Science in China Series G: Physics, Mechanics & Astronomy

© 2009 SCIENCE IN CHINA PRESS

Springer-Verlag

www.scichina.com
phys.scichina.com
www.springerlink.com

Spatial chaos-based image encryption design

LIU ShuTang & SUN FuYan[†]

College of Control Science and Engineering, Shandong University, Ji'nan 250061, China

In recent years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. In this paper, permutation and substitution methods are incorporated to present a stronger image encryption algorithm. Spatial chaotic maps are used to realize the position permutation, and to confuse the relationship between the cipher-image and the plain-image. The experimental results demonstrate that the suggested encryption scheme of image has the advantages of large key space and high security; moreover, the distribution of grey values of the encrypted image has a random-like behavior.

spatial chaos, two-dimensional logistic map, spatial bifurcation, image encryption

During the last decades, the use of chaos in cryptography has been of great interest in many areas, including a database, internet transaction banking, multimedia systems, and medical imaging, because chaotic systems have several significant advantages favorable to secure communications[1−3], such as aperiodicity (useful for one time pad cipher), sensitive dependence on initial conditions and system parameters (useful for confusion and diffusion processes), and ergodicity and random-like behaviors (useful for producing output with satisfactory statistics). Chaotic communication schemes are based on either discrete or continuous systems. Many cryptosystems based on continuous systems utilize the idea of synchronization of chaos[4−6]. However, recent studies show that the performance of these communication schemes is very poor and most models of chaos communications are insecure[7]. Recently, much attention has been given to chaotic communication schemes based on discrete systems, and many encryption schemes have been proposed based on different principles[8−16]. The basic ideas may be classified into the following major types: value transformation[8], position permutation[10], and their combining form[11]. Moreover, multiple chaotic systems[12], high-dimensional chaotic systems[13], multiple iterations of chaotic systems[14] and other techniques[15,16] have been proposed. But some of them have been known to be insecure, and various cryptanalyses have exposed some inherent drawbacks of chaotic cryptosystems[17−19]. To improve the degree of the privacy, spatiotemporal chaotic systems are widely used in chaotic cryptography for the excellent chaotic dynamical properties[16]. A spatiotemporal chaotic system is a spatially extended system that exhibits spatiotemporal chaos, i.e., nonlinear dynamics in both space and time. Coupled map lattices (CMLs) are often adopted as the basic model of a spatiotemporal chaos system. Wang et al.[17] have shown that the communication with the CMLs is more secure than the communication with a single map.

In this paper, a new design of a class of chaotic cryptosystems is suggested to overcome the aforementioned drawbacks by using high dimensional chaotic map and some conventional cryptography techniques for obtaining the high level security. A spatial chaotic map is a high-dimensional dynamical system based on the

Received March 11, 2008; accepted May 23, 2008
doi: 10.1007/s11433-009-0032-2

[†] Corresponding author (email: fuyan.sun@gmail.com)

Supported by the National Natural Science Foundation of China (Grant No. 60874009) and the Foundation for the Author of National Excellent Doctoral Dissertation of China (Grant No. 200444)

nonlinear duality function[20], and a lot of research results of spatial chaos system, such as spatial periodic orbits, spatial lyapunov exponents and spatial chaos synchronization have been given[20−29]. Here we use high-dimensional chaos as the basic structure of the cryptography, which leads to the following significant advantages: Due to the high-dimensionality and chaoticity, the output cipher-text has high complexity, long periodicity of computer realization of chaos, and effective byte confusion and diffusion in many directions in the variable space. All these properties are favorable to achieve high practical security. In this paper, we propose that the image encryption/decryption method belongs to the combining form of value transformation and position permutation. Spatial chaotic map is used to generate random sequence to shuffle the positions of pixels in the image. Meanwhile, another two different parameters spatial chaotic maps are used to confuse the relationship between cipher-image and plain-image.

1 Spatial chaotic system

The spatial generalized two-dimensional (2D) system difference form goes as follows[22,23,26−28]:

$$x_{m+1,n} + \omega x_{m,n+1} = f(\mu,(1+\omega)x_{m,n}), \tag{1}$$

where $f(\mu,(1+\omega)x_{m,n})$ is nonlinear function, m、n *and* $x_{m、n}$ are three dimensional space geometric coordinates, μ is a real parameter, and ω is a constant. In fact, System (1) can be regarded as a discrete analog of the following functional partial differential system:

$$\frac{\partial v}{\partial x} + \omega\frac{\partial v}{\partial y} = f(\mu,(1+\omega)v). \tag{2}$$

System (2) is a *convection equation* with a forced term, quite classical in physics. Therefore, qualitative properties of System (1) may lead to some useful information for analyzing this companion partial differential system.

