Vol 16 No 12, December 2007
1009-1963/2007/16(12)/3616-08

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Image encryption using high-dimension chaotic system*

Sun Fu-Yan(孙福艳)[a)†], Liu Shu-Tang(刘树堂)[a)], and Lü Zong-Wang(吕宗旺)[b)]

[a)] *College of Control Science and Engineering, Shandong University, Jinan* 250061, *China*
[b)] *Corporate Engineering Department, Johnson Electric (ShenZhen) Co. Ltd, ShenZhen* 518125, *China*

(Received 28 February 2007; revised manuscript received 3 April 2007)

In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques. This paper proposes a new approach for image encryption based on a high-dimensional chaotic map. The new scheme employs the Cat map to shuffle the positions, then to confuse the relationship between the cipher-image and the plain-image using the high-dimensional Lorenz chaotic map preprocessed. The results of experimental, statistical analysis and key space analysis show that the proposed image encryption scheme provides an efficient and secure way for real-time image encryption and transmission.

Keywords: Arnold cat map, image encryption, chaotic encryption
PACC: 0545

1. Introduction

During the last decades, owing to the frequent flow of digital images across the world over transmission media, it has become essential to secure them from leakages. Many applications like military image databases, confidential video, cable TV, etc. require a reliable, fast and robust security system to store and transmit images. The traditional image encryption technique regards plain-text as the original data stream, and due to some intrinsic features of images, such as bulk size data and high correlation among pixels, traditional encryption algorithms such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are not suitable for practical image encryption. Many encryption schemes have been proposed based on different principles in order to improve the degree of privacy.[1−7] Among them, chaos based encryption techniques have shown their superior performance, and it has been proved that in many aspects chaotic maps have important characteristics related to the fundamental requirements of conventional encryption algorithms:[8−14] for instance, aperiodicity (useful for one time pad cipher), sensitive dependence on initial conditions and system parameters (useful for confusion and diffusion processes), ergodicity and random-like behaviours (useful for producing output with satisfactory statistics). Therefore, some elaborated constructions are needed to successfully employ chaos in encryption. A number of chaos based image encryption schemes have been developed in recent years which we discuss briefly in this paragraph. In Ref.[7], an encryption method called CKBA (chaotic key-based algorithm) was presented. The algorithm changed the pixel values of the plain-image. However, Li and Zhang[9] pointed out that CKBA is very weak to the chosen or known plain-text attack, and its security to brute-force cipher text-only attack is overestimated by the authors. In Ref.[3], an encryption algorithm using chaotic Kolmogorov flows was designed. In this scheme, diffusing the value of pixels and permuting were applied, which significantly increase the resistance against statistical and dynamical attacks. In order to improve the security of the image encryption algorithm, two-dimensional (2D) Cap/Baker maps, etc., have been used for encryption schemes. Recently, in order to de-correlate relations among pixels rapidly, a new scheme employs a three-dimensional (3D) map to shuffle the positions of image pixels and uses another chaotic map to confuse the relationship between the cipher-image and plain-image, for example, 3D Cat/Baker map.[11,12] But Wang *et al* pointed out[15,16] that the lack of security discourages the use of these cryptosystems for practical applications.

A new approach is suggested in this paper for fast and secure image encryption. A high-dimensional chaotic map is used to shuffle the positions of pix-

*Project supported by the National Natural Science Foundation of China (Grant No 60472112) and the Foundation for the author of National Excellent Doctoral Dissertation of China (Grant No 200444).
†Corresponding author. E-mail: fuyan_sun@126.com

els in the image, and to confuse the relationship between cipher-image and plain-image. It is found that there are exceptionally good properties of mixing and sensitivity to initial conditions and parameters in the Arnold Cat map,[16−18] thus it is used for permutation. The rest of this paper is organized as follows. Section 2 describes the proposed method. Section 3 presents the experiments, and the security of the new scheme is evaluated. Section 4 concludes the paper.

2. The proposed cryptosystem

The image encryption algorithm includes two steps. Firstly, the positions of the pixels of the original image are shuffled by the Arnold cat map. Then the pixel values of the shuffled image are encrypted by the Lorenz chaotic system.

