A Summary of image Encryption Algorithm Based on Chaotic Sequence

Yukun Guo*

School of Information & Techonlogy Center, Hexi University, Zhangye, Gansu, 734000, P.R. China

Abstract: As a kind of special nonlinear phenomenon, chaos has a series of excellent features such as pseudo-randomness, orbit unpredictability, the extreme sensitivity to initial conditions and system parameters, non-repetition of iteration, and so on. Because an increasing number of widely used image and multimedia information has characteristics such as large amount of data and high redundancy, it has become a challenge to the traditional encryption technology. Having natural randomness and concealment, chaotic signal is well fit for secrecy communication.

Keywords: Chaos, hyper-chaos, image encryption algorithm, redundancy.

1. INTRODUCTION

In 1963, Lorenz published Determinism Aperiodic Flow, then the famous Lorenz Equation was given, which was the first example that a deterministic equation can export the chaotic solution in the dissipative system, thus opening a prelude to the in-depth study of chaos. The emergence of chaos put an end to the classical science [1-5].

In 1975, Chinese-American Li Tianyan and American mathematician Yorke published a paper Cycle 3 Contains Chaos which shocked the academia. The word Chaos was used in the literature for the first time, which set a precedent for chaos research. In 1989, Robert A. J. Matthews published a paper to analyze the question that Logistic chaotic map acted as sequence key stream generators and improved it. He proposed a chaotic stream cipher scheme based on deformation Logistic map. It is the first essay clearly putting forward chaotic password, getting wide attention and reference. Concerned by more and more researchers from different fields, chaotic password became a hot spot.

In 1989, L. M. Pecora found that when certain conditions are met, chaotic systems can be constructed into a synchronization system. Such synchronization chaos can be used to communicate. In the same year, Carroll constructed the first synchronized chaotic circuit, thus people began the study of the chaotic sequence cipher. Many magazines and meetings such as Physics Letters A, Int. J. Bifureation and Chaos, Physiea l Review, IEEETrans. on Circuits and System, IEEEInt.Sy, Osiumon Circuits and Systems, published a great number of research results related to chaotic cipher.

In 1998, Baptista and E. Alvarez put forward a scheme to look up cleartext in the phase space of chaotic system based on the retrieval mechanism of chaos encryption and secrecy communication. These chaotic passwords opened up a new direction for the study of chaotic encryption despite the fact that they have been successfully deciphered. Subsequently Carrol *et al.* proposed the sequence password generator based on Lorenz system, and Bernstein *et al.* proposed the sequence password generator based on the first-order non-uniform sampling digital PLL system.

In 2002, Jin-hu *et al.* proposed a new 3D chaotic system by connecting the Lorenz system and Chen system.

In early 2007, Kocarev *et al.* proposed an encryption algorithm based on Logistic chaotic mapping grouping, which discussed the characteristics such as diffusion and disorder that chaos has and cryptography demands. J. Fridrich proposed a symmetric encryption algorithm based on two-dimensional Baker chaos mapping which is used in image encryption.

In 2011, Lu Huibin and Sun Yan published a paper Image Encryption Scheme Based on the New Hyper Chaotic System, in which hyper chaos was proposed. A new hyper-chaotic system was constructed and a new scheme of image encryption based on this hyper chaotic system was put forward as well. In the four-dimensional mapping system, with the increase of parameter and system variables, the key room is increasing too, thus resisting exhaustive attack effectively. The encrypted image pixel is distributed randomly and will result in higher security.

2. THE DEVELOPMENT OF IMAGE ENCRYPTION ALGORITHM BASED ON CHAOS SEQUENCE

2.1. The Design of Image Encryption Algorithm Based on Improved Logistic Mapping

One-dimensional Logistic mapping is a very simple chaotic mapping from the perspective of mathematics. It is also of the early typical chaotic systems. It sets a precedent for the development of the chaotic sequence.

