Color Image Encryption using Hyper Chaos Chen

Danial Roohbakhsh
Department of Electrical Engineering, Mashhad
Branch Islamic Azad University, Mashhad, Iran
IT Specialist, Social Security Organization,
Mashhad, Iran

Mahdi.Yaghoobi
Department of Electrical Engineering, Mashhad
Branch Islamic Azad University,
Mashhad, Iran

ABSTRACT

In this paper, a color image encrypting method based on chaos theory is introduced. Image encryption because of some intrinsic features of images, such as high data volume and high correlation among pixels, the encrypting text is different. For this reason the classic method of encrypting text for this purpose is not high performance. For two reasons, the proposed method compared with other methods with high security. First, use the hyper chaos and the second large of the space key. In the simulation results, various experiments have been conducted to analyze the security of the proposed method.

Keywords

Encrypting, Information, Security, Hyper chaos

1. INTRODUCTION

Today, with advances in technology and increases in charge of computers, data volume also increased. Hence, the researchers sought to minimize the information, and at the same time, high security [1]. Use the old methods of encrypting, because the calculations high do not apply. On the other hand, information security should be considered at all times. Recently, the use of chaos functions for encrypting data of interest is located. Chaotic dynamics of some features that are important, it is very sensitive to initial conditions (that is, very little difference in the initial conditions that will change future behavior of the rate difference is proportional to Lyapunov exponent) [2]. First in 1989, was used for the encryption from chaotic systems [3]. More research has been introduced to provide encryption methods, most of which have used the properties of chaotic systems [4]. Recently, different methods based on chaos theory is used for encrypting, such as quick encryption [5], encrypting block [6] and Neural Networks [7] mention. An important principle in sensitive cryptographic keys is wrong. Also, if the key is large enough to be resistant against attacks. Hence, due to the inherent complexity of the chaos, the encryption strength will be greater [8]. In this paper, an adaptive color image encryption method based on chaos we'll discuss. Using MATLAB simulation was performed, and the test commonly used in image processing on the proposed encryption algorithm is studied. The proposed method consists of two main parts, the logical sequence of pixels with Arnold chaotic map disappears. Then in the second stage, the image is distorted in the hyper chaotic Chen system is encrypted. In the next section, we will discuss a little about Arnold mapping. In the next section, the chaotic Chen system will be discussed. In the fourth part of the proposed method is presented in fifth section Simulation results show that the proposed method is robust encryption.

2. ARNOLD MAPPING

In 1960, Russian mathematician Vladimir Arnold used the most general two-dimensional chaotic map for an image [9]; the name was Arnold Cat Map. If a matrix N * N, pixel with coordinates (x, y), we wrote to Arnold in equation (1) will be:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) = \begin{bmatrix} I & t \\ q & tq+I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{modN}) \qquad (1)$$

Which q and t are the control parameters of the matrix A, and should be chosen so that the determinant of the matrix A is equal to one. These two parameters will be part of the encryption key. Fig.1 shows the falling cat image by mapping Arnold. Mod is the remainder divided by n, for each of the components. This is because the values obtained from the image matrix size are not exceeded. Pixels of an image map Arnold moved, so the image cannot be understood, if it is sufficient to repeat the original image will be generated again.

3. HYPER CHAOS CHEN DYNAMIC

The Chen system is described by the hyper chaotic dynamic such as:

$$\begin{aligned} \dot{X}_1 &= a(x_2 - x_1) \\ \dot{X}_2 &= -dx_1 + cx_2 - x_1 - x_4 \\ \dot{X}_3 &= x_1 x_2 - bx_3 \\ \dot{X}_4 &= x_1 + k \end{aligned} \qquad (2)$$

Where $x_i (i = 1, 2, 3, 4)$ the states and a, b, c, d are positive constant parameters of the system and -0.7<k<0.7 [10].

If the parameters of equation (2) as: $a = 36, b = 3, c = 28, d = -16$, behavior of the system (2) as shown in Fig.2 will be.