2.1. Encryption by Arnold cat map

The classical Arnold cat map is a two-dimensional invertible chaotic map[18] described by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1, \quad (1)$$

The above 2D cat map is now generalized by introducing two control parameters, p and q, then discretized as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N, \quad (2)$$

where p and q are two positive integers. Here, the parameters p, q and the number of iterations M all can be used as the secret keys. Since there only exists a linear transformation and mod function, it is very efficient to shuffle the pixel positions by using the Arnold cat map. After several iterations, the correlation among the adjacent pixels can be disturbed completely. Some experiments are given in Section 3 to demonstrate the efficiency of Arnold cat map. It must be emphasized that not all choices of the parameters will produce a correct generalization of the cat map. In particular, to make sure that the map is one-to-one, the determinant of A must equal 1. In addition, not all useful features of chaos can be preserved by discretization. For example, after discretization, an aperiodic chaotic map may become periodic, which will degrade the security of chaotic encryption. For example, when $p = 25$ and $q = 5$, after six rounds of iterations, an image of size 256×256 will turn back to its original. Figure 1 shows this phenomenon. As a remedy, we adopt the high-dimension Lorenz map to change the pixel values to improve the security. The following will further discuss the process.

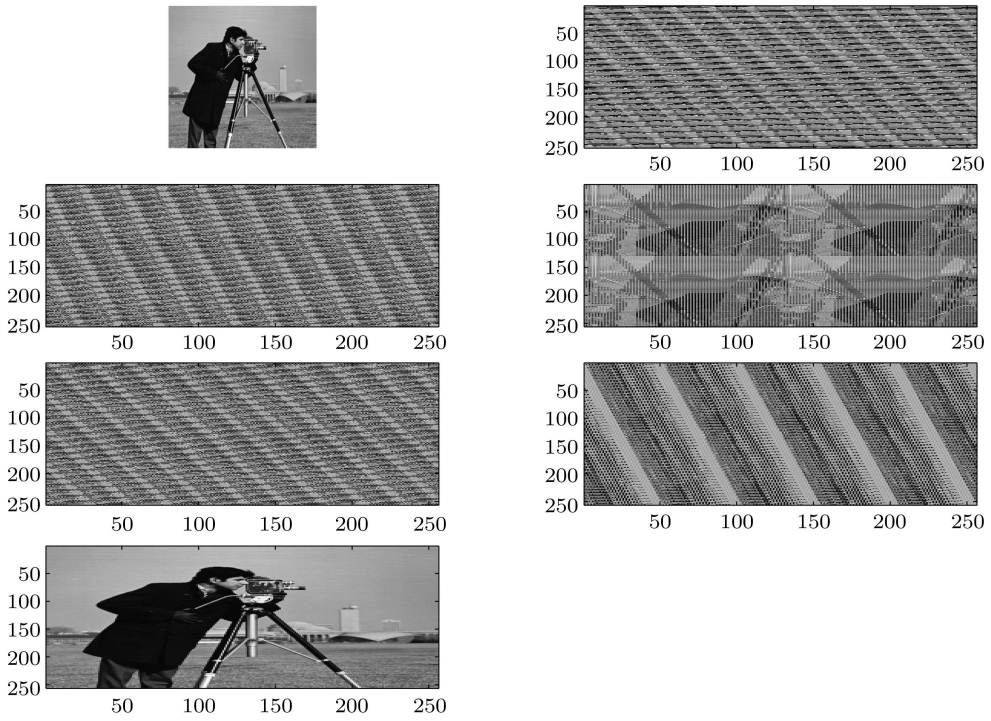


Fig.1. Periodic phenomenon in discretizing the cat map.

2.2. Encryption by Lorenz chaotic system

There are two reasons for adopting diffusion in an encryption algorithm. On one hand, the diffusion process is very efficient to render the discretized chaotic map non-invertible, on the other hand, it can change the statistical properties of the plain-image, and makes the histogram of the cipher-image fairly uniform. Therefore, for a secure encryption scheme, the diffusion processing is necessary. For the purpose of diffusion, in order to realize diffusion, the 'XOR' and 'MOD' operations will be applied in the new scheme, to each pixel in between every two adjacent rounds of the cat map.

The Lorenz system is a classical high-dimensional chaotic system and has been studied widely.[19−22] The encrypting sequences produced by this system have three excellences. One is that the structure of this system is more complex than the low-dimensional chaotic systems. It is more difficult to forecast such chaotic sequences. The second is that the real value sequences of three system variables can be used singly or put together to use. The design of encrypting sequence is more convenient. The third is that three initial conditions and three control parameters of this system all can be made as the secret-keys. Therefore, the Lorenz chaotic system is more advantageous than the low-dimensional chaotic system if some control variables are rejoined in the designing process. The dynamic equation of the Lorenz system is

