A novel image encryption algorithm using Alternate and Control Parameters Structure

Mohammad Mirzaei [a,*], Khadijeh Aghajani [b], Saleh Fakhrali.M [c]

[a] Computer engineering University of Tehran, Tehran, Iran

[b] Computer engineering University of Mazandaran, Mazandaran, Iran

[c] Computer engineering Amirkabir University of Technology, Tehran, Iran

Abstract

Cryptography methods are used for transportation of important and security images nowadays and various methods are exposed to reach this purpose but, of the most common methods in image cryptography, there are chaos based algorithms. In this paper it is tried to introduce a new cryptography method for RGB and grayscale images based on the efficiencies of mapping methods like chaos mapping Cat map , standard map and logistic map going along with OCML method. Since there is no change in the first pixel in most of chaos mapping methods and therefore utilizing this defect by attackers in order to obtain important data in the image, value of the first pixel will change in both of proposed methods and some parameters are taken from the result picture to increase the security of these methods. ACPS algorithm is made of two main parts which are control block and OCML block and they are used alternatively in each round.

Keywords:

Control block, standard map, logistic map, Cat map, OCML (One-way Coupled Map Lattices)

1-Introduction

Regarding to ever-increasing requirement for secure transferring of information in internet, in communication networks and in other almost high inner one, image encryption is one of the useful ways in secure communication. Since there is high volume of information in images, using text encryption processes such as AES, DES and so forth is impossible. At present chaos based process in data security and in confidential communication Systems are developing. Since in such chaos systems, either *synchronization control* process or non *coherent demodulation* process may be used, it will be a weak point of them if there will be no enough recognition in chaos system parameters and *transmitter* structure; therefore, the attackers can rebuild state space by the use of the *synchronization control.* In non coherent process, plain image would also be acquired by locating the symbol period window through tracking and estimation [1-3].

Various algorithm have been presented in image encryption as the *bit circulation* of pixels used in some encryption algorithm [4] in some other, blocks with changeable length from the plain image is encrypted to the blocks with same length in which the length of usable security key is various [5], some of the others divide the plain image to the block with certain sizes and use the key for making one pad and combination of generated pad with the plain image [6] the others change RGB levels and the

situation of any pixel with one another and use several chaos systems to produce chaos sequence [7].Some procedures convert 2D images to cubes then using 3D maps to encrypt these cubes ;thereafter, convert it to a 2D image [8].

In this article the OCML process used for permutation and standard map, Cat map are used for substitution of image pixels .To achieve more security through permutation and diffusion procedures in any round we can use obtained image from previous round in making parameters that have effective role in both.

We will explain *OCML* and *control block* in the second section of this paper, proposed *algorithm* in the third section, experimental *results* and *analysis of ACPS algorithm* in the fourth section and the last section concludes this paper.

2- Control Block and OCML Block

2-1-Control block

In proposed algorithm we have used a control block [9].In this block we employed three kinds of various maps, one control parameters generator, one diffusion block .Diagram shown in Fig.1.

2-1-1-Control Parameters Generator

By using input image in control parameters generator some parameters are produced to increase proposed algorithm security that would be as follow:

1-**M** parameter which is a function of variable ***r, s,*** pixel **(1,1)** and pixel(**N,N**) and this parameter employed as a logistic map iterative number.

2-***K*** parameter is equal to:

$$K=[X(M)\times 2^{36}]\ mod\ 2^{20} \quad (1)$$

3-***P*** parameter is equal to:

$$P=[X(M)\times 2^{24}]\ mod\ N \quad (2)$$

4-***Q*** parameter is equal to:

$$Q = ([X(M)\times 2^{48}]\ mod\ 2^{24})\ mod\ N \quad (3)$$

That ***N*** stands for image width and [] stands for integral sector.

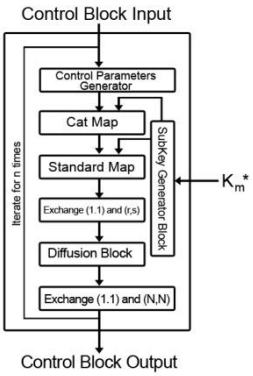

Fig.1. Block diagram of control block

2-1-2- Cat map

This map is chaos-based in which *R-level* is defined as follow:

$$\begin{bmatrix} x_{i+1}(R) \\ y_{i+1}(R) \end{bmatrix} = C \begin{bmatrix} x_i(R) \\ y_i(R) \end{bmatrix} mod\ N \quad (4)$$

In *ACPS* for permutation by using of cat map, we randomly employ four matrixes for *C*. in various rounds including:

$$\begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix}, \begin{bmatrix} PQ+1 & P \\ Q & 1 \end{bmatrix}, \begin{bmatrix} P & 1 \\ PQ-1 & Q \end{bmatrix}, \begin{bmatrix} P & PQ-1 \\ 1 & Q \end{bmatrix} \quad (5)$$

That ***P*** and ***Q*** are great by control parameters generator and the selection of C by using some part of secure key which is resulting of sub key generator block will be defined.