4. THE PROPOSED METHOD

a. Mapping

In this process by Arnold mapping the pixels of the original image is cluttered. Arnold wrote 7 (it=7) times on the original image are applied, so that the image is completely incomprehensible and also greatly reduces the correlation between the pixels. Figure 3 shows the steps described.

b. Encryption using Hyper Chaos Chen

At this stage, the pixels in disarray, and their values using hyper chaotic Chen encryption. First, one of the four variables produced by Chen is set aside. The system repeats the number of all pixels in the image. Index variable that will be excluded from the equation (3) becomes apparent.

$$\begin{cases} index = \mathrm{mod}((x_1 + x_2 + x_3 + x_4), 4) \\ index = index + 1 \end{cases} \quad (3)$$

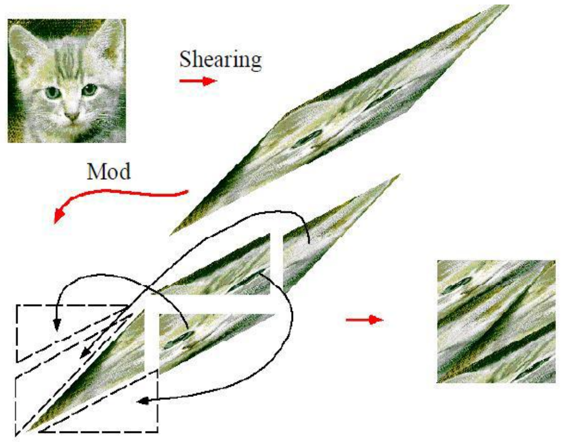

Fig.1 Arnold mapping process

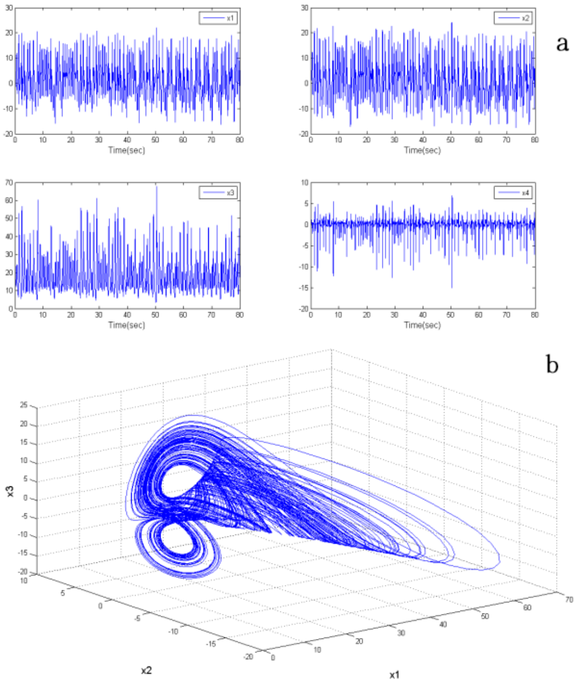

Fig.2 a: State variables and b: Phase plane trajectory of hyper Chen system

For all pixels, all $i = 1, 2, 3, 4$ are calculated, and the remainder divided by 4, the index variable is stored.

In the second phase, the remaining three variables from the previous stage, respectively, with the colors red, green and blue pixels are all cluttered image according to equation (4).

$$\begin{aligned} CR_i &= R_i \oplus (x_1)_2 \\ CG_i &= G_i \oplus (x_2)_2 \quad\quad (4) \\ CB_i &= B_i \oplus (x_3)_2 \end{aligned}$$

