

An Approach of Image Hiding and Encryption Based on a New Hyper-chaotic System

Hongxing Yao , Meng Li*

Institute of System Engineering, Jiangsu University, Zhenjiang 212013, PR China

(Received 9 November 2008, accepted 21 November 2008)

Abstract. This paper presents an improved image hiding method based on a new hyper-chaotic system. The binary sequences that generated based on the new hyper-chaotic system are applied to pre-encrypt the image, including improved magic- cube scrambling and pixels permutation; then further processing are used to hide the pre-encrypted image. The effect of hiding is also analyzed by using the method of accessing. Simulation results of this method indicate that the method has good efficiency and security characteristic.

Keywords: hyper-chaotic system; binary sequences; image hiding; image encryption.

1 Introduction

The development of Internet provides a new way for digital information which can be made spreading faster and more conveniently. Because of the characteristic of digital images, some security problems come out besides the extensive usage of these images. Therefore, credible encryption techniques for digital images are indispensable and necessary for protecting the rights and interests of data owner, copyright and person's right to privacy[1]. Some traditional encryption techniques are not suitable for encrypting the digital images because of the differences between letter and digital image, some new methods were applied to such areas as encrypt images based on chaotic systems. Over the last decade various effective methods have been proposed and utilized to achieve the control and stabilization of chaotic systems, even to experimental systems like Cryptography etc[2].

Nonlinear chaotic systems have been extensively studied within scientific, engineering and mathematical communities[3]. In 1963, Lorenz found the first chaotic attractor in a three-dimensional autonomous system when he studied atmospheric convection. Since then, Several control schemes have been successfully established[4], and the Lorenz system has been extensively studied in the field of chaos theory and dynamical systems and been used in some method about image encryption. For a chaotic system, there is just one positive Lyapunov exponent. Messages masked by such simple chaotic systems are not always safe[5]. It is suggested that this problem can be overcome by using higher-dimensional hyper-chaotic systems, which have increased randomness and higher unpredictability[6]. Due to its higher unpredictability than chaotic system, the hyper-chaos may be more useful in some fields such as cryptography.

This paper presents an improved image hiding method based on a new hyper-chaotic system. The binary sequences that generated based on the new hyper-chaotic system applied to pre-encrypt the image, including improved magic- cube scrambling and pixels permutation; then it further used to hide the pre-encrypted image.

2 Binary Sequence Based on a Hyper-chaotic System

Hyper-chaos was first reported by Rossler in 1979[7]. In the past years, the generation of hyper-chaos has been studied with increasing interests[8]. Hyper-chaotic Rossler system and hyper-chaotic Chua's circuit

* Corresponding author. E-mail address: lm@ujs.edu.cn

are two well-known hyper-chaos examples. Recently, based on the Lorenz system, a new chaotic system was reported by Zengqiang Chen[9]. The system is described as follows:

$$\begin{cases} \dot{x} = a(y - x) + eyz \\ \dot{y} = cx - xz + y + u \\ \dot{z} = xy - bz \\ \dot{u} = -ky \end{cases} \quad (1)$$

Fixing $a = 35, b = 4.9, c = 25, d = 5, e = 35$ and varying k and b , when k and b varies, the corresponding three Lyapunov exponents[10] of system (1) are shown in Table 1 and Table 2 .

Table 1 Some Typical Parameter Values of k					Table 2 Some Typical Parameter Values of b				
k	λ_1	λ_2	λ_3	λ_4	b	λ_1	λ_2	λ_3	λ_4
10	4.409	0.131	0	-43.440	3.8	2.251	0.680	0	-40.734
22	4.031	0.252	0	-43.182	5.5	2.496	0.751	0	-42.747
67	3.069	0.669	0	-42.638	7.6	2.761	0.760	0	-45.118
109	2.411	0.792	0	-42.103	9.9	2.562	0.743	0	-47.203
126	2.158	0.859	0	-41.917	11	2.247	0.705	0	-47.951

The new system has only one equilibrium, but it has bigger positive Lyapunov exponents than those hyper-chaotic systems already known. So the new system may be more useful in some fields such as encryption, communication. It is said that we always dispose of the grey value matrix of images to encrypt the digital images, and the range of grey value is between 0-255. Known to the Shannon theorem, the secret key need enough magnitude and an entropy as high as possible[11]. Fixed initialization parameter $a = 35, b = 4.9, c = 25, d = 5, e = 35, k = 100$ and randomly select a beginning value in experiment adopt 4 rank Runge-Kutta method carried on solve and step size to 0.01. After several steps, 4 groups of sequence were created, and grouped as X, Y, Z and U . And then the binary sequences were generated based on these four groups of hyper-chaotic sequences in Method 1.