2-1-3-Standard map

The *standard map* is determined as:

$$X_{i+1}(R) = (x_i(R) + y_i(R)) \bmod N \quad (6)$$

$$y_{i+1}(R) = \left(y_i(R) + K(R)\sin\frac{2\pi X_{i+1}(R)}{N}\right) \bmod N \quad (7)$$

2-1-4-Logistic map

This map determined as in below [11]:

$$X_{n+1}(R) = \mu_R X_n(R)(1 - X_n(R)) \quad (8)$$

To reach a secure chaos system, one should consider restricted areas of the map parameters including:

$$\mu \in [3.9, 4] \quad , X(0) \in (0, 1) \quad (9)$$

2-1-5-Diffusion block

Calculate the cipher-pixel value according to:

$$C_R(k) = \phi_R(k) \oplus \{(P_R(k) + \phi_R(k)) \bmod G\} \oplus C_R(k-1) \quad (10)$$

The above formula will also be repeated for *G-level* and *B-level* that G in an image with a *256 RGB-scale* is equal to *256. P[k]* is equal to plain image that has various numbers in three levels of *R, G,* and *B.C[k]* is equal to output pixel running of diffusion block and *C (k-1)* is previous output pixel from diffusion block.

$$\Phi(k) = [X_2(k) \times 2^{2L}] \bmod 2^{2L} \quad (11)$$

$$L = \log_2 G \quad (12)$$

X_2 *(k)* is also gained from the logistic map.

2-2-OCML block

To substitute pixels at the basis of security key within plain image we use one-way coupled map lattice so-called *OCML* in the proposed algorithm [11, 13].

$$X_{n+1}(j)_R = (\alpha(j)_R . X_n(j)_R + \beta(j)_R . X_n(j-1)_R) \bmod 1 \quad (13)$$

$n = 1, 2, 3, \ldots, N \times N$, $j = 0, 1, 2, 3$

This formula is repeated in *B-level* and *G-level* as well .α*(j)* and β*(j)* are parameters of system and are secure key dependant .x_o *(j)* is primal term. X_n *(o)* is sequence key of *OCML*. Usable key in the block is a *192 bit* security key.

3-Proposed algorithm

We have emerged three processes of cat map, standard map and *OCML* in order to make a chaos alternative map In *ACPS* algorithm one-192 bit security key is used for making usable sub keys in different encryption rounds known as generating block .Outputs of the block are k_i and k_i^* that k_i is 192 bit used in *OCML* block and k_i^* is 96 bit used in control block .Encryption and decryption of *ACPS* algorithm shown in Fig. 2 and Fig.3.

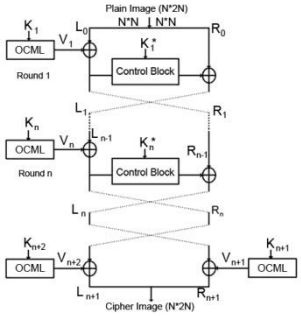

Fig.2. Block diagram of encryption process

To decrypt cipher image to plain image, we need original security key and specific pixel (r,s).

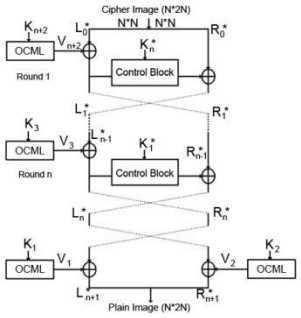

Fig.3. Block diagram of decryption process

The outcome of ACPS algorithm on *Peppers* image had been shown in Fig.4.

