Available online at www.sciencedirect.com
ScienceDirect
Chaos, Solitons and Fractals 38 (2008) 213–220
CHAOS SOLITONS & FRACTALS
www.elsevier.com/locate/chaos

Image encryption based on a new total shuffling algorithm

Tiegang Gao [a,*], Zengqiang Chen [b]

[a] College of Software, Nankai University, Tianjin 300070, PR China
[b] Department of Automation, Nankai University, Tianjin 300070, PR China

Accepted 10 November 2006

Communicated by Prof. M.S. El Naschie

Abstract

This paper presents image encryption scheme, which employs a new image total shuffling matrix to shuffle the positions of image pixels and then uses the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image. The experimental results demonstrate that the new image total shuffling algorithm has a low time complexity and the suggested encryption algorithm of image has the advantages of large key space and high security, and moreover, the distribution of grey values of the encrypted image has a random-like behavior.

1. Introduction

With the rapid developments in digital image processing and network communication, electronic publishing and widespread dissemination of digital multimedia data over the Internet, protection of digital information against illegal copying and distribution has become extremely important. To meet this challenge, many new encryption schemes have been proposed [1–4]. Among them, chaos-based algorithms has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption, and it has been proved that in many aspects chaotic maps have analogous but different characteristics as compared with conventional encryption algorithms [5–9].

The chaos-based encryption was first proposed in 1989 [10], since then, many researchers have proposed and analyzed a lot of chaos-based encryption algorithms, these work all have been motivated by the chaotic properties such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity. While classical encryption algorithms are sensitive to keys, so some elaborated constructions are need to achieve satisfying and safer chaos-based encryption.

It is well known a good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute-force attacks infeasible [11]. Recently, in [12], a fast chaotic cryptographic scheme based on iterating a logistic map was proposed, and no random numbers need to be generated and the look-up table used in the cryptographic process is updated dynamically. In [13], a two-dimensional chaotic cat map is generalized to 3D

* Corresponding author.
E-mail address: gaotiegang@nankai.edu.cn (T. Gao).

0960-0779/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chaos.2006.11.009

for designing a real-time secure symmetric encryption scheme, which employs the 3D cat map to confuse the relationship between the cipher-image and the plain-image. Also recently, the authors in [14] thought that the algorithm for encoding binary images using one-dimensional chaotic map [15] is not secure enough, and there is the same problem with the algorithm proposed in [16], to overcome the drawbacks such as small key space and weak security of one-dimensional chaotic map, a nonlinear chaos algorithm is proposed in [17], which shows high-level security and acceptable efficiency.

A new image encryption scheme is suggested in this paper, different from the 2D or 3D chaotic map that is used to shuffle the pixel positions of the plain-image, a new image total shuffling matrix is used to shuffle the position of the pixels and the states combination of two chaos are used to change the grey values of the plain-image in our method. The rest of this paper is organized as follows. Section 2 presents the proposed image total shuffling algorithm and image encryption algorithm through combination of states of chaotic systems. Section 3 describes some simulation outcomes, some security analysis are given in Section 4. Finally, Section 5 concludes the paper.

2. The proposed encryption algorithm

2.1. Generation of image total shuffling matrix

Image data have strong correlations among adjacent pixels, in order to disturb the high correlation among pixels; an image total shuffling matrix is used to shuffle the position of the plain-image. Without loss of generality, we assume that the dimension of the plain-image $N \times M$, the position matrix of pixels is $P_{i,j}$, $i = 0, 1, \ldots, M-1$; $j = 0, 1, \ldots, N-1$ the procedure of generation for shuffling matrix is described as follows:

(1) For Logistic map $x_{n+1} = 4x_n(1 - x_n)$ and a given x_0, after do some iterations, a new x_0 is derived, then let

$$l = \mathrm{mod}(x_0 \times 10^{13}, M) \tag{1}$$

Obviously, $l \in [0, M-1]$.

(2) Continue to do the iteration of Logistic map and do (1) until we get M different data which are all between 0 and $M-1$, these data can be recorder in the form of $\{h_i, i = 1, 2, \ldots, M\}$, where $h_i \neq h_j$ if $i \neq j$. Then rearrange the row of matrix $P_{i,j}$ according to $\{h_i, i = 1, 2, \ldots, M\}$, that is, move the h_1 row to the first row, h_2 row to the second row, thus a new position matrix $P^h_{i,j}$ is generated based on the transformation.