Noting that when $n=n_0$, $\omega=0$, the system may be reduced to one-dimensional model:

$$x_{m+1,n_0} = f(\mu,x_{m,n_0}). \tag{3}$$

Because n_0 is a constant, the above equation can be written as

$$x_{m+1} = f(\mu,x_m). \tag{4}$$

This is a familiar one-dimensional model. Specially, when $f(\mu,x_m) = \mu x_m(1-x_m)$, the equation is described as

$$x_{m+1} = \mu x_m(1-x_m), \tag{5}$$

which is a well-known classical one-dimensional Logistic system. When the parameter $3.7<\mu<4$, the system is chaotic.

Particularly, when $f(\mu,(1+\omega)x_{m,n}) = 1-[\mu(1+\omega)\times x_{m,n}]^2$, the 2D discrete dynamic system is described as

$$x_{m+1,n} + \omega x_{m,n+1} = 1-[\mu(1+\omega)x_{m,n}]^2. \tag{6}$$

Research shows that when $2>\mu\geqslant 1.55$, $\omega\in(-1,1)$, the system is in a chaotic state. Since there are two iterations variables, it can be called the spatial 2D Logistic map.

The spatial chaotic system is a generalization of one-dimension chaotic map[22−29]. Since there are m and n two variables in spatial chaotic map, the encrypting sequence produced by this system is more complex and random-like than the one-dimensional chaotic system (only one variable m). It is more difficult to forecast such chaotic sequences. Therefore, spatial chaotic system is more advantageous than the low-dimensional chaotic system. Compared with the one-dimensional logistic chaotic system, there are two control parameters μ and ω in the spatial chaotic system, and what's more, simulation shows that the generalized spatial dynamic system orbit is extremely sensitive to the parameters[22−29]. The above spatial chaotic system generates chaotic behaviors for a wide parameter range, so the parameters μ, ω and initial values may all be used as secret keys. Specially when the parameters $\mu=1.75$, $\omega=-0.05$, the chaotic and 2D bifurcation behavior of System (6) are shown in Figures 1—3.

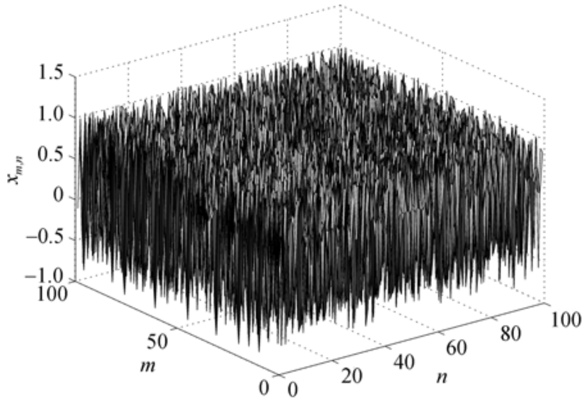

Figure 1 Chaotic behavior of spatial chaotic system when $\mu=1.75$, and $\omega=-0.05$.

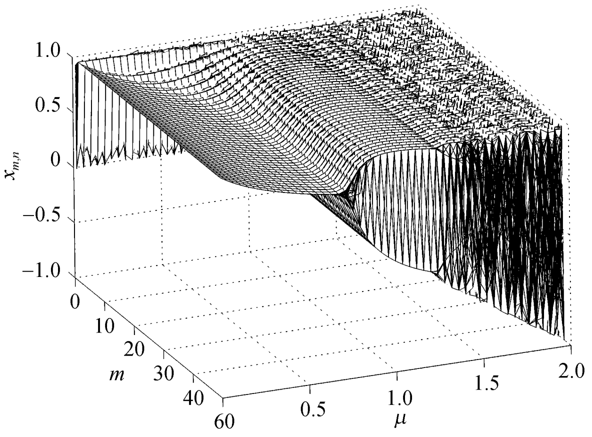

Figure 2 Bifurcation behavior of System (6) in space.

