Science in China Series F: Information Sciences

A chaos-based image encryption algorithm using alternate structure

ZHANG YiWei[1†], WANG YuMin[2] & SHEN XuBang[1]

[1] Xi'an Microelectronics Technology Institute, Xi'an 710054, China;
[2] National Key Lab of Integrated Service Networks, Xidian University, Xi'an 710071, China

Combined with two chaotic maps, a novel alternate structure is applied to image cryptosystem. In proposed algorithm, a general cat-map is used for permutation and diffusion, as well as the OCML (one-way coupled map lattice), which is applied for substitution. These two methods are operated alternately in every round of encryption process, where two subkeys employed in different chaotic maps are generated through the masterkey spreading. Decryption has the same structure with the encryption algorithm, but the masterkey in each round should be reversely ordered in decryption. The cryptanalysis shows that the proposed algorithm bears good immunities to many forms of attacks. Moreover, the algorithm features high execution speed and compact program, which is suitable for various software and hardware applications.

chaotic encryption, general cat-map, OCML, image encryption

1 Introduction

The chaos is an outer complex behavior produced by the internal random property of the nonlinear definite system, which is a pseudo-random movement while it looks like a random process. Today, chaos-based techniques have been involved in data securities and confidential communication systems. Recently, many methods concerning chaotic carrier modulation in digital communication that can overcome the multipath-related problems are to present certain securities. However, these methods whether adopting synchronization control or noncoherent demodulation have been compromised without knowing the parameters of the chaotic system or even the transmitter structure[1−3]. Attackers can utilize the chaotic synchronization to reconstruct the state space, and noncoherent methods will be broken if people can locate the symbol period window through tracking and estimation.

On the other hand, based on the conventional cryptography, designing the chaotic encryption algorithm independent of modulation/demodulation techniques is another interesting research area,

Received July 16, 2006; accepted March 2, 2007
doi: 10.1007/s11432-007-0026-5
†Corresponding author (email: changdavid@163.com)
Supported by the National Natural Science Foundation of China (Grant No. 60473027)

which concerns how to preserve the information security by using secret keys. Usually a robust encryption scheme should have the following fundamental characteristics[4]: 1) Mapping the plaintext to the random ciphertext; 2) sensitive to the plaintext; 3) sensitive to the secret key.

The chaotic system bears some similar characteristics, such as the pseudo-random, the initial condition sensitivity and the parameter sensitivity. Thus, many researches are focused on applications of mapping the discrete chaotic maps to the cryptosystem[5−8]. Also, different chaotic maps have their own specialties that are suitable for various occasions.

Nowadays, image and video information have been widely used in our daily life. Due to some intrinsic features of image, such as bulk data capacities and high correlations among pixels, traditional encryption algorithms are not suitable for the practical image encryption. In ref. [4], the author extends the cat-map to the general cat-map that can be used for the pixel permutation and diffusion. The one-way coupled map lattice (OCML)[6], which can be used to substitute each pixel in the same size image, shows complex behavior in the two-dimensional space. However, encrypting an image only by one sort of chaotic map has some deficiencies for the short key length and the weak ability against brute-force attack[7]. This paper applies an alternate structure of the classic block cipher, which is combined with two chaotic maps, to the image cryptosystem. The general cat-map is used for the permutation and the diffusion, while OCML for substitution. These two methods are operated alternatively in each round of encryption process. Experimental results show that the proposed algorithm can resist many forms of cryptanalysis (such as statistical analysis, chosen plaintext attack, etc.) and is adequate for encrypting images or the data block.

2 General cat-map and OCML (one-way coupled map lattice)

The proposed algorithm employs two chaotic maps with different characteristics, respectively. In the following, a brief introduction will be given.

2.1 General cat-map

Arnold's cat-map is a well-known two-dimensional invertible chaotic map[8] that is defined as follows:

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

where the adjoint matrix $|C|=1$ and the standard notation "$x(\bmod 1)$" represents the fractional part of a real number x. The range of values among this map is restricted to (0,1).