For the new matrix $P^h_{i,j}$, we will produce column shuffling matrix column by column. The process is presented next.

(1) Use the present x_0 to do the iteration of Logistic map and then let

$$l = \mathrm{mod}(x_0 \times 10^{13}, N) \tag{2}$$

It is easily can be seen, $l \in [0, N-1]$.

(2) Continue to do the iteration of Logistic map and do (2) until we get N different data which are all between 0 and $N-1$, these data can be expressed $\{l_i, i = 1, 2, \ldots, N\}$, where $l_i \neq l_j$ if $i \neq j$. Then rearrange the data of every column for the first row of matrix $P_{i,j}$ according to $\{l_i\}$, that is, move the l_1 column to the first column, l_2 column to the second column, thus a new column transformation of the first row of matrix $P^h_{i,j}$ is generated.

(3) From the second row till the last row of matrix $P^h_{i,j}$, do the same column transformation in the same way as the second step, thus a new image total shuffling matrix $P^{hl}_{i,j}$ is given, and if N and M are not very big, the algorithm have lower time complexity, which can be summarized in Table 1.

Table 1
Time complexity of *image total shuffling algorithm*

Size of the image	The average number of iteration needed to accomplish a row transformation
32×32	80
64×64	300
128×128	520
256×256	1600

2.2. Lorenz chaotic system and Chen's chaotic system

In the proposed encryption scheme, Lorenz chaotic system is one that is employed in key scheming, which is modeled by Beldhouche and Qidwai [18]

$$\begin{cases} \dot{x}_1 = p(x_2 - x_1), \\ \dot{x}_2 = -x_1x_3 + rx_1 - x_2, \\ \dot{x}_3 = x_1x_2 - tx_3. \end{cases} \tag{3}$$

where p, r and t are parameters, when $p = 10$, $r = 28$, $t = 8/3$, the system is chaotic.

Another chaotic system in our scheme is Chen's chaotic system, which is described as follows [18]:

$$\begin{cases} \dot{x}_4 = a(x_5 - x_4), \\ \dot{x}_5 = (c - a)x_4 - x_4x_6 + cx_5, \\ \dot{x}_6 = x_4x_5 - bx_6. \end{cases} \tag{4}$$

where a, b and c are parameters, when $a = 35$, $b = 3$, $c = 28$, the system is chaotic. Simulation shows the system orbit is extremely sensitive to the parameter c.

Although the equation of Chen's system are very similar to that of Lorenz system, the topologically they are not equivalent [17]. The chaotic behaviors of the two systems are shown in Fig. 1.

2.3. Encryption algorithm design

The image encryption scheme is based on the combination of state variables of the above two chaotic systems. Three of the variables are combined differently, which may produce 20 different combinations table, which is given in Table 2.

Then, the encryption process is given as follows:

Step 1: Assume the dimension of original grayscale image is $N \times N$, the pixels of the image are arranged by order from left to right and top to bottom, then we can get image data set $B = \{B_1, B_2, \ldots, B_{N\times N}\}$, in which each element is the decimal grey value of the pixel.

Step 2: Generate a $N \times N$ magic total shuffling matrix, and shuffle the position of the pixels of plain-image according to the matrix.

Step 3: Iterate the Lorenz chaotic system and Chen's chaotic system for N_0 and M_0 times to avoid the harmful effect of transitional procedure, respectively. $N_0 \neq M_0$.

Step 4: The Lorenz system and Chen's system are iterated simultaneity, and as a result, six decimal fractions x_1, x_2,x_3, x_4, x_5, x_6 will be generated. These decimal values are preprocessed firstly as follows:

$$x_i = \mathrm{mod}((\mathrm{abs}(x_i) - \mathrm{Floor}(\mathrm{abs}(x_i)) \times 10^{13}, 256), \quad i = 1, 2, \ldots, 6$$