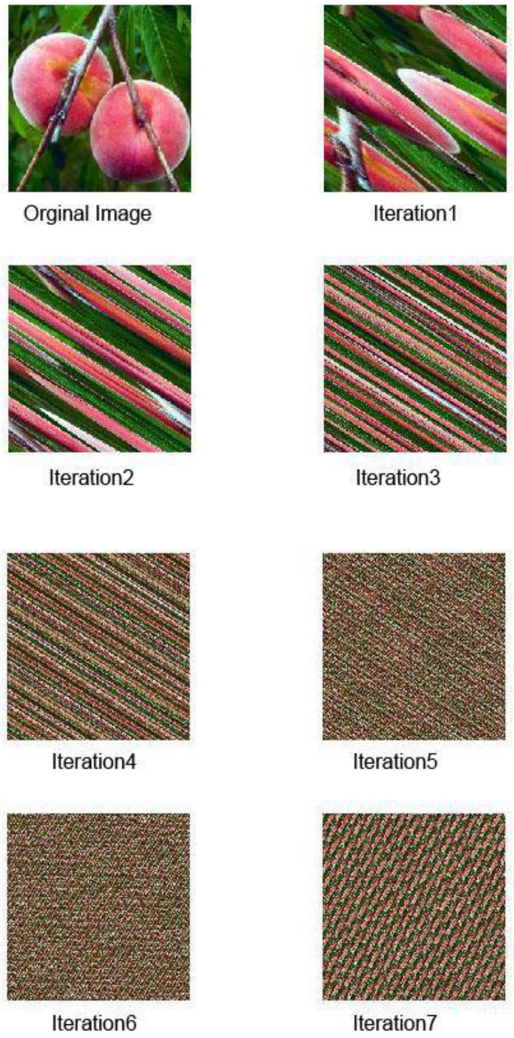

Fig.3 Arnold mapping the image on fruit

c. Decrypt

The decryption of the proposed method will be discussed. The algorithm to decrypt the encrypted image, Chen the basic values of the parameters t, q, and number of repetitions of the Arnold map is available.

Now we should all go back to decryption of process to be reversed. The initial value x_i and system parameters Chen is the key, so x_i is in the stage production. Then, according to equation (3), we calculate the index is excluded. Finally, the color of each pixel of the image is encrypted with xi according to equation (4) is XOR.

Now, at this stage, the first step is reached. Now, at this stage, the first step is reached. The seven steps, we can apply the inverse Mapping Arnold on the image to the original image is reached (Note: The number of repetitions Arnold Mapping is part of the key). The inverse Arnold map to the original image in the form of equation (5) obtained.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{modN}) = \begin{bmatrix} tq + I & -t \\ -q & I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{modN}) \quad (5)$$

5. EXPERIMENTAL RESULTS

In this section, experimental results obtained using MATLAB software will be described. Performance of the proposed method is evaluated by tests will be common in image processing.

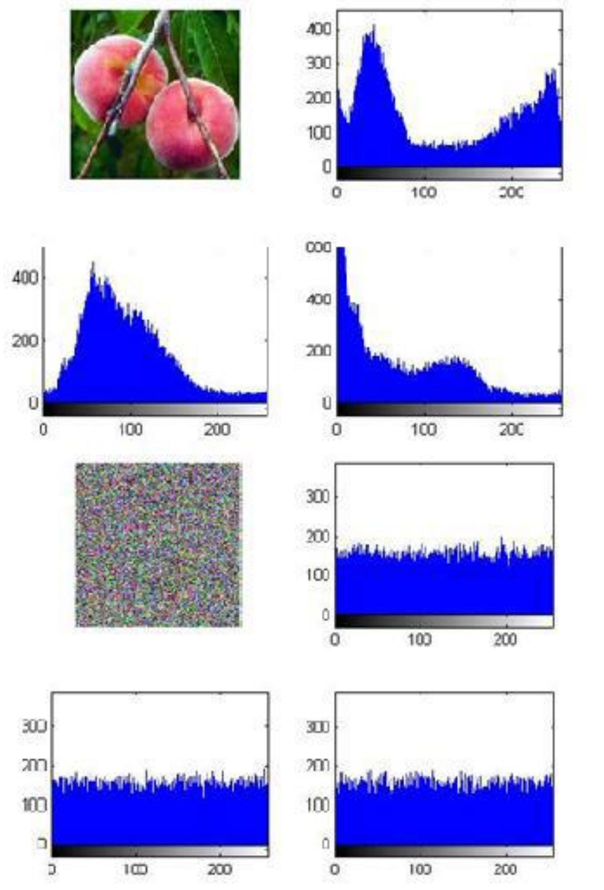

Fig.4 histogram of the original image and encrypted image

a. Histogram analysis

Histogram, show the number of pixels in each gray level for an image [11]. By comparing the encrypted image and the original image, it can be seen that the proposed method of image histogram encoded by appropriate uniformity. That is to say, the probability calculated from the histogram of the original image by the attackers will be very weak. To better understand, see Fig.4

b. Sensitivity to the wrong key

Sensitivity to key mistake in this article only for Chen system parameters is studied. If you enter the correct parameters are expected in other words, the image of Arnold Mapping get cluttered. Now, beginning with the correct key, and then with little change in the parameters, trying to get the image Mapping. In other words, this test shows that the chaotic system is sensitive to the initial conditions. Hyper Chen system with the initial conditions are $x_0 = [12 \quad 8 \quad 25 \quad 4]^T$, and with a little different initial conditions are $x_0 = [12 \quad 8.000001 \quad 25 \quad 4]^T$. Table 1 illustrates results.

