chaotic systems, Communications in Nonlinear Science and Numerical Simulation, Volume 17, Issue 1, January 2012, Pages 305-316, ISSN 1007-5704, DOI: 10.1016/j.cnsns.2011.04.005.

[4] Kun Zhang, Hua Wang, Hui Fang, Feedback control and hybrid projective synchronization of a fractional-order Newton-Leipnik system, Communications in Nonlinear Science and Numerical Simulation, Volume 17, Issue 1, January 2012, Pages 317-328, ISSN 1007-5704, DOI: 10.1016/j.cnsns.2011.04.003.

[5] Wei J, Liao XF, Wong KW, Xiang T. "A new chaotic cryptosystem", Chaos, Solitons& Fractals, vol. 30, pp.1143-52, 2006.

[6] Lian S, Sun J, Wang J, Wang Z. "A chaotic stream cipher and the usage in video protection", Chaos, Solitons&Fractals , vol.34, pp.851-59, 2007.

[7] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," Phys. Lett. A vol. 366, pp.391-396, 2007.

[8] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, A. [2008] "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons& Fractals 35, pp. 408-19.

[9] VinodPatidar, N.K. Pareek, G. Purohit, K.K. Sud, A robust and se-cure haotic standard map based pseudorandom permutation-substitution scheme for image encryption, Optics Communications, In Press, Cor-rected Proof, Available online 26 May 2011, ISSN 0030-4018, DOI: 10.1016/j.optcom.2011.05.028.

[10] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation,Information Sciences, Volume 181, Issue 6, 15 March 2011, Pages 1171-186, ISSN 0020-0255, DOI: 10.1016/j.ins.2010.11.009.
[11] Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, Guanrong Chen, A new chaos-based fast image encryption algorithm, Applied Soft Computing, Volume 11, Issue 1, January 2011, Pages 514-522, ISSN 1568-4946, DOI: 10.1016/j.asoc.2009.12.011.
[12] Di Xiao, Frank Y. Shih, Using the self-synchronizing method to improve security of the multi chaotic systems-based image encryption, Optics Communications, Volume 283, Issue 15, 1 August 2010, Pages 3030-036, ISSN 0030-4018, DOI: 10.1016/j.optcom.2010.03.063.
[13] K. Umeno, Phys. Rev. E 58 (1998) 2644.
[14] R. Chacon, A.M. Garcia-Hoz, Europhys. Lett. 57 (1) (2002) 7.
[15] K. Umeno, RIMS Kokyuroku 1098 (1999) 104.
[16] R.L. Devancy, An Introduction to Chaotic Dynamical Systems. Addison Wesley, 1982.
[17] T. Xiang, K. Wong and X. Liao, Selective image encryption using a spatiotemporal chaotic system, Chaos 17 (2007), p. 023115.
[18] P. Li, Z. Li, W. Halang and G. Chen, A stream cipher based on a spatiotemporal chaotic system, Chaos SolitonsFract 32 (2007), pp. 1867–1876.
[19] S. Wang, J. Kuang, J. Li, Y. Luo, H. Lu and G. Hu, Chaos-based secure communications in a large community, Phys Rev E 66 (2002), p. 065202.
[20] S. Behnia, M. Teshnehlab, P. Ayubi, Multiple-watermarking scheme based on improved chaotic maps, Communications in Nonlinear Science and Numerical Simulation, Volume 15, Issue 9, September 2010, Pages 2469-2478, ISSN 1007-5704, DOI: 10.1016/j.cnsns.2009.09.042.
[21] M. A. Jafarizadeh and S. Behnia, “Hierarchy of one- and many-parameter families of elliptic chaotic maps of cn and sn types”, Physics Letters A vol. 310, pp.168-176, 2003.
[22] R.L. Devancy, An Introduction to Chaotic Dynamical Systems. Addison Wesley, 1982, pp. - .
[23] E. Ott. Chaos in dynamical system .Cambidge university pess, 2002, pp. .
[24] A. Akhavan, H. Mahmodi, A. Akhshani, A new image encryption algorithm based on one-dimensional polynomial chaotic maps, Lect. Notes Comput. Sci. 4263 (2006) 963971.