$$\begin{aligned} \mathrm{d}x/\mathrm{d}t &= \sigma(y-x), \\ \mathrm{d}y/\mathrm{d}t &= \gamma x - zx - y, \\ \mathrm{d}z/\mathrm{d}t &= xy - bz, \end{aligned} \tag{3}$$

where σ, γ and b are the control parameter of the system, and the system exhibits chaos when the empiric value is $\sigma = 10, \gamma = 28, b = 8/3$. If σ and b are constant, then the chaos period of the Lorenz system is infinite. The chaotic behaviour of the Lorenz system is studied by using the fourth order Runge-Kutta method to the above equation. It is based on these qualifications: the control parameters $\sigma = 10, \gamma = 28, b = 8/3$; the initial conditions $x_0 = 1.8552, y_0 = 1.2254, z_0 = 1.2545$; integer step size $h = 0.001$; iteration steps 60000. The autocorrelation and mutual correlation characteristics of the x_i, y_i and z_i real value chaotic sequences are shown in Fig.2 and Fig.3 respectively.

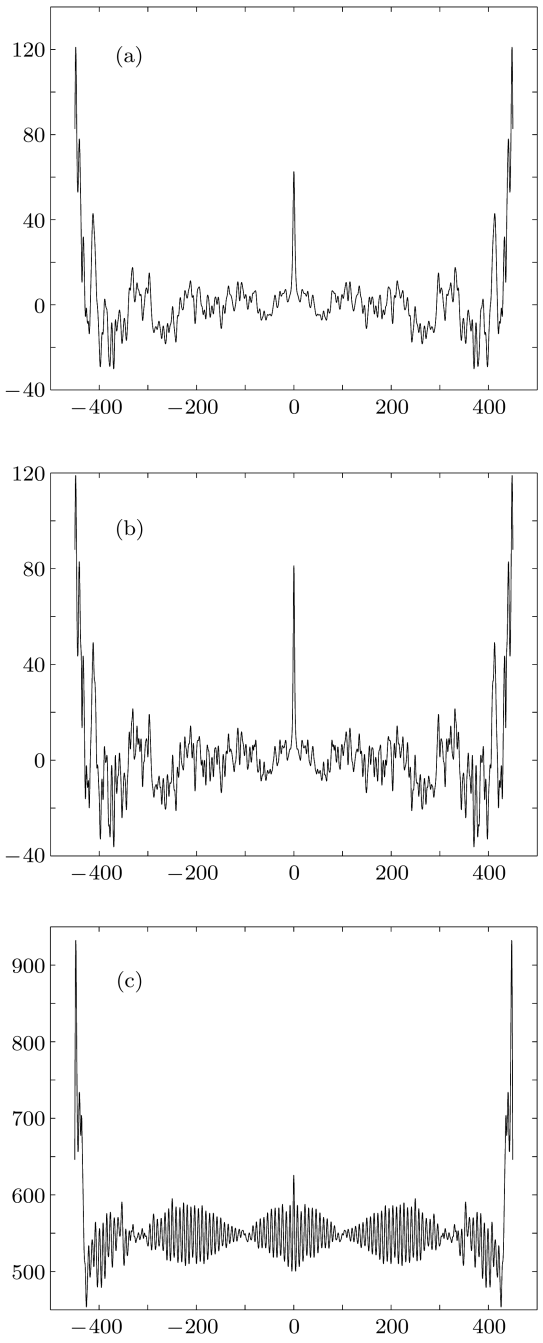


Fig.2. (a) Autocorrelation characteristics of x_i. (b) Autocorrelation characteristics of y_i. (c) Autocorrelation characteristics of z_i.

According to Golomb's three postulates for a pseudo-random sequence, the ideal chaotic sequence should have such statistical characteristics as the following: its average value is zero, the autocorrelation is the delta function, and the mutual correlation is zero. It is easy to see that their correlation characteristics are not ideal from Fig.2 and Fig.3. So we have made

the pretreatment for the sequences as follows:

$$x_k(i) = 10^n x_k(i) - \text{round}(10^n x_k(i)). \quad (4)$$

Taking the value $n = 4$, the x_i, y_i, and z_i real value chaotic sequences after the pretreatment show good performance. Their autocorrelation and mutual correlation characteristics are shown respectively in Fig.4 and Fig.5.