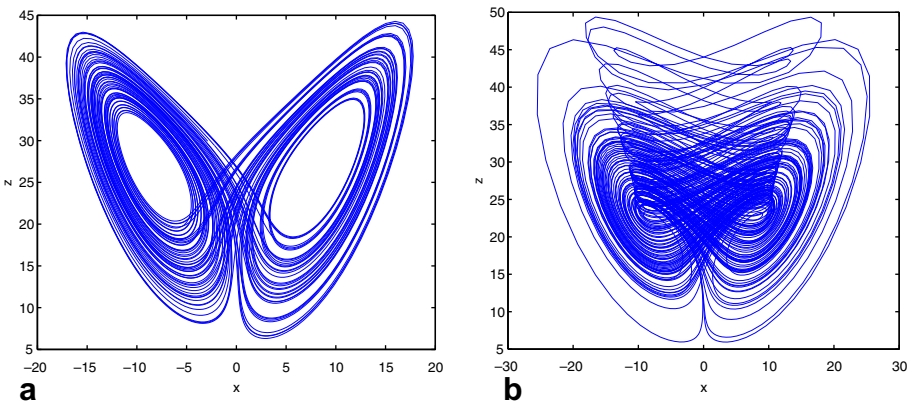

Fig. 1. Chaos attractors of Lorenz system (a) and Chen system (b).

Table 2
Different combinations of States between Lorenz and Chen system

Serial number	Combination of states	Serial number	Combination of states
0	(x_1, x_2, x_3)	1	(x_1, x_2, x_4)
2	(x_1, x_2, x_5)	3	(x_1, x_2, x_6)
4	(x_1, x_3, x_4)	5	(x_1, x_3, x_5)
6	(x_1, x_3, x_6)	7	(x_1, x_4, x_5)
8	(x_1, x_4, x_6)	9	(x_1, x_5, x_6)
10	(x_2, x_3, x_4)	11	(x_2, x_3, x_5)
12	(x_2, x_3, x_6)	13	(x_2, x_4, x_5)
14	(x_2, x_4, x_6)	15	(x_2, x_5, x_6)
16	(x_3, x_4, x_5)	17	(x_3, x_4, x_6)
18	(x_3, x_5, x_6)	19	(x_4, x_5, x_6)

where abs(x) returns the absolute value of x. Floor(x) returns the value of x to the nearest integers less than or equal to x, to make the states of the two chaotic systems correlative, let

$$x_4 = x_4 \oplus x_1, x_5 = x_5 \oplus x_2 x_6 = x_6 \oplus x_3 \tag{5}$$

Step 5: Generates $\bar{x}_1$ by using the following formula:

$$\bar{x}_1 = \mathrm{mod}(x_1, 20) \tag{6}$$

As $\bar{x}_1 \in [0, 19]$, so from Table 1, we select the corresponding group that are used to perform encryption operation if $\bar{x}_1$ equals to the serial number of sequence of the group. The encryption operation is to do XOR between 3 bytes of image data and the 3 bytes of resulting group data, according to the following formula:

$$\begin{aligned} C_{3\times i+1} &= (B_{i+1} \oplus B_{x_1}) \oplus C_{3\times i} \\ C_{3\times i+2} &= (B_{3\times i+2} \oplus B_{x_2}) \oplus C_{3\times i+1} \\ C_{3\times i+3} &= (B_{3\times i+3} \oplus B_{x_3}) \oplus C_{3\times i+2} \end{aligned} \tag{7}$$

where $i = 0, 1, \ldots$ represents the $i-1$th iteration of the two chaotic systems. The symbol $\oplus$ represents the exclusive OR operation bit-by-bit. B_{x_i} $i = 1, 2, 3$ represents state values of the corresponding group with respect to serial $\bar{x}_1$. The initial C_0 is set to be 128, the process do not end until the set $B = \{B_1, B_2, \ldots, B_{N\times N}\}$ is all encrypted. Then the encrypted pixel set $C = \{C_1, C_2, \ldots, C_{N\times N}\}$ is written to the cipher-image.

3. Experimental analysis

Experimental analysis of the proposed image encryption algorithm in this paper has been done. The plain-image with the size 200×200 is shown in Fig. 2a and the histogram of the plain-image is shown in Fig. 2b. Image we get through change of 200×200 image total shuffling matrix is shown in Fig. 2c and the corresponding histogram in shown in Fig. 2d. The encrypted image is shown in Fig. 2e and the histogram is shown in Fig. 2f. From the figure, one can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image.

4. Security analysis

A good encryption should resist all kinds of known attacks, it should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. Some security analysis has been performed on the proposed image encryption scheme.

4.1. Key space analysis

In our algorithm, the initial values of Lorenz system and Chen's system are used as secret keys, if the precision is 10^{-14}, the key space size is 10^{84}. Moreover, the initial iteration number N_0 and M_0 are also used as the secret keys. This is enough to resist all kinds of brute-force attacks.