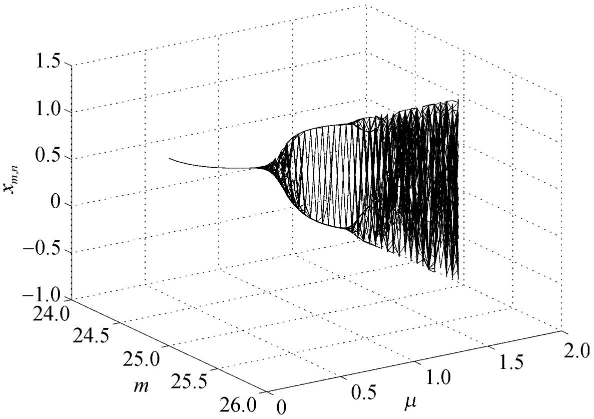

Figure 3 A section of spatial bifurcation phenomena of System (6).

In the proposed method, three different parameter values spatial chaotic maps are employed to achieve the goal of image encryption. The first is when $\mu_1 = 1.6$, $\omega_1 = -0.05$, the second is when $\mu_2 = 1.75$, $\omega_2 = -0.05$, and the third is when $\mu_3 = 1.78$, $\omega_3 = -0.05$. The corresponding equations are as follows:

$$x_{m+1,n} - 0.05x_{m,n+1} = 1 - 1.6[(1-0.05)x_{m,n}]^2, \tag{7}$$

$$y_{m+1,n} - 0.05y_{m,n+1} = 1 - 1.75[(1-0.05)y_{m,n}]^2, \tag{8}$$

$$z_{m+1,n} - 0.05z_{m,n+1} = 1 - 1.78[(1-0.05)z_{m,n}]^2. \tag{9}$$

2 The proposed method

2.1 Permutation

According to Golomb's three postulates for pseudo-random sequence, idea chaotic sequences should have such statistical characteristics as follows.

Its average value is zero, the autocorrelation is delta function, and the mutual correlation is zero.

A demonstration of autocorrelation and cross-correlation properties of the achieved sequence $\{x_{i,j}\}$ by eq. (7) is given in Figure 4. Figure 4(a) shows the autocorrelation characteristics, and Figure 4(b) shows the cross-correlation characteristics of two sequences only with a low change ($<10^{-10}$) of initial value, which indicates that $\{x_{i,j}\}$ is sensitive to the secret key. One may know that $\{y_{i,j}\}$ and $\{z_{i,j}\}$ are also sensitive to the secret key in the same way.

Image data have strong correlations among adjacent pixels, and in order to disturb the high correlation among pixels, a higher-dimensional spatial chaotic map is used to shuffle the position of the plain-image. Without loss of generality, we assume that the dimension of the plain-image is $M \times N$; the position matrix of pixels is $Q_{i,j}$ $(i = 0,1,\ldots,M-1,\ j = 0,1,\ldots,N-1)$. The procedure for shuffling the position of pixels is described as follows:

Step 1: For System (7) and a given $x_{0,0}$, after doing

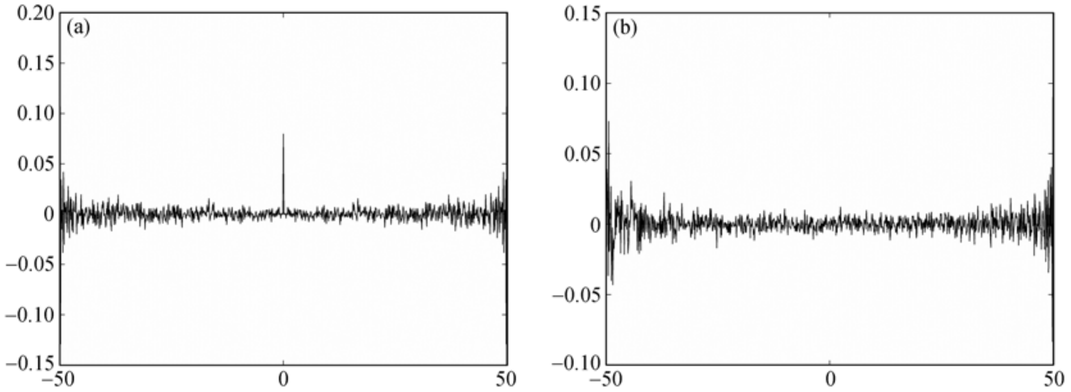

Figure 4 Autocorrelation and cross-correlation characteristics.