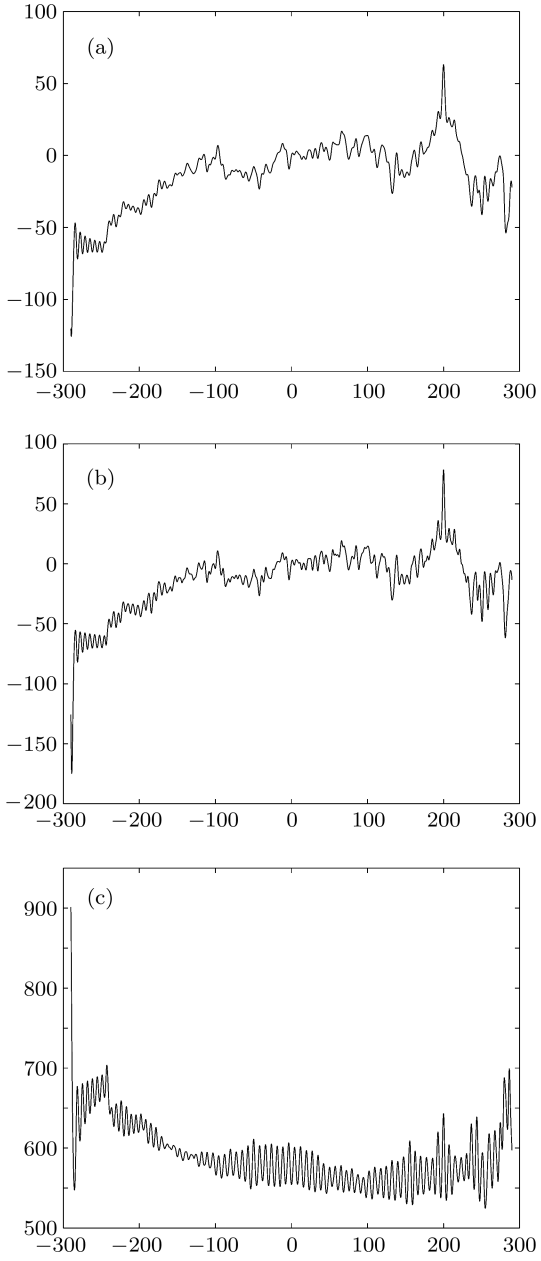


Fig.3. (a) Mutual correlation characteristics of x_i. (b) Mutual correlation characteristics of y_i. (c) Mutual correlation characteristics of z_i.

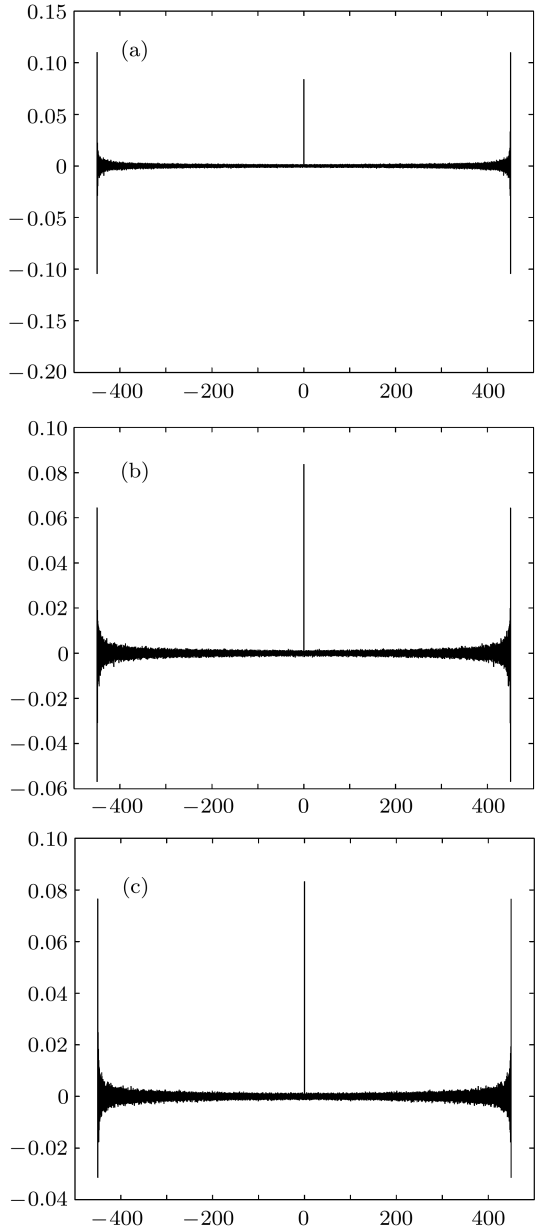


Fig.4. (a) The sequence pretreatment x_i autocorrelation characteristics. (b) The sequence y_i autocorrelation characteristics after pretreatment. (c) The sequence z_i autocorrelation characteristics after pretreatment.