(A) The definition of Logistic mapping

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

1874-4443/14 2014 Bentham Open

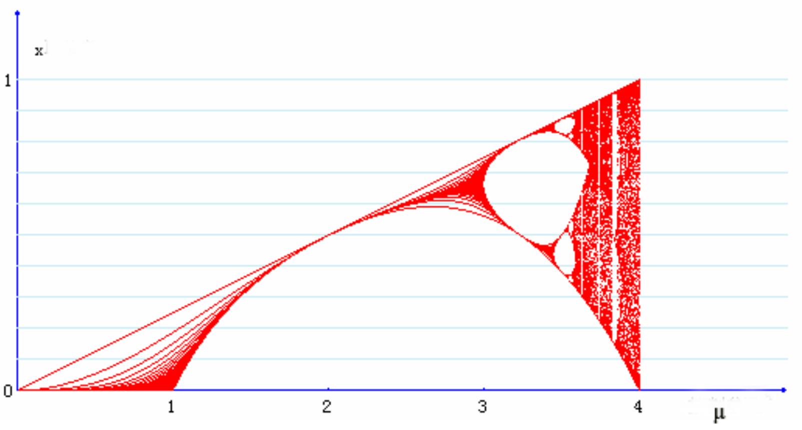

Fig. (1). Logistic mapping trajectory.

The simplest map contains the basic idea of modern chaos theory including period doubling bifurcation and basic framework and mode of nonlinear theory. When 3.569945<μ ≤4, Logistic map shows a chaotic state.

(B) The random likeness of Logistic mapping

In the formula (1), set the initial value X0 = 0.5, parameter μ =3.98, generating a chaos sequence whose length is 300. It is observed that Iterative values are generated in a pseudo-random distribution state while μ∈[0,4] is especially close to 4. While in other values, generated values will converge to a specific value after a certain number of iterations, which is unacceptable for us.

Fig. (**1**) describes when the X0 values are given, the value iteration may get for different values of μ :

Points in the graph indicates all possible X ranges. We can see from the figure that the value range of X are more close to the average distribution in the 0 to 1 area where μ is the closer to 4. In this range, the value range of X is more close to the average distribution in the 0 to 1 area, so it is better that the Logistic control parameters we need to choose should be closer to 4.

(C) The improved Logistic mapping

Due to chaotic pseudo random probability statistics method can be used to the quantitative study of the characteristics of chaotic sequence. It is easy to prove that Logistic mapping does not meet the uniform distribution. In order to get better uniform distribution and random system, the formula (1) can be changed as follows:

$$y_n = \frac{1}{\pi}\sin^{-1}(\sqrt{x_n}), n = 1,2,3... \tag{2}$$

$$F\{y \le Y\} = F\left\{x \le \sin^2(\frac{\pi Y}{2})\right\}$$

$$= \int_0^{\sin^2(\frac{\pi Y}{2})} \rho(x)\,dx \tag{3}$$

$$= \int_0^{\sin^2(\frac{\pi Y}{2})} \frac{1}{\pi\sqrt{x(1-x)}} dx = Y$$

Therefore, the probability distribution function of the variable y is as follows:

$$\rho(Y) = \frac{dF}{dY}\{y \le Y\} = 1 \tag{4}$$

We found that type (4) satisfies uniform distribution in (0,1) region, the random distribution is better than type (1).

(D) Encryption algorithm description

Set A (M × N) to represent that the image size is M × N, A(x,y), x∈[0,M-1], y∈[0,N-1]) represents the gray value at point (x, y) of image A,A`(x,y)(x∈[0,M-1], y∈[0,N-1]) represents the encrypted gray value at point (x, y).

When designing encryption algorithm, set 4 initial parameters, two as parameters μ1 and μ2 of the Logistic system and the other two for the initial system value X10` and X20`, to build two groups of chaotic sequence y1{i}and y2{i} and carry out XOR of pixel gray value of the original image one by one. If you get an odd point, carry out XOR with y1{i} sequence encryption; if you get an even point, carry out XOR with y2{i}.