The two-dimensional cat-map could be generalized to integer field for $N\times N$ pixels' image encryption:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N, \tag{2}$$

where the phase space are extended to $\{0,1,2,\cdots N-1\}$, that is, the range of parameters in matrix $C(|C|=ad-bc=1)$ and state variables becomes integer field from 0 to $N-1$. The inverse operation of eq. (2) is

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \bmod N = C^{-1} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} \bmod N. \tag{3}$$

For $N\times N$ pixels permutation, an empty output space with $N\times N$ pixels should be established at

first. Then, the pixel (i, j) of the output space serves as initial state (x_0, y_0). From eq. (2), a new coordinate can be obtained as (x_1, y_1) through a round of iteration, and the original image pixel (x_1, y_1) is put into the place (x_0, y_0) in the output space at last. Conveniently, a matrix transform $Catmap(\cdot)$ can be defined to operate all pixels in a given image. For example, if an initial coordinate space of 3×3 pixels is $I_0 = \begin{pmatrix} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2) \end{pmatrix}$, assuming $C = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, the output coordinate space I_1 (through a round of iteration) becomes

$$I_1 = Catmap(I_0) = \begin{pmatrix} (0,0) & (1,2) & (2,1) \\ (1,1) & (2,0) & (0,2) \\ (2,2) & (0,1) & (1,0) \end{pmatrix}. \tag{4}$$

From ref. [4], the author suggests four forms of adjoint matrix C, and one should make a choice from $\begin{pmatrix} 1 & b \\ c & bc+1 \end{pmatrix}$, $\begin{pmatrix} bc+1 & b \\ c & 1 \end{pmatrix}$, $\begin{pmatrix} a & 1 \\ ad-1 & d \end{pmatrix}$ and $\begin{pmatrix} a & ad-1 \\ 1 & d \end{pmatrix}$ as the adjoint matrix employed in the encryption. It should be indicated that for better permutation efficiency, proper loops of iterations are necessary. However, such measure fails to improve the security, because n loops of iterations result in

$$\begin{pmatrix} x_m \\ y_m \end{pmatrix} = \prod_{n=0}^{m-1} C_n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = B \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}. \tag{5}$$

Therefore, attackers can perform equivalent key analysis to the matrix B.

2.2 OCML (one-way coupled map lattice)

As a spatio-temporal system, a 2D OCML model can be given as follows[6,9]:

$$x_i(t+1) = (1-\varepsilon)\cdot f(x_i(t)) + \varepsilon \cdot f[x_{i-1}(t)] \quad (0 < \varepsilon < 1), \tag{6}$$

where t and i denote the temporal and spatial axes, respectively. The function $f(x)$ is the Logistic map $f(x) = \mu x(1-x)$. When boundary conditions are given and $\mu = 4$, the whole lattices within the 2D OCML model will go into the chaotic state over (0, 1) interval.

When encrypting images, 32-bit or higher precision should be adopted for fix-point operations. The 24-bit MSB of each lattice can be used to perform XOR operation separately with the three types of gray-scale (R, G and B). Owning to this binary substitution per pixel, the statistical property of encrypted image will change greatly compared with the original one.

3 A novel image encryption algorithm using alternate structure

In ref. [10], Feistel indicated that a product cipher in which two or more ciphers are combined properly is stronger than either of the component systems alone. Combining the two chaotic maps above, this section gives a novel image encryption algorithm using chaotic maps alternately.

The original images should be partitioned or merged into $N\times 2N$ pixel blocks at first. In doing so, the proposed algorithm encrypts an $N\times 2N$ plaintext block into an $N\times 2N$ ciphertext block. The details of the scheme are presented next (Figure 1).