Method 1

(1) Choose sequence X, Z and its length are both n . Take the decimal fraction of X, Z , rename the new sequence as X_d, Z_d .

(2) A function is defined to divide the line X_d and Z_d as 32 zones, and each zone marking a number from 0 to 31. Corresponding zones to the binary system are equivalent to 0000 to 1111. For example, zone 16 rightness is equivalent to binary system 1000.

(3) Make two binary sequence X_d, Z_d , basis different chaotic sequence value according to step (2), the length of every sequence is fourfold to the original chaotic sequence.

(4) Generate an encryption sequence basis two binary sequences X_d, Z_d , which is in step (3) as the format $(X_d(i), Z_d(i)), i = 1, 2, \dots, 4n$. Its length is $8 \times n$.

Follow the same steps to the sequence Y, U and then we get two binary sequence named L_1 and L_2 to be used for image encryption in the next part.

3 Image Hiding and Encryption

3.1 Encryption

Usually, there are three ways for encrypting images: displacing the pixels point, changing the grey value and combining the two methods[12]. This paper present a method based on chaotic sequence in Method 2. Method 2 (Image Encryption)

Suppose a BMP image which has one layer with the size of $M \times N \times K$

Step 1: get sequence $L_1(M \times N \times K)$ and $L_2(M \times N \times K)$ generated by "Method 1" and change the value matrix of image from decimal system to binary system as sequence L .

Step 2: make an OR operation with the sequence L_1 and L in order to get a cryptographical sequence $C = \{C_1, C_2, \dots, C_{M \times N \times K}\}$ and change it to the image format.

Step 3: define one dimension sequence $I = \{I_1, I_2, \dots, I_{M \times N}\}$, I_i is the position of the pixels i .

Step 4: suppose function $F(x, y)$ is to get the arithmetical compliment of $x \div y$; function $G(x, y)$ is to change the position of I_x and I_y ; then make $h = M \times N$ do the magic-cube scrambling as follows:

- if $L_2(i) = 0, L_2(i + 1) = 0$, do $G(i, j), i = j$;
- if $L_2(i) = 0, L_2(i + 1) = 1$, do $G(i, j), j = F(i, h/4) + h/4$;
- if $L_2(i) = 0, L_2(i + 1) = 0$, do $G(i, j), j = F(i, h/4) + h/2$;
- if $L_2(i) = 0, L_2(i + 1) = 0$, do $G(i, j), j = F(i, h/4) + 3h/4$;

Iterative the operating for $h/4$ steps, save the the value of image.

3.2 Hiding

After the image encryption, the image can be hidden into carrier image. There are some image hiding methods[13], this paper presents a new way for hiding image which uses the low bit of the pixels of the image value matrix. It is known that the range of grey value of a digital image is between 0-255, in binary system the range is equivalent to 0-1111 1111 in computers today. When we change the last two bit of one pixels' grey value, its true value only range from -3 to +3, and the little change can hardly be distinguished by naked eyes. So we can hide one image into others and those pictures can't be distinguished whether it has been changed or not. To reduce the encryption key space, this paper uses a new method to process the image hiding.

Method 3 (Image Hiding)

Suppose a BMP image (O) has one layer with the size of $M \times N \times K$

Step 1: choose a carrier image(C) the same size of the original image (O), get the depth value d of image C and change the data matrix of C into binary system.

Step 2: change the head part and data matrix of image O into binary system marked as two one-dimension sequence named $T = \{T_1, T_2, \dots, T_E\}$ and $I = \{I_1, I_2, \dots, I_{M \times N \times K}\}$. Increase the depth value d to D . Get the data matrix of C and change it into one-dimension sequence named \bar{I} . Suppose function $int(x)$ get the integer part of x . We can get the value of D as the way described by formula 2.

$$D = \text{int} \left(\frac{E + M \times N \times K}{M \times N} + 1 \right) \tag{2}$$

Step 3: combine T and I as I' and suppose the circulation step is i . Make an OR operation between the bit of I' in which the position is j and the bit of \bar{I} in which the position is k , then make $j = j + 1, k = k + 1$ and do the same operation again. The value of j and k can be achieved by formula 3 and formula 4.

$$j = 2 \times i - 1 \tag{3}$$

$$k = K(i - 1) - 1 \tag{4}$$

$i = 1, 2, \dots, \frac{E+M \times N \times K}{2}$. Do step 3 while $i \leq \frac{E+M \times N \times K}{2}$.