The encryption process consists of four steps of operations.

Step 1 The pixels of the shuffled image are arranged and transformed into one-dimensional vector

denoted by I, $I = \{I_1, I_2, ..., I_{N\times N}\}$, let the dimension of the vector I be N. In which each element is the decimal grey value of the pixel. Convert decimal pixel values to binary numbers and get a new set $d = \{d_1, d_2, ..., d_{N\times N}\}$.

Step 2 Choose an arbitrary initial condition x_0 and three specific values for the external parameter σ, γ, and b for which the map is chaotic. Iterate the Lorenz chaotic map for N_0 times. The pretreatment is carried for Lorenz chaotic real value sequences.

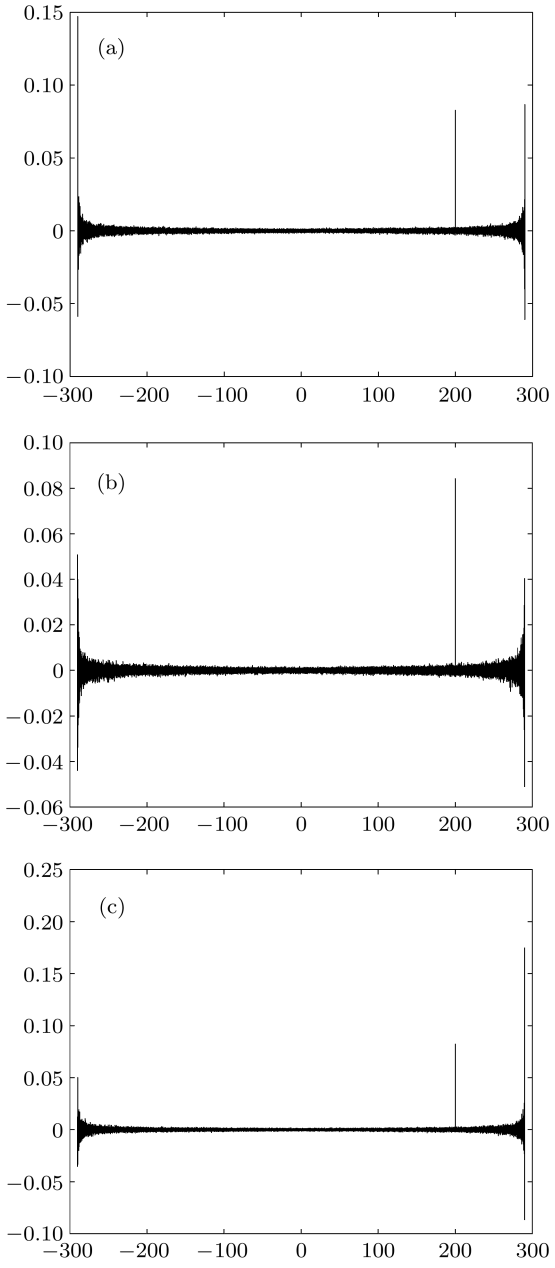


Fig.5. (a) The sequence x_i mutual correlation characteristics after pretreatment. (b) The sequence y_i mutual correlation characteristics after pretreatment. (c) The sequence z_i mutual correlation characteristics after pretreatment.

Step 3 The Lorenz chaotic system is iterated continuously; for each iteration, we can get three values x_i, y_i and z_i, and preprocess these decimal values, then convert decimal values to get binary numbers $b_{x_i}, b_{y_i}, b_{z_i}$ as follows

$$b_{x_i} = \text{de2bi}(\text{mod}(\text{Abs}(10^n x_k(i) - \text{round}(10^n x_k(i))) \times 10^{15}, 256)) \quad (5)$$

where Abs(x) returns the absolute value of x. The function de2bi(x) converts decimal number x to binary value. In the same way, b_{y_i}, b_{z_i} can be obtained.

Step 4 Using an invertible geometrical rule, we encrypt the shuffled image as

$$c_{3\times(i-1)+1} = (d_{3\times(i-1)+1} + b_{y_i})\text{mod}2 \oplus b_{x_i}, \quad (6)$$

$$c_{3\times(i-1)+2} = (d_{3\times(i-1)+2} + b_{z_i})\text{mod}2 \oplus b_{y_i}, \quad (7)$$

$$c_{3\times(i-1)+3} = (d_{3\times(i-1)+3} + b_{x_i})\text{mod}2 \oplus b_{z_i}. \quad (8)$$

where $i = 1, 2, ...,$ represents the ith iteration of the Lorenz chaotic system. The Lorenz system is iterated until all the elements in the set $d = \{d_1, d_2, ..., d_{N\times N}\}$ encrypted. In order to improve the security, we can encrypt the image several times by taking the last value of x_i, y_i and z_i from step 3 as an initial condition.