c. Key space analysis

Decryption key of the proposed method are: $(t, q, it, x_{1,2,3,4}, \mathrm{a, b, c, d, k})$, that the values as : (1,1,7,12,8,25,4,36,3,28,-16,0.4) respectively, Calculating the size of the key binary code (00101100), and the 8 bits allocated to each of them. This means that there are 2^{184} possibilities for the permutation. Desired key length to resist fierce attack by guessing is 70 bits [13]. Hence, the key will be achieved by the proposed method highly desirable.

d. The proposed method of resistance against attacks

In fact, a frenzied attack, guess the key through the various permutations. On the other hand, specific encryption mechanisms and the key are needed. Otherwise attack exposure cannot be applied [15]. Due to the hyper chaotic Chen system and the stage of bollix, key length is long. So, it is almost impossible to guess the key is to have a great time. Attack Rhouma and Belghith, one of the most interesting episodes introduced to deal with the chaos-based encryption. However, when used in the encryption mechanism is available. Otherwise, image access to, image encrypted by not possible [16]. The solution to this type of attack is that for each image, different values of the parameters and initial conditions in hyper chaos, is available.

6. CONCLUSION

In this paper, a color image encryption method based on chaos was introduced. First, the picture becomes cluttered Arnold mapping, then the image obtained with the combination of by hyper Chen chaos. The results of the simulation are: 1. simple structure 2. Sensitivity of hyper chaos 3. To implement bollix image obtained 4-length key. It was demonstrated that the proposed method can resist the attack of the crazy.

7. REFERENCE

[1] Geol, Amnesh, and Nidhi Chandra, “A Technique for Image Encryption with Combination of Pixel Rearrangement Scheme Based On Sorting Group-Wise Of RGB Values and Explosive Inter-Pixel Displacement”, pp.16-22, 2012

[2] J.C. Yen, J.I. Guo, “A New Chaotic Key-Based Design for Image Encryption and Decryption”, Proceeding IEEE International Conference on Circuits and Systems,vol.4, pp. 49-52, 2000

[3] R.Valerij, “Symmetry of the modified Mandelbrot set”, Pi in the Sky(9):20–1.2005

[4] Narendra Singh, Aloka, “Optical image encryption using fractional Fourier transform and chaos”, Optics and Lasers in Engineering.Vol 46, Issue 2, Pages 117–123.February 2008

[5] Kadir, Abdurahman, Wang, “A chaotic image encryption algorithm based on perceptron model”, Nonlinear Dynamics, Vol. 62, pp. 615-623,2011.

[6] Liao X, Chen G, Wang Y, “A new chaos-based fast image encryption algorithm”, Applied Soft Computing Journal, Vol.11, PP. 514-522,

[7] Alireza Jolfaei, Abdolrasoul Mirghadri, “Image Encryption Using Chaos and Block Cipher”, Computer and Information, Vol 4, No 1,pp 172-179, 2011.

[8] Tiegang Gao, Zengqiang Chen, “"A new image encryption algorithm based on hyper-chaos”, Physics Letters A ,Vol.372, Issue 4, PP 394–400, 21 January 2008

[9] R Jun, P., J. Shangzhu, and L. Yongguo,” Design and Analysis of an Image Encryption Scheme Based on

Chaotic Maps", International Conference ICICTA, pp. 1115-1118, 2010

[10] Li, Ling, Weinan Wang, and Jinjie Li, "A Novel Image Encryption Algorithm Based on High-dimensional Compound Chaotic Systems ", International Conference on Multimedia Technology (ICMT), pp.5715-5718, July 2011.

[11] Jolfaei, Alireza, and Abdolrasoul mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp120-122, 2010

[12] S, Rakesh, Ajitkumar A Kaller, Shadakshari B C, and Annappa B, "Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping", International Journal on Cryptography and Information Security, (IJCIS),Vol.2, No.1, pp 49-57, 2012.

[13] Gao, Tiegang, Qiaolun Gu, Zengqiang Chen, and Renhong Cheng, "An Improved Image Encryption Algorithm Based on Hyper-chaos", Fourth International Conference on Innovative Computing Information and Control (ICICIC), pp.1281-1284, 2009

[14] Prasad, Manjunath, and K.L.Sudha, "Chaos Image Encryption using Pixel shuffling.",pp.170-177, 2011

[15] Bruce Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C", John Wiley & Sons, Inc, Publication Date 1996

[16] R, Rhouma, and Belghith S "Cryptanalysis of a new image Encryption Based on hyper chaos", Physics letters pp.5973-5978, 2008