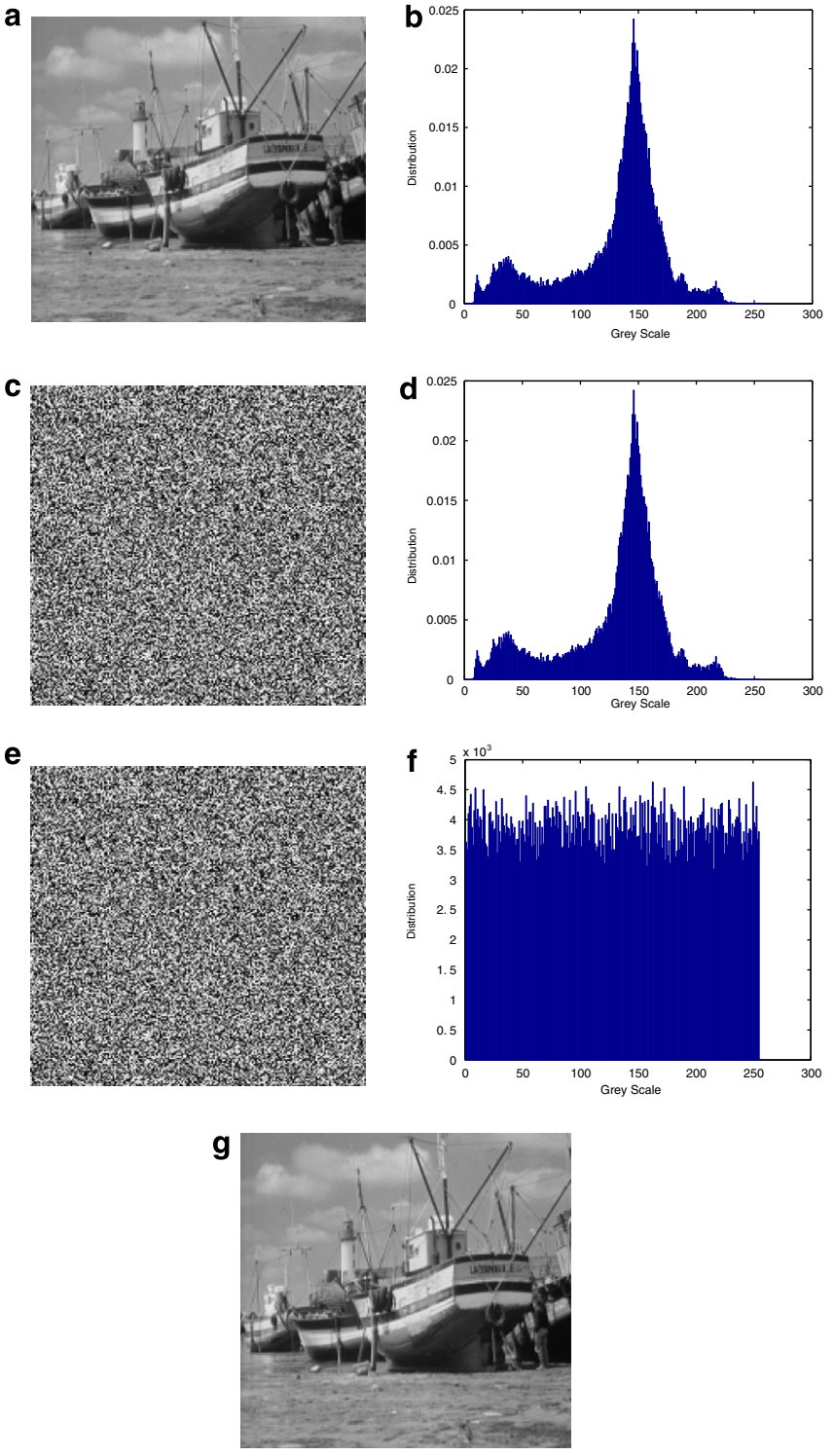

Fig. 2. Image encryption and decryption experimental result: (a) original image; (b) histogram of the original image; (c) image after change with magic square matrix; (d) histogram with magic square matrix change; (e) ciphered image; (f) histogram of the ciphered image; and (g) decrypted image.