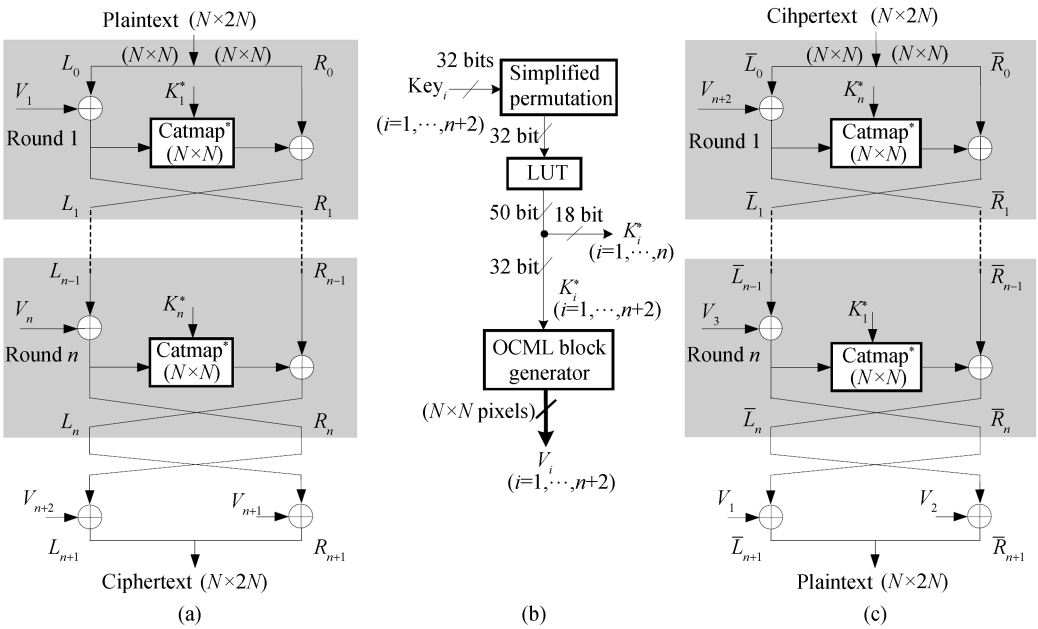

Figure 1 Image encryption algorithm using the alternate structure. (a) Encryption; (b) subkeys generation; (c) decryption.

1. Partition the $N\times 2N$ plaintext block into two $N\times N$ left and right parts (L_0 and R_0).

2. Use the subkey K_1 for generating an $N\times N$ OCML block V_1 to perform XOR operation (per pixel) with the block L_0.

3. Adopt the general cat-map associated with the gray-scale diffusion to permute the output block from step 2, and the 18-bit subkey K_1^* is used for the general cat-map.

4. Perform XOR operation (per pixel) between R_0 and the output block from step 3, the result of which is taken as the left part L_1 in the next round. At the same time, the output block from step 2 is intended to be the right part R_1 in the next round.

5. Reiterate steps 2—4 to execute n rounds of encryption. After that, L_n and R_n should make a swap and perform XOR operation with V_{n+1} and V_{n+2}, respectively. Finally, the left part L_{n+1} and the right part R_{n+1} are merged again into a ciphertext block with $N\times 2N$ pixels.

The whole encryption procedure is shown in Figure 1(a). To resist chosen plaintext attack, the general cat-map is associated with gray-scale diffusion ($Catmap*(\cdot)$ in Figure 1). Let us assume $C_n(i,j)$ is the pending gray-scale of the permuted pixel, and $C_{n+1}(i',j')$ is the gray-scale of the last processed pixel. Considering the following measure to make every gray-scale of pixel inter-dependent:

$$C_{n+1}(i,j)=[C_n(i,j)+A*C_{n+1}(i',j')]\bmod 256, \tag{7}$$

$C_{n+1}(i,j)$ is the updated gray-scale diffused by $C_n(i,j)$ and $C_{n+1}(i',j')$. The coefficient A is an arbitrary integer and suitable A (for instance A=99) can enhance the diffusion effect among pixels.

In Figure 1(b), subkeys K_i and K_i^* are produced by a 32-bit masterkey Key_i in each round. K_i is used to produce the $N\times N$ OCML block V_i; 18-bit K_i^* is designed for general cat-map in which 2 bits are used to choose adjoint matrix C from four suggested forms (at section 2.1), and the rest two 8 bits serve as two parameters in C. The secret key spreading is carried out through the following

steps:

1. Spread the 32-bit Key_i into 50 bits through a simplified permutation and a LUT (look-up table);

2. 18 bits of the 50-bit spread output become K_i^*, and the rest 32-bit K_i is used for iteration (using Logistic map) to produce row and column boundary conditions, in order to get the whole $N \times N$ OCML block V_i (referring to eq. (6)).