2.2. Color Image Encryption Algorithm Based on Two-dimension Cat Map Chaotic System

The cat mapping [5] was first introduced by Arnold. It is so named because it is often demonstrated using a cat face. The equation of the formula is as below:

$$\begin{cases} x_{n+1} = (x_n + y_n) \bmod 1 \\ y_{n+1} = (x_n + 2y_n) \bmod 1 \end{cases} \tag{5}$$

mod1 shows that only the decimal part is taken, that is, x mod 1=1-[x], therefore, the phase space (x_n, y_n) is limited to the unit square $[0,1]\times[0,1]$. Transform Type(5) into matrix form as below:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix} = C\begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \tag{6}$$

Type (6) defines matrix C, and cat mapping is an Area Preserving Map (no attractor) for |C|=1. At the same time the cat mapping is a one-one mapping, so every point in the unit matrix shifts to another point uniquely in the unit matrix. Cat mapping has the two typical factors generating chaotic motion, stretching (to multiply matrix C to enlarge x and y) and folding (modulus makes x and y return to matrix again). Actually, cat mapping is chaotic mapping.

Extend the cat mapping as follows. Firstly, extend the phase space to {0, 1, 2, ⋯, N-1}×{0, 1, 2, ⋯, N-1}, that is, only take the positive integer from 0 to N-1; Secondly, extend the equation to the most general two-dimensional reversible area preserving equation:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \mathrm{C} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod \mathrm{N} \qquad (7)$$

a, b, c, and d in the formula are positive integers, whose conservative area requires |C|=ad-bc=l. Under this requirement, only three parameters of a, b, c, and d are independent. For instance, we can set a, b, and c independent, then d is decided by the criterion of the conservative area.

Formula (7) can also written as,

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \bmod \mathrm{N} \qquad (8)$$

It can be seen from formula (8) that this mapping has a fixed point (0,0), that is, point (0,0) does not change after n iterations. In order to avoid fixed point, do a modular operation on the initial point (x0, y0) after n iterations, then add 1 to the results as the new coordinates (xn, yn), then formula(8) can also be transformed as:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & \mathrm{b} \\ \mathrm{c} & \mathrm{d} \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \mathrm{C}^{\mathrm{n}} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \bmod \mathrm{N} \; +1 \qquad (9)$$

Transform formula (9) into formula (10) which have two independent parameters:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & \mathrm{p} \\ \mathrm{q} & \mathrm{pq+1} \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \bmod \mathrm{N} \; +1 \qquad (10)$$

Formula (10) indicates a new coordinate (xn, yn) after adding 1 to the result of nth iterative computation initial point (x0, y0). It can be proved that formula (10) has some characteristics of the chaotic mapping which are one-one mapping. Therefore, we can use formula (10) to scramble the points of plaintext image pixel dots, i.e., Put each pixel coordinates (i, j) of the original plaintext image as the initial value (x0, y0), with the given coefficient matrix (determined by the independent parameters p, q) and the iterations n as encryption key. Put the generated iteration results (xn, yn) as the new point (i `, j`) which is replaced from the original image pixel point (i, j).

When designing the encryption algorithm based on this mapping, use generalized cat mapping to scramble each pixel of three primary colours separately, and the RGB tricolor of image A to be encrypted respectively use different key parameters (pi, qi, ni) to calculate the new coordinates RA (xi,yi), GA（xi,yi), BA（xi,yi）of RGB using x=x0+p*y0 and y=p*x0+(q*p+1)*y0. Then we can use the new tricolor coordinate to scramble images. Finally, compound the scrambled images and we`ll get a new matrix A1 to decrypt it through anti-operation.

$$\begin{cases} x = x0 + p * y0 \\ y = p * x0 + \left(q * p + 1\right) * y0 \end{cases} \qquad (11)$$