4.2. Key sensitivity test

Several key sensitivity tests are performed. Fig. 3a–d illustrates the sensitivity of our scheme to the secret key x_1, x_2, x_3, x_4, x_5, x_6, N_0 and M_0. Fig. 3a is the decrypted image with the parameters to be $x_1(0) = 0.3000000000001$, $x_2(0) = -0.4$, $x_3(0) = 1.2$ $x_4(0) = 10.2$, $x_5(0) = -3.5$, $x_6(0) = 4.4$ and $N_0 = 3000$ and $M_0 = 2000$ while the actual encryption parameters are all the same except that $x_1(0) = 0.3$. Fig. 3c is the decrypted image with all the parameters to be same as that used in encryption algorithm except $N_0 = 3001$. Fig. 3b and d are corresponding histograms of the decrypted image. So it can be concluded that the chaotic encryption algorithm is sensitive to the key, a small change of the key will generate a completely different decryption result and cannot get the correct plain-image.

4.3. Analysis of correlation of two adjacent pixels

To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels, respectively, in a ciphered image, some simulations are carried out. Firstly, randomly select 2500 pairs of two adjacent pixels from the image, then calculate the correlation coefficient of each pair by using the following formulas [12]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x_i))^2$$

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

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

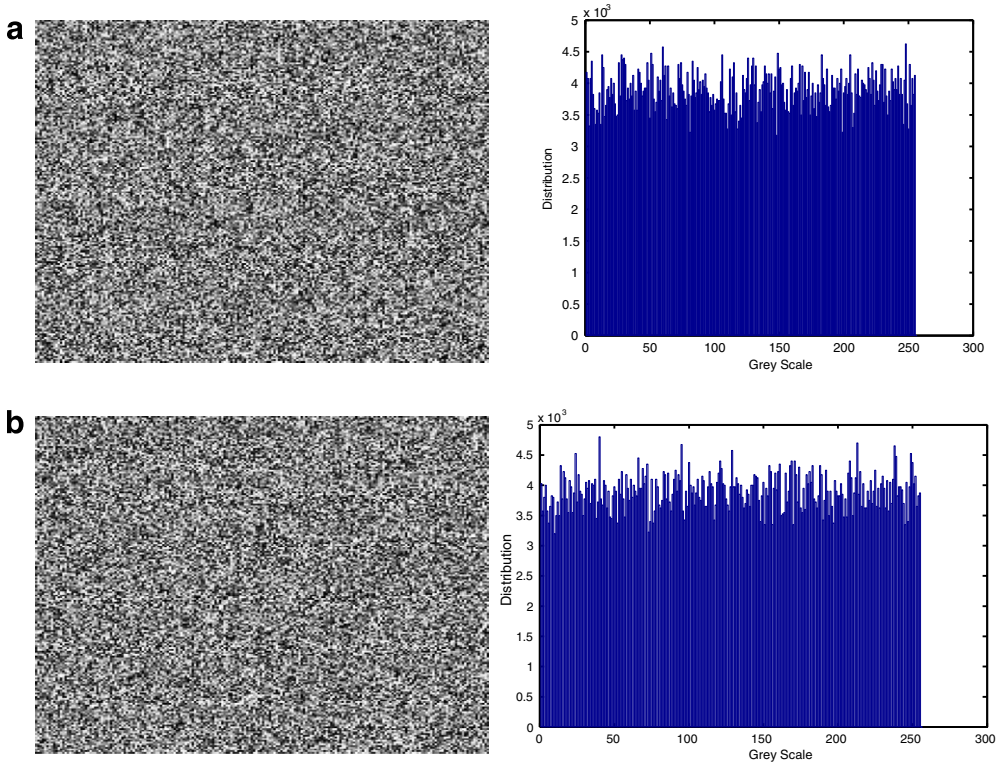

Fig. 3. Image encryption and decryption experimental result: (a) decrypted image with different initial value and (b) decrypted image with different initial iterate value.