3. Experimental results and security analysis

In this paper, experimental analysis of the proposed encryption scheme has been done with several images. Figure 6 is the 256 grey-scale plain-image and shuffled image of size 256×256. The histograms of the plain-image and the corresponding shuffled image are shown in Fig.7. The secret keys are chosen as $p = 25, q = 5, M = 7$. As can be seen, cat map only shuffles the pixel positions of the image, and does not change the statistical characteristic of the image. Figure 8 is its cipher-image and the corresponding histogram obtained by use of Lorenz chaotic system. The parameters are selected as $\sigma = 10, \gamma = 28, b = 8/3$, the secret keys to change the pixel values of the shuffled image are $x_0 = 1.8552, y_0 = 1.2254, z_0 = 1.2545$, as can be seen, the histogram is fairly uniform. Figure 9 is the decrypted image using the right keys and wrong keys respectively. It is easy to see that the decrypted image is clear and correct with any distortion if the keys are right. But if we use the wrong keys ($x_0 = 1.855200000000001, y_0 = 1.2254, z_0 = 1.2545$), an unexpected image will be got. Figure 10 shows the

correlation distribution of two horizontally adjacent pixels in the plain-image and that in the cipher-image. These correlation analysis proves that the chaotic encryption algorithm satisfies zero co-correlation.

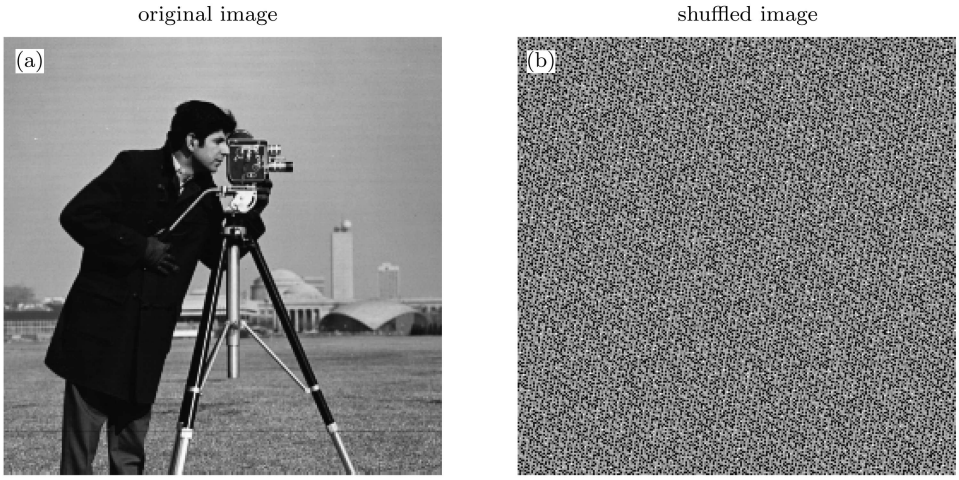


Fig.6. Plain-image and shuffled image.

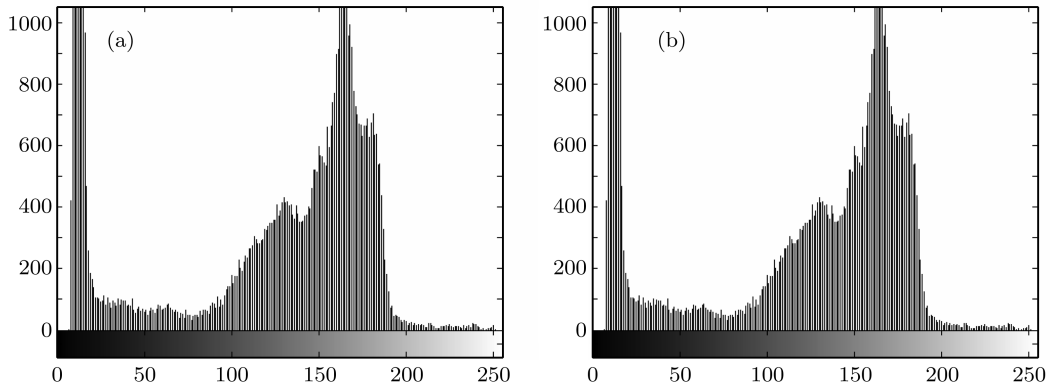


Fig.7. Histograms of the plain-image and shuffled image.