As is shown in Figure 1(c), the decryption program can easily be deduced. An $N \times 2N$ ciphertext block still need to be partitioned into two $N \times N$ left and right parts ($\overline{L}_0$ and $\overline{R}_0$), but the sequence of secret keys should be reversely ordered compared with the encryption process. In particular, the decryption has the same processing procedure with the encryption rather than its inverse transformation, and besides, the general cat-map associated with gray-scale diffusion ($Catmap^*(\cdot)$) employed in decryption is also positive operation rather than inverse one. The pseudo code of decryption is presented next:

for $i = 0$ to $n-1$

$$\overline{R}_{i+1} = \overline{L}_i \oplus V_{n+2-i};$$

$$\overline{L}_{i+1} = Catmap^*(\overline{R}_{i+1}) \oplus \overline{R}_i;$$

end for

$$\overline{R}_{n+1} = \overline{L}_n \oplus V_2;$$

$$\overline{L}_{n+1} = \overline{R}_n \oplus V_1.$$

4 Experimental results and security analysis

We made many simulations with gray and color images. In experiments the OCML block is generated by 32-bit fix-point operations, in which (eq. (6)) $\varepsilon = 0.875$ (0e0000000h) and $\mu = 4$ (left shift 2 bits when multiplication in Logistic map) are given. From Figure 1(b), every round of encryption/decryption uses a 32-bit secret key. If the number of round $n = 8$, then the total length of a masterkey is 32×8+32+32=320 bits, which results in good robustness to brute-force attack.

4.1 Key sensitive test and statistical analysis

One of the evaluation criterions for encryption algorithm is the avalanche effect[11]. If a cryptographic function is to satisfy the strict avalanche criterion, the output bit should change with a probability of one half whenever a single input bit is complemented. A 512×512 pixels image is divided into two 256×512 blocks up and down in experiments. When any bit of Key_i in a round is changed, the bit information of the whole ciphertext block changes greatly to 49% being closed to one half. The key sensitive test results are shown in Figure 2.

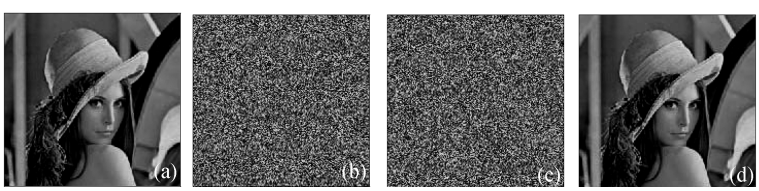

Figure 2 Result of the key sensitive test (8 rounds of encryption). (a) Original image; (b) encrypted image; (c) decrypted image with wrong key (1 bit change); (d) decrypted image with correct key.

In subkeys sensitive tests, for a round of encryption, 500 pairs of nuanced subkeys are used to test the avalanche effect among the OCML substitution function (using the subkey K_i), the $Catmap^*(\cdot)$ function (using the subkey K_i^*), and their product operation (using K_i and K_i^*). Average ratios of changed bit information between two ciphered blocks using nuanced subkeys are shown in Table 1. In experiments, the subkey K_i only changes the least significant bit, and K_i^* merely changes an arbitrary bit.

Table 1 Subkeys sensitive test in one round of encryption

Changed subkeys	K_i	K_i^*	K_i and K_i^*
Average ratio of changed bit infomation	44.30%	49.66%	49.91%

At the same time, the statistical property of the encrypted image varies obviously, as shown in Figure 3. The gray-scales of the encrypted image uniformly distribute over the entire pixel plane, and the similar histogram can be obtained under different plain-images and keys. The advantages of product ciphers are realized thanks to the chaotic maps with various specialties, which make the equivalent key analysis of the general cat-map (in ref. [7]) invalid.