Step 4: change the final data into image format, and save image C.

With all the operation in Method 2 and Method 3 we obtain the encryption image, and with the practice in Matlab system the effect will be shown in the next part.

4 Effects of the Image Hiding and Encryption Methods

According to Table 3, there are three Encryption keys: 8806286790001672, 8806286790001673, 8806286790001674. Also fix the initialization parameter $a = 35, b = 4.9, c = 25, d = 5, e = 35, k = 100$ and the integer part of x, y, z, u as $x_0 = 10, y_0 = 6, z_0 = 4, u_0 = 51$.

Table 3 Encryption Key

	Key 1-4	Key 5-8	Key 9-12	Key 13-16
encryption key	XXXX	XXXX	XXXX	XXXX
According to the the initial value of the chaotic system	4 numerals after the decimal point of initial value X	4 numerals after the decimal point of initial value Y	4 numerals after the decimal point of initial value Z	4 numerals after the decimal point of initial value U

The standard of impersonality fidelity in the experiment was defined in formula 5 and formula 6 as PSNR and PMSE. The bigger the value of PSNR, the better the impersonality fidelity; the less the value of PMSE, the higher the similitude the two images. Critical value is 31db.

Definition 1: suppose there are carrier image $G(M \times N \times S)$ and mixed image $F(M \times N \times S)$, S is the depth of images. The value of PSNR and PMSE can be got in formula 5 and formula 6:

$$PSNR = 10 \lg \left[\frac{M \times N \times S \times 255^2}{\sum_{s=1}^S \sum_{i=1}^M \sum_{j=1}^N (G_s(i, j) - F_s(i, j))^2} \right] \quad (5)$$

$$PMSE = \left[\frac{1}{M \times N \times S} \sum_{s=1}^S \sum_{i=1}^M \sum_{j=1}^N (G_s(i, j) - F_s(i, j))^2 \right]^{\frac{1}{2}} \quad (6)$$

the critical value of $PSNR$ and $PMSE$ is 31.

4.1 Effects Shown by Images

In the experiment, the accurate key to encryption is 8806286790001673. Fig. 1 is the contrast between the original image and the encrypting image; Fig.2 and Fig.3 are the contrast between carrier images and final hiding images, it can hardly be distinguished by naked eyes; Fig.4 is the contrast between the original image and the decrypting image; the two pictures in Fig.5, use the wrong key (8806286790001672 and 8806286790001674) when decrypting.

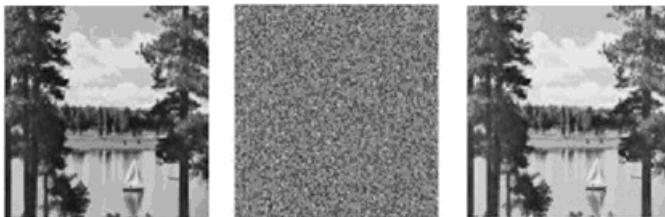


Figure1: Contrast between the original image and the encrypting image

4.2 Effects Shown by Practical Data

Table 4 is contrasts between those pictures above calculated by formula 5 and formula 6, and all the values in Table 4 show that the result of the method of image hiding and encryption is good.