some iterations, $x_{m,n}$ is derived as a new $x_{0,0}$, and then let

$$h = \mathrm{mod}(x_{0,0} \times 10^{14}, M), \qquad (10)$$

$h \in [0, M-1]$. Continue to do the iteration of spatial chaotic map and do eq. (10) until one gets M different data which are all between 0 and $M-1$, and these data may 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 $Q_{i,j}$ according to h_i, $i = 1, 2, \ldots, M$, that is, move the h_1 row to the first row and h_2 row to the second row, and thus a new position matrix $Q_{i,j}^h$ is generated based on the transformation. For the new matrix $Q_{i,j}^h$, we will produce column shuffling matrix column by column. The process is presented in the following.

Step 2: Using the present $x_{0,0}$ to do the iteration of eq. (7), then let

$$c = \mathrm{mod}(x_{0,0} \times 10^{14}, N). \qquad (11)$$

It is easy to see that $c \in [0, N-1]$. Continue to do the iteration of spatial chaotic map and do eq. (11) until we get N different data, all between 0 and $N-1$, and these data can be expressed c_i, $i = 1, 2, \ldots, N$, where $c_i \neq c_j$, if $i \neq j$. Then rearrange the data of every column for matrix $Q_{i,j}^h$ according to c_i, that is, move the first column to the c_1 column and the second column to c_2 column, and thus a new column transformation of matrix $Q_{i,j}^h$ is generated.

In order to further enhance the security, the column transformation can be done line by line, that is, from the first row of matrix till the last row of matrix $Q_{i,j}^h$, the column transformation in the same way as the second step can be done under different $x_{0,0}$.

2.2 Substitution

The encryption process consists of three steps of operation.

Step 1: Each element of the pixels of the shuffled image is the decimal grey value. Convert decimal pixel values to binary numbers and get a new $M \times N$ matrix $B(i, j)$.

Step 2: Choose two arbitrary initial conditions $y'_{0,0}$, $z'_{0,0}$, and quantize $y'_{0,0}$, $z'_{0,0}$ to binary values $y_{0,0}$, $z_{0,0}$. The two binary chaotic sequences $\{y_{i,j}\}$ and $\{z_{i,j}\}$ are generated corresponding to eqs. (8) and (9). Respectively, intercept finite sequences from $\{y_{i,j}\}$ and $\{z_{i,j}\}$ to construct two $M \times N$ matrixes Y and Z.

Step 3: The substitution of $C(i, j)$ is defined by

$$C(i,j) = (((B(i,j) + Y(i,j)) \bmod 2) \otimes Z(i,j),$$

where $0 \leqslant i \leqslant M-1$, $0 \leqslant j \leqslant N-1$. This operation is implemented until all the elements in the image are encrypted. The decryption process is evident. Conversely, the encryption process is executed and the decrypted image will be obtained.

3 Experimental results and security analysis

3.1 Key sensitivity test

In this paper, experimental analysis of the proposed encryption scheme has been done with several images. Figure 5 is the 256 grey-scale plain-image and encrypted image of size 256×256 with the key: $K = (x_{0,0} = y_{0,0} = z_{0,0} = 0.98;\ \omega_1 = \omega_2 = \omega_3 = -0.05;\ \mu_1 = 1.6,\ \mu_2 = 1.75,\ \mu_3 = 1.78)$. The histograms of the plain-image and the corresponding encrypted image are shown in Figure 6. As is seen, the encrypted histogram is fairly uniform. Figure 7(a) is the decrypted image by using the right keys. It can be seen that the decrypted image is clear and correct without any distortion. But if we use the wrong keys: $K = (x_{0,0} = y_{0,0} = z_{0,0} = 0.98;\ \omega_1 = \omega_2 = \omega_3 = -0.05;\ \mu_1 = 1.6,\ \mu_2 = 1.75,\ \mu_3 = 1.78000000000001)$ or $K = (x_{0,0} = y_{0,0} = z_{0,0} = 0.98000000000001;\ \omega_1 = \omega_2 = \omega_3 = -0.05;\ \mu_1 = 1.6,\ \mu_2 = 1.75,\ \mu_3 = 1.78)$, two the unexpected images will be gotten. Figure 7(b) shows the decrypted image by using the incorrectly key. So it may be concluded that the spatial chaotic encryption algorithm is sensitive to the key, a small change of the key will generate a completely different encryption result and cannot get