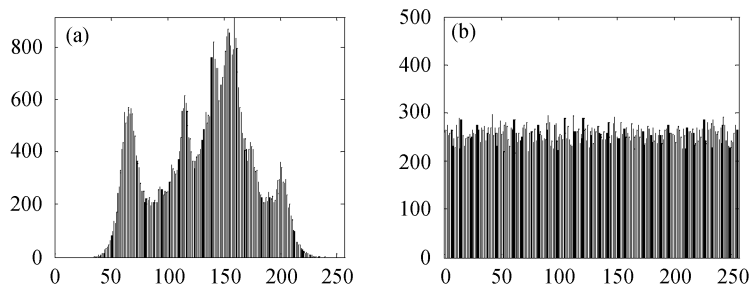

Figure 3 Histogram of the original image and the encrypted image. (a) Original image; (b) encrypted image.

4.2 Plain-image sensitivity and cipher-image correlation

If a tiny change among original image results in a great variation over the whole encrypted image, known and chosen plaintext attack will have difficulty taking affect. Therefore, two plain-images with only 1 pixel difference are encrypted by using the same secret key. Under different rounds of encryption, average ratios of changed bit information between those two cipher-images are shown in Figure 4.

To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a cipher-image, the following procedure was

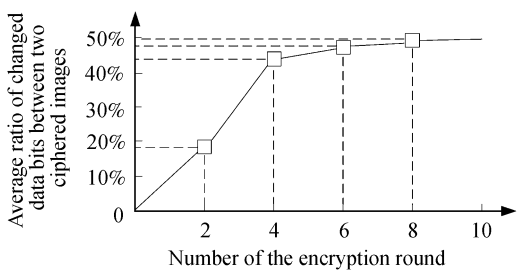

Figure 4 Plain-image sensitive test with only one pixel difference.

carried out. Firstly, randomly select 1000 pairs of two adjacent pixels (x_i, y_i) from an image. Then, calculate the correlation coefficient of each pair by using the following discrete formulas:

$$r_{xy} = \mathrm{cov}(x, y)/(\sqrt{D(x)}\sqrt{D(y)}), \tag{8}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{9}$$

where $E(x)$ and $D(x)$ are discrete mean value and mean variance, respectively. Figure 5 shows the correlation distribution of two horizontally adjacent pixels in original and encrypted images. Similar results for diagonal and vertical directions are obtained.

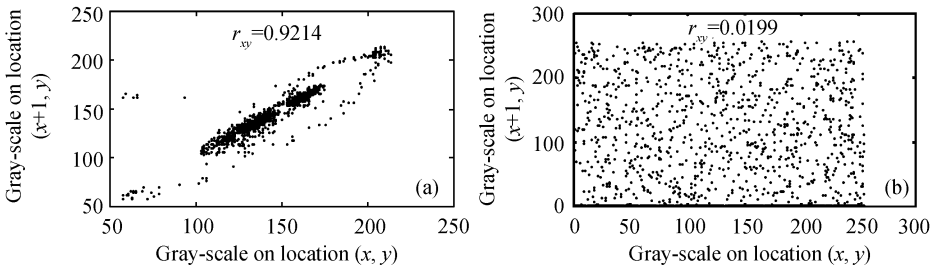

Figure 5 Correlation distributions of two horizontally adjacent pixels**.** (a) Original image; (b) encrypted image.

Correlation coefficients under different scenarios are listed in Table 2, which indicates that the relative good correlation in the original image is effectively destroyed by encryption.

Table 2 Correlation coefficients r_{xy} of two adjacent pixels

Direction	Before encryption	After encryption
Horzontal	0.9214	0.0199
Vertical	0.8993	0.0172
Diagonal	0.9062	0.0228

4.3 Decryption test of blurred cipher-image

Because the decryption has the same processing procedure with the encryption rather than its inverse transformation, the decryption is equivalent to encrypting the cipher-image once again. Therefore, the plain-image sensitivity will affect the quality of decrypted image if the cipher-image is blurred by noise or geometrical distortion. To improve the quality, the algorithm robustness has to decrease accordingly. In experiments, if the operation of gray-scale diffusion (eq. (7)) is canceled, the quality of decrypted image can be recovered to a certain degree. When the salt and pepper noise, Gauss noise and the scratching loss are added to the cipher-image, the experimental results under four rounds of encryption are shown in Figure 6.