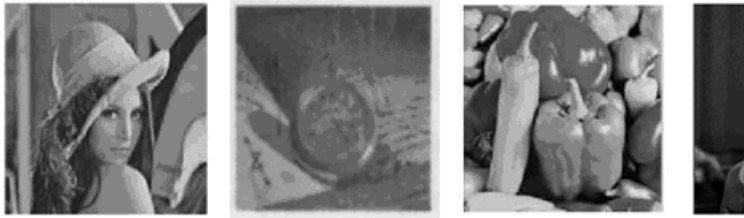


Figure2:Carrier images

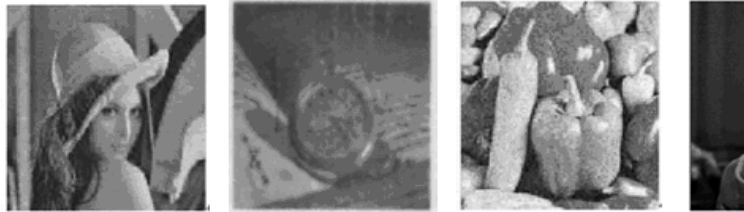


Figure3:Final hiding images

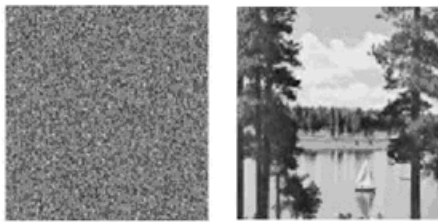


Figure4:Decrypting image with the right key

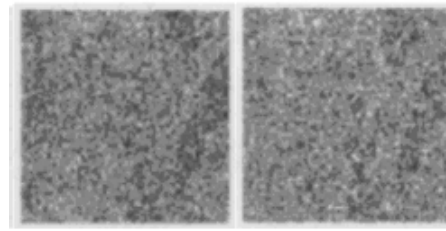


Figure5:Decrypting image with the wrong key

Table 4 Effect Analysis

	PSNR	PMSE
Fig.2.a and Fig.3.a	42.156371	1.350902
Fig.2.b and Fig.3.b	39.573144	3.775146
Fig.2.c and Fig.3.c	34.257269	5.550945
Fig.2.d and Fig.3.d	36.694031	5.102782
Fig.1.a and Fig.1.c	34.355122	4.881192
Fig.1.b and Fig.4.a	37.168534	3.673158
Fig.1.a and Fig.4.b	34.355231	3.672187
Fig.1.a and Fig.1.b	4.1839271	158.483145
Fig.1.a and Fig.5.a	3.4728693	160.389615
Fig.1.a and Fig.5.b	4.1579240	159.472321

5 Conclusion

This paper presents an improved image hiding method based on a new hyper-chaotic system. The binary sequences generated based on the new hyper-chaotic system are applied to pre-encrypt the image, including improved magic-cube scrambling and pixels permutation; then further processing are used to hide the pre-encrypted image based on low bit position change of the carrier image. The effect of hiding is also analyzed by using the method of Simulation on Matlab system. All the results indicate that the method has good efficiency and security characteristic in cryptography area. Also the encryption key space is big enough for security demand and can be used in practicality image encrypting.

Acknowledgements

This work was partially supported by the National Nature Science Foundation of China (Grant Nos. 70871056).

References

- [1] Diffie W, Hellman M: New Direction in Cryptography[J]. *IEEE Trans on Information Theory*.22(6): 644654(1976)
- [2] B. A. Idowu¹ , U. E. Vincent , A. N. Njah: Control and Synchronization of Chaos in Nonlinear Gyros via Backstepping Design . *International Journal of Nonlinear Science*. Vol.5:11-19(2008)
- [3] Guoliang Cai,Juanjuan Huang:A New Finance Chaotic Attractor.*International Journal of Nonlinear Science*. 3 (3):213-220(2007)
- [4] Guoliang Cai, Weihuai Zhou, Zhenmei Tan:Stabilization of Higher Periodic Orbits of Discrete-time Chaotic Systems. *International Journal of Nonlinear Science*. 4 (2):118-126(2007)
- [5] G. Perez, H.A. Cerdeira, *Phys. Rev. Lett.* 74 (1995) 1970.
- [6] L. Pecora, *Phys. World* 9 :17(1996)
- [7] O.E. Rossler, *Phys. Lett. A* 71 :155(1979)
- [8] Y. Li, G. Chen, L.Wallace, K.S. Tang, *IEEE Trans. CAS-II* 52 :204(2005)
- [9] Zengqiang Chen, Yong Yang, Guoyuan Qi, Zhuzhi Yuan: A novel hyperchaos system only with one equilibrium[J]. *ScienceDirect Physics Letters A* 360:696-701(2007)
- [10] Zhang Jia - shu, Tian Lei, Tai Heng - ming: A new watermarkingmethod based on chaotic maps[C]//*IEEE International Conference onMultimedia and Expo, Taipei, Taiwan*. 939- 942(2004)
- [11] Hans Delfs, Helmut Knebl. Introduction to cryptography : principles and applications [M]. beijing:TSINGHUA University press, 2007.
- [12] CHEN Gang, FENG Zhi-gang, CHEN Li-hong: A new image encryption algorithm [J]. *Journal of Jiangsu University (National Science Edition)* Nov.549552(2004)
- [13] Wolfram S. :Theory and application of cellular automata[M]. *Singapore: World Scientific*.18- 59(1986)