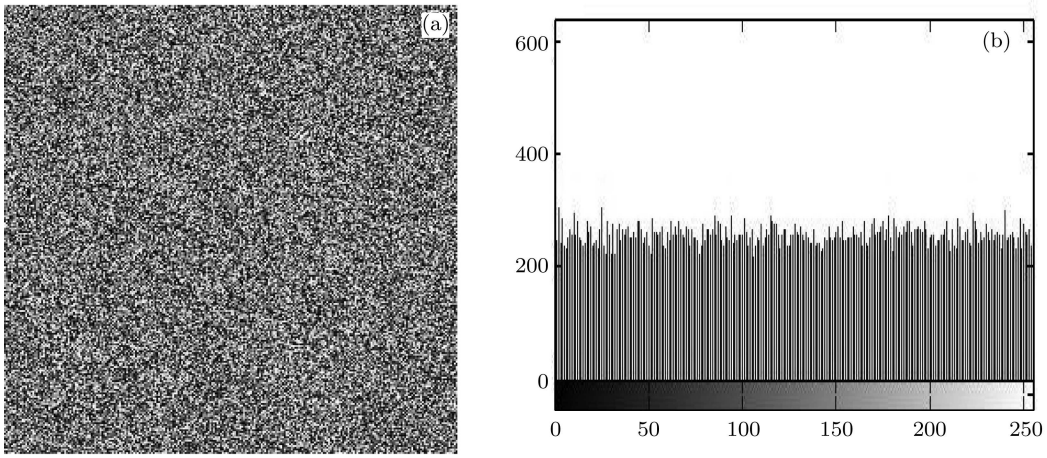


Fig.8. Cipher-image and histogram after the Lorenz chaotic system encryption.

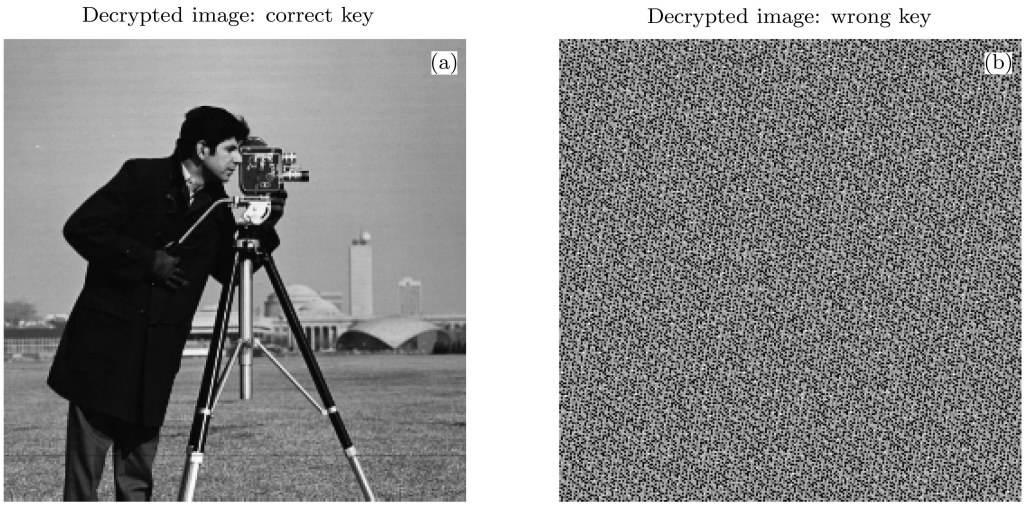


Fig.9. Decrypted images using the right keys and using the keys ($x_0 = 1.855200000000001$, $y_0 = 1.2254$, $z_0 = 1.2545$).