Table 3 lists the MSE (mean square error) and the MAE (mean absolute error) to represent the degree of similarity between original image and decrypted image when the cipher-image is contaminated

From Table 3, Gauss noise produces more infections on the decrypted image. The scratching loss and the pepper and salt noise produce lower interferences, which can be effectively eliminated through filtering and enhancing. It should be indicated that if the operation of gray-scale diffusion is employed, the blurred cipher-image could hardly be recovered. Therefore, users should balance

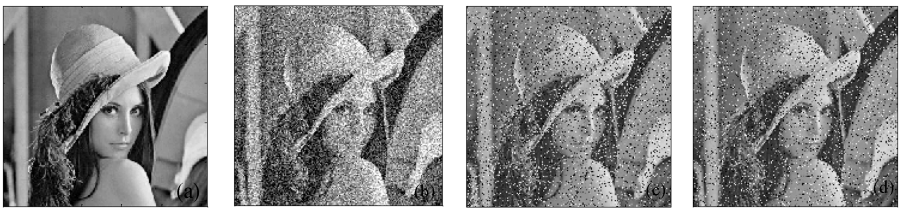

Figure 6 Decrypted images when the cipher-image is blurred by noise or geometrical distortion (four rounds of encryption). (a) Noise free; (b) gauss noise ($\mu=0$, $\sigma=10$); (c) scratching with vertical 5% pixels rubbed; (d) Salt and pepper noise ($p=0.05$).

Table 3 Degree of similarity between original image and decrypted image when the cipher-image is contaminated

Similarity degree	Round	Gauss noise ($\mu=0$, $\sigma=10$)	Scratching (5% pixels rubbed)	Pepper and salt noise ($p=0.05$)
MSE	n=4	1890.65	1122.35	1155.89
	n=8	4131.50	2792.78	3423.80
MAE	n=4	27.20	9.03	10.22
	n=8	49.40	26.92	29.97

between the algorithm robustness and the recovery capability in different applications.

5 Conclusion

A novel image encryption algorithm using two chaotic maps alternately is discussed in this paper. Compared with the single chaotic map scheme, the proposed algorithm exhibits higher robustness. Both the encryption and the decryption in this scheme have the same processing procedure, so there is no need to design the decryption system additionally. Due to the structure similar to the style of Feistel block cipher, the proposed algorithm can complete the encryption of two pixel blocks (L_0 and R_0) at one time, which is helpful for increasing data throughput. 32-bit fix-point operations are employed in our experiments, and then the security analysis shows that the method can resist many forms of cryptanalysis. Furthermore, the algorithm features high execution speed and compact program, which is suitable for various software and hardware applications.

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, 522－525

2 Alvarez G, Montoya F, Romera M, et al. Breaking two secure communication systems based on chaotic masking. IEEE Trans Circ Syst, 2004, 51(10): 505－506

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, 50(20): 275－279

4 Ma Z G, Qiu S S. An image cryptosystem based on general cat map. J China Inst Commun (in Chinese), 2003, 24(2): 51－57

5 Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos, 1998, 8(6): 1259－1284

6 Kaneko K. Spatiotemporal chaos in one- and two-dimensional coupled map lattices. Phys D, 1989, 37: 60－82

7 Guo J S, Jin C H. An attack with known image to an image cryptosystem based on general cat map. J China Inst Commun (in Chinese), 2005, 26(2): 131－135

8 Chen G, Mao Y, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 2004, 21(3): 749－761

9 Wang S H, Xiao J H, Wang X G, et al. Spatial orders appearing at instabilities of synchronous chaos of spatiotemporal systems. Eur Phys J B, 2002, 30(4): 571－575

10 Feistel H. Cryptography and computer privacy. Sci Am, 1973, 228(5): 15－23

11 Webster A F, Tavares S E. On the design of S-boxes. Advances in Cryptology: Proceedings of CRYPTO'85. Berlin: Springer-Verlag, 1985, 523－534