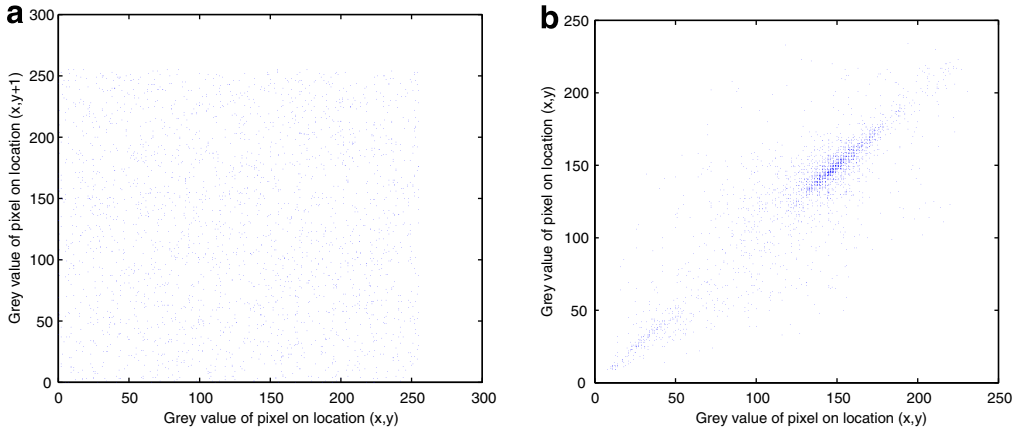

Fig. 4. Correlations of two vertically adjacent pixels in the original image and in the ciphered image: (a) correlations in the ciphered image and (b) correlations in the original image.

Table 3
Correlation coefficients of two adjacent pixels in two images

Model	Original image	Ciphered image
Horizontal	0.9169	−0.0131
Vertical	0.9287	−0.0273
Diagonal	0.8668	−0.0313

where x and y are grey values of two adjacent pixels in the image. Fig. 4 shows the correlation distribution of two vertically adjacent pixels in the original image and that in the ciphered image. The correlation coefficients are 0.9287 and −0.0273, respectively. Other test results are shown in Table 3.

5. Conclusions

In this paper, a new chaos encryption algorithm is proposed, which uses image total shuffling matrix to shuffle the pixel positions of the plain-image and then the combination of chaos is used to change the grey values of the shuffled-image. Some security analysis are given to demonstrate that the key space of the new algorithm is large enough to make brute-force attacks infeasible, digital simulations have been carried out with detailed numerical analysis, demonstrating the high security of the new image encryption scheme, which may have some potential application in image encryption and information transmission based on Internet.

Acknowledgements

The author would like to thank the support from CNSF Grant # 60374037 and 60574036, the Specialized Research Fund for the Doctoral Program of Higher Education of China Grant # 20050055013, and the Program for New Century Excellent Talents of China (NCET) to Z.Q. Chen.

References

[1] Chang CC, Hwang MS, Chen TS. A new encryption algorithm for image cryptosystems. J Syst Software 2001;58:83–91.
[2] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos 1998;8(6):1259–84.
[3] Zhang LH, Liao XF, Wang XB. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals 2005;24:759–65.
[4] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circ Syst Mag 2001;1(3):6–21.
[5] Kocarev L, Jakimovski G. Chaos and cryptography: from chaotic maps to encryption algorithms. IEEE Trans Circ Syst – 1 2001;48(2):163–9.

[6] Bu SL, Wang BH. Improving the security of chaotic encryption by using a simple modulating method. Chaos, Solitons & Fractals 2004;19:919–24.
[7] Mao YB, Chen G, Lian SG. A novel fast image encryption scheme based on the 3D chaotic baker map. Int J Bifurcat Chaos 2004;14:3613–24.
[8] Chee CY, Xu D, Steven R, Bishop B. A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation. Chaos, Solitons & Fractals 2004;21:1129–34.
[9] Chien T-I, Liao T-L. Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization. Choas, Solitons & Fractals 2005;24:241–55.
[10] Matthews R. One the derivation of a chaotic encryption algorithm. Cryptologia 1989;8(1):29–42.
[11] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. 2nd ed. New York: Wiley; 1995.
[12] Wong KW. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A 2002;298:238–42.
[13] Chen G, Mao YB, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Choas, Solitons & Fractals 2004;21:749–61.
[14] Li S, Zheng X. Cryptanalysis of a chaotic image encryption method. In: Proceedings of the IEEEE international conference on circuits and systems, vol. 2; 2002. p. 708–11.
[15] Yen JC, Go JI. A new chaotic – key-based design for image encryption and decryption. In: Proceedings of the IEEE international conference on circuits and systems, vol. 4; 2000. p. 49–52.
[16] Beldhouche F, Qidwai U. Binary image encoding using 1D chaotic map. In: Proceedings of the IEEE annual technical conference; 2003. p. 39–43.
[17] Gao HJ, Zhang YS, Liang SY, Li DQ. A new chaotic algorithm for image encryption. Choas, Solitons & Fractals 2006;29:393–9.
[18] Lü JH, Chen GR. A new chaotic attractor coined. Int J Bifurcat Chaos 2002;12(3):659–61.