3. THE ENCRYPTION ALGORITHM BASED ON GENERALIZED CAT MAP AND 3D UNIFIED CHAOTIC SYSTEM

In 2011, Jin-hu *et al.* [3] proposed a new 3D chaotic systems, which connects the Lorenz system and Chen system, while the Liu system is only a special case. For these reasons, it was called the unified chaotic system. The formula is as below:

$$\begin{cases} x' = (25\alpha + 10)(y - x) \\ y' = (28 - 35\alpha)x - xz + (29\alpha - 1)y \\ z' = xy - (8 + \alpha)z / 3 \end{cases} \qquad (12)$$

$\alpha \in [0,1]$ in formula(12). In this range the system has global chaotic characteristics. When α =0.8 this system belongs to the generalized Liu system, when α <0.8 this system belongs to the generalized Lorenz system, and when α >0.8 this system belongs to the generalized Chen system.

In the cat map encryption algorithm, only the plaintext matrix is scrambled while the pixel is not substituted. Then the new algorithm produced does RGB three tricolor gray value substitution encryption to the previous image scrambled by cat mapping with the three sequences x, y, and z of the unified chaotic system. Furthermore, different keys are taken for each pixel. Methods to construct keys is to take 3 numbers after the decimal point as positive integer, then do modulus operation to 256 to construct keys. The generated cipher image not only uses cat map to scramble but also use keys calculated from equation (12) for gray value substitution. Thus the complexity of chaotic sequences is greatly improved and can resist various attacks. Therefore, the arithmetic has higher security.

4. SUPER CHAOS AND ITS APPLICATION ON IMAGE ENCRYPTION

In 2013, Lu *et al.* [6] constructed a new hyperchaotic system and put forward a new image encryption scheme based on the chaotic mapping. With the increase of variable parameters and system variables of the four-dimensional mapping, number key increases too. Thus chaotic system becomes more complicated and can resist various attacks more effectively with higher security.

The new kinetic equation hyperchaos system is as follows:

$$\begin{cases} x` = a\left(y - x\right) \\ y` = bx - xz + \omega \\ z` = -cz + dx2 \\ \omega` = -ry \end{cases} \tag{13}$$

In equation (13), when a=10, b=45, c=2.5, d=4, and r=5 [6-8], the system has a typical chaotic attractor, which will generate chaotic attractor image by using the fourth order Runge-Kutta discretization algorithm to iterate 10000 times and then taking the last 9900 data sets.

Chaotic sequence generated by this four-dimensional hyperchaotic system has the following characteristics: 1) system structure is more complex than lower dimension system; 2) when the sequence produced by the system is processed, encryption chaotic sequence of the combination of single variable or multi-variable can be produced; 3) system has a huge key space.

When designing encryption algorithm, still use the method of disturbing high correlation between adjacent pixels in an image, that is, to scramble the image matrix according to the coordinates.

Hyperchaotic sequence should be constructed first. After giving the initial value, use the fourth order Runge-Kutta discretization algorithm to iterate for N0 times, generating 4 chaotic sequence, x1(k), x2(k), x3(k), and x4(k). Its first 10000 values are abandoned and then use the values after that as chaotic sequence to construct new chaotic sequence:

$$\begin{cases} x1\left(k\right) = abs\left(x1\left(k\right)\right) - fix\left(x1\left(k\right)\right) \\ x3\left(k\right) = abs\left(x3\left(k\right)\right) - fix\left(x3\left(k\right)\right) \end{cases} \tag{14}$$

Use the new sequence X1 (k) and X3 (k) as the line number and column number of plaintext matrix to scramble the plaintext, then obtain the encrypted image.

This algorithm only changes the pixel point while the gray histogram of the image is not changed, thus the security is still not high. The following algorithm will encrypt the scrambled cipher text by pixel value substitution.