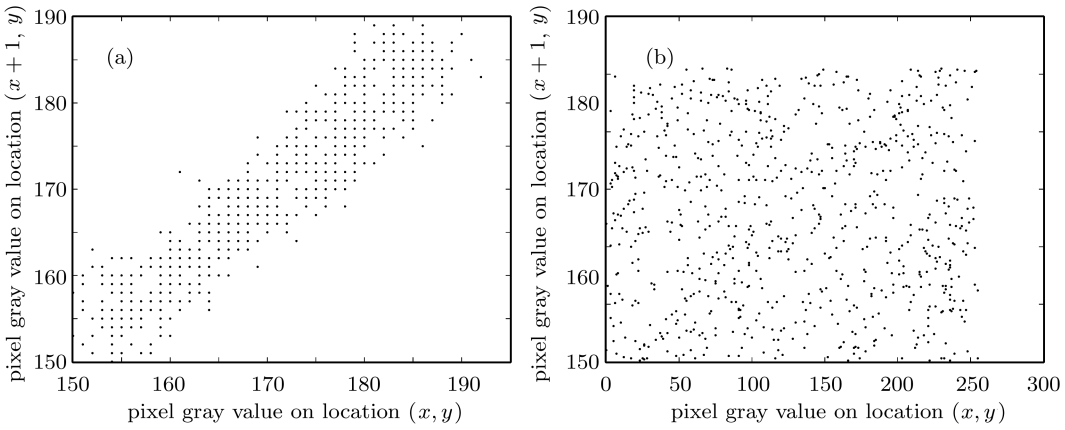


Fig.10. (a) Correlations of two horizontally adjacent pixels in the plain-image. (b) Correlations of two horizontally adjacent pixels in the cipher-image.

A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. If the precision is 10^{-15}, the key space size is 10^{45}. Moreover, the parameters p, q, and the number of iterations M all can be used as the secret keys, the key space is large enough to resist the attacks.

Compared with traditional block ciphers such as DES, IDEA and AES, the proposed chaos-based cryptosystem has some distinct properties. Firstly, the proposed cryptosystem is suitable for large volume data encryption such as image, audio and perhaps also video data. Secondly, the proposed cryptosystem has high key sensitivity. This means that a slight change in the key will cause great changes in the ciphertext. This property makes various sensitivity-based attacks difficult to break the cryptosystem. Thirdly, from Fig.10 one can see that the encryption process permutes the plaintext so greatly that the correlation between two adjacent pixels is very small. Thus, it is difficult for a statistical attack to break it by analysing the pixels' correlations. Moreover, the encryption algorithm is simple and easy to realize.

4. Conclusions

This paper presents a new encryption algorithm: it shuffles image positions by using a cat map and changes pixel values by using a high-dimensional Lorenz chaotic system. The proposed algorithm overcomes the drawbacks of small key space and weak security in the widely used one-dimensional Logistic system. The experimental results demonstrate that the encryption algorithm shows advantages of large key space and high security.

References

[1] Bourbakis N and Alexopoulos C 1992 *Pattern Recogn.* **25** 567

[2] Chang H K and Liu J L 1997 *Signal Process. Image Commun.* **10** 279

[3] Scharinger J 1998 *J. Electron Eng.* **7** 318

[4] Fridrich Jiri 1998 *Int. J. Bifurcat. Chaos* **8** 1259

[5] Cheng H and Li X B 2000 *IEEE Trans Signal Process.* **48** 2439

[6] Chang C C, Hwang M S and Chen T S 2001 *J. Syst. Software* **58** 83

[7] Yen J C and Guo J I 2000 *Proc IEEE Int. Conference Circuits and Systems* **4** 49

[8] Kocarev L 2001 *IEEE Circ Syst Mag.* **1** 6

[9] Li S and Zhang X 2002 2002 *Proc IEEE Int Symposium Circuits and Systems* (Scottsdale, AZ) **2** 708

[10] Kocarev L and Jakimovski G 2001 *IEEE Trans. Circ. Syst.* **48** 169

[11] Mao Y B and Chen G 2004 *Int. J. Bifurcat. Chaos* **14** 3613

[12] Chen G, Mao Y B and Chui C K 2004 *Int. J. Bifurcat. Chaos, Solitons Fractals* **21** 749

[13] Pareek N K, Vinod Patidar and Sud K K 2003 *Phys. Lett.* A **309** 75

[14] Mao Y and Chen G 2003 *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics* (Berlin: Springer)

[15] Wang K, Pei W J, Zou L H and He Z Y 2006 *Acta Phys. Sin.* **55** 6243 (in Chinese)

[16] Wang K and Pei W J 2005 *Phys. Lett.* A **343** 432

[17] Lian S G and Sun J S 2005 *Phys.* A **351** 645

[18] http://mathworld.woffram.com/ArnoldsCatMap. html

[19] Liu Y Z, Jiang C S, Lin C S and Jiang Y M 2007 *Chinese Physics* **16** 660

[20] Liu Y Z, Jiang C S and Lin C S 2007 *Acta Phys. Sin.* **56** 707 (in Chinese)

[21] Zou Y L, Zhu J and Chen G R 2005 *Chin. Phys.* **14** 697

[22] Wang J Z, Chen Z Q and Yuan Z Z 2006 *Acta Phys. Sin.* **55** 3956 (in Chinese)