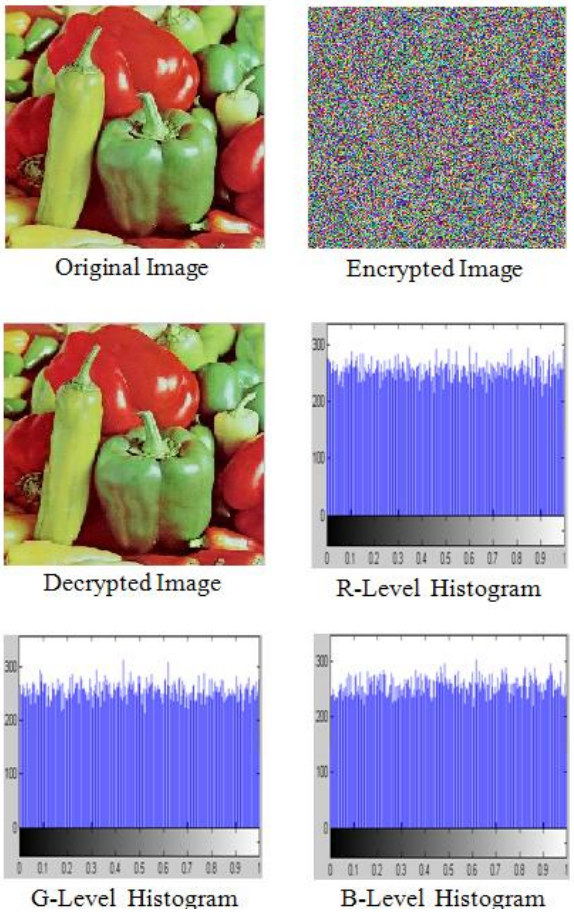

Fig.4. ACPS application on Peppers image

4-Practical results and secure analysis

4-1-Key space analysis

A good image encryption algorithm should be sensible to secure key and key space should be as long as enough that brute-force attack is impossible to break the cipher. In proposed algorithm in block control the key including primal numbers of μ_1, μ_2, $x_1(o)$,$x_2(o)$ that are coordinate of (r,s) and (r,s) $\in$ [1,N] and $\mu_1,\mu_2 \in [3,9,4]$ and $x_1(o),x_2(o) \in (0,1)$ Suppose precision of a floating-point number is 10^{-10} then $x_1(0)$ and $x_2(0)$ of each can be valued in 10^{10} states, μ_1 and μ_2 can also be valued in (4-3.9)*10^{10} states. Variables of *r* and *s* also have *N* states, and 96 bit key has 2^{96} states. Due to all of these parameters, key space is equal to $N^2 * 10^{38} * 2^{96}$ Because of using one-192 bit input key in OCML block, we have mood space equal to 2^{192} in any round for this key, so in this algorithm key space is generally equal to $N^2 * 10^{38} * 2^{192}$. On the basis of [14], IEEE standard, the computational precision of the 64-bit double-precision numbers is about $\mathbf{10^{-15}}$; therefore, the space of key space of the proposed algorithm can be elevated to $N^2 * 10^{58} * 2^{192}$ in specific usages.

4-2-Differntial attack

A small alteration in plain image should make considerable change in encryption image in order to resist differential attacks Evaluating the effect of change in plain image we use two common quantities measures to one extent of pixel .Number of Pixels Changing Rate (NPCR) and Unified Average Changing Intensity (UACI) are defined as follows[15]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times L} \times 100 \qquad (14)$$

$$UACI = \frac{1}{W \times L}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100 \qquad (15)$$

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (16)$$

In mentioned formula C_1, C_2 are two encrypted images whereas their plain images differ only in one pixel .The volume of parameters shown in table 1.

Table 1
NPCR and UACI at different rounds

	1	2	3	4
NCPR	0.0061	99.9939	100	99.9959
UACI	0.0014	33.3035	33.4071	33.3601

4-3- Statistical analysis

To resist statistical analysis, Shannon suggested using of diffusion and confusion [16].To consider correlation coefficient rate between two pixels we have employed 5000 pair of adjacent pixels in each of horizontal, vertical and diagonal directions in which correlation coefficient is equal to [17, 18].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \quad (17)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (18)$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \quad (19)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (20)$$

Table 2
Correlation coefficients of two adjacent pixels

	Plain-Image	Cipher-Image
Horizontal	0.8301	- 0.0077
Vertical	0.8658	- 0.0098
Diagonal	0.7547	- 0.0305

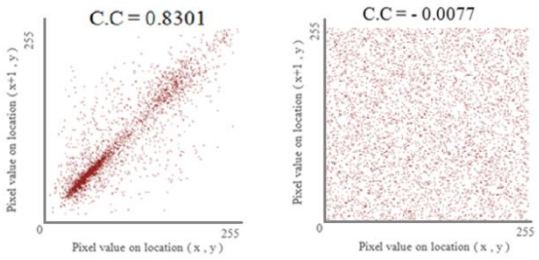

Fig.5. Correlation coefficients of two horizontally adjacent pixels

4-4- Key sensitivity test

Assume that a 24-character ciphering key is used. This means that the key consists of 192 bits. A typical key sensitivity test has been performed, according to the following steps:
First, a 256 * 256 image is encrypted by using the test key ***k***=''123456789012345678901234''.
Then, the least significant bit of the key is changed, so that the original key becomes, say ***k'***=''123456789012345678901235'' in this example, which is used to encrypt the same image. Finally, the above two ciphered images, encrypted by the two slightly different keys, are compared.
The result is: the image encrypted by the key ***k*** has 99.99% of difference from the image encrypted by the key ***k'*** in terms of pixel RGB-scale values, although there is only one bit difference in the two keys. Fig. 6 shows the test result.

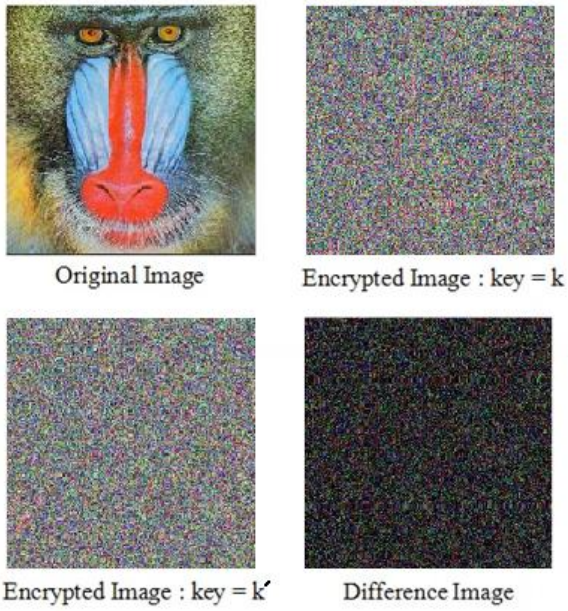

Fig.6.Key sensitive test

5- Conclusion

In this paper various maps have been applied. In regard to configurations of map and image usage for controlling of encryption procedure the outcome of loading compared with two recent years works was fantastic.[19,23] as if a number of rounds that are more than one contain UACI > 0.3330 and NCPR > 0.9999 and correlation rate among encrypted pixel are very low.

References

[1] Ogorzatek M J, Dedieu H. Some tools for attacking secure communication systems employing chaotic carriers. In: Proceedings of the 1998 IEEE Symposium on Circuits and Systems, Monterey, 1998.

[2] Alvarez G, Montoya F, Romera M, et al. Breaking two secure communication systems based on chaotic masking. IEEE Trans Circ Syst, 2004.

[3] Hu G J, Feng Z J, Meng R L. Chosen ciphertext attack on chaos communication based on chaotic synchronization. IEEE Trans Circ Syst, 2003.

[4] Shujun Li , Xuan Zheng . on the security of an image encryption method. The 2002 IEEE International Conference on Image Processing (ICIP 2002), September, 2002, Rochester, New York, Proceedings of ICIP 2002, vol. 2, pp. 925-928.

[5] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah . Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems. International Journal of Information Technology Volume 3 Number 4.

[6] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah. An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption . 2005.

[7] C.K. Huang , H.H. Nien . Multi chaotic systems based pixel shuffle for image encryption, 2009.

[8] Guanrong Chen , Yaobin Mao , Charles K. Chui , A symmetric image encryption scheme based on 3D chaotic cat maps , 2004.

[9] Yong Wang , Kwok-Wo Wong , Xiaofeng Liao , Tao Xiang , Guanrong Chen . A chaos-based image encryption algorithm with variable control parameters , 2008.

[10] Gabriel Peterson . Arnold's Cat Map , Math 45 – Linear Algebra,1997.

[11] ZHANG YiWei , WANG YuMin , SHEN XuBang . A chaos-based image encryption algorithm using alternate structure, 2007.

[12] Kwok-Wo Wong , Bernie Sin-Hung Kwok , Wing-Shing Law . A fast image encryption scheme based on chaotic standard map , 2008.

[13] Rhouma Rhouma , Soumaya Meherzi , Safya Belghith . OCML-based colour image encryption , 2007.

[14] IEEE Computer Society. IEEE standard for binary floating-point arithmetic, ANSI/IEEE Std. 754-1985; August 1985.

[15] Sahar Mazloom , Amir Masud Eftekhari-Moghadam . Color image encryption based on Coupled Nonlinear Chaotic Map , 2009 .

[16] Shannon CE. Communication theory of secrecy system. Bell Syst Tech J 1949;28:656–715.

[17] Tiegang Gao , Zengqiang Chen . Image encryption based on a new total shuffling algorithm , 2008 .

[18] S. Behnia , A. Akhshani , H. Mahmodi , A. Akhavan . A novel algorithm for image encryption based on mixture of chaotic maps , 2008 .

[19] Xiaojun Tong , Minggen Cui . Image encryption with compound chaotic sequence cipher shifting dynamically , 2008 .

[20] Tiegang Gao , Zengqiang Chen . A new image encryption algorithm based on hyper-chaos , 2008 .

[21] Xiaojun Tong , Minggen Cui , Zhu Wang . A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator , 2009 .

[22] Kwok-Wo Wong , Bernie Sin-Hung Kwok , Ching-Hung Yuen . An efficient diffusion approach for chaos-based image encryption , 2009 .

[23] Fuyan Sun , Shutang Liu , Zhongqin Li , Zongwang Lu . A novel image encryption scheme based on spatial chaos map , 2008 .