1）Modulus operation to 256 of the positive integers composed of the four chaotic sequences generated by hyperchaotic system performed and then the secret key can be obainted. The key formula is as follows,

xi=mod(fix(abs(xi)-floor(abs(xi))*1015),256) i=1,2,3,4

2) To produce x0`, x0`=mod(x4,4). When x0`=0, use sequence (x1, x2, x3); when x0`=1; use sequence (x2, x3, x4); when x0`=2, use sequence (x1, x3, x4). Take 3 pixels at a time from the scrambled cipher text images, do the XOR encryption one by one respectively according to the value of x0`. The ciphertext has the effect of scrambling and pixel substitution. The pixels of the cipher image are distributed in [0, 255], with higher security.

5. SUMMARY AND FUTURE OUTLOOK

Overall, the dimension and complexity of chaotic sequences are increasing, thus the constructed encryption sequences are more complex and the key space is larger. There are three encryption methods: the image coordinates scrambling, the pixel value XOR substitution and the combination of the two methods.

Although many chaotic encryption scheme have been proposed and chaotic system is becoming more and more complex, the chaotic cryptology theory is not fully mature. At present, most of the chaotic encryption systems are using natural chaotic system. They may not have strict confidentiality in cryptology. Actually, defects have been found in many chaotic cryptography methods. For instance, Short decoded chaotiemasking decipher and the chaotiemasking encryption scheme which are developed by the United States Navy Research Institute by using NLDforecasting methods. Moreover, Wheeler also pointed out that there is severe finite precision effect in Matthews' chaotic sequences cipher, so it was not suitable for practical applications [7, 9-11].

Study chaotic cryptography is still a leading challenging topic. Hence, intensive research needs to be done on chaotic encryption mechanism, and how to fully use chaotic system to encrypt digital image. Chaotic system have a large number of results, to evaluate the abundant prior research results and the security of chaotic ciphers, and overcome the finite precision effect should be the focus of future result.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] C. Y. Guan, and F. Gao, “A encryption algorithm based on chaos sequence,” *Journal of Beijing Institute of Technology*, vol. 23, no. 3, pp. 363-366, 2003.

[2] C. J. Wang, and F. Zhang, “A new algorithm for communication,” *Computer & Digital Engineering*, vol. 34, pp. 26-31, 2006.

[3] D. Tang, and Z. T. Li, “A image algorithm based on chaos sequence,” *Computer engineering and Science*, vol. 25, no. 4, pp. 7-9, 2003.

[4] Y. R. Wang, Y. Wang, and X. S. Zhan, “Analysis of the performance of the algorithm of image encryption based on Chaos,” *Journal of Henan University*, vol. 36, no. 2, pp. 88-90, 2006.

[5] J. A. Gonzalez, “Absolutely unpredieatable chaotic sequences,” *International Journal of Bifurcation and Chaos,* vol. 10, no. 8, pp. 1867-1874, 2000.

[6] H. B. Lu, and Y. Sun, “Image encryption scheme based on new hyper chaotic system,” *Journal of Computer Science*, vol. 38, no. 6, pp. 149-152, 2011.

[7] X. Sun, K. X. Yi, and Y. X. Sun, “A image encryption algorithm based on Chaos System,” *Journal of Computer Aided Design & Computer Graphics*, vol. 14, no. 2, pp. 136-139, 2002.

[8] H. Cheng, and X. Li, “Partial eneryption of compressed images and videos,” *IEEE Transactions on Signal Processing,* vol. 48, no. 8, pp. 2439-2451, 2000.

[9] S. Q. Pang, Y. J. Liu, and C. X. Zhu, “Implementation and application of circuit hyperchaotic Lorenz system,” *Computer Engineering and Applications*, vol. 49, no. 7, pp. 235-239, 2013.

[10] P. P. Dang, and P. M. Chan, “Image encrption for secure Internet multimedia applications,” *IEEE Transactions on Consumer Electronics,* vol. 46, no. 3, pp. 395-403, 2000.

[11] J. Yen，and J. Guo, “A new chaotic key-based design for image eneryption and decryption,” *ISCAS2000 IEEE-International Symposium on Circuits and Systems,* Geneva, Switzerland, 2000.

Received: November 13, 2014 Revised: December 17, 2014 Accepted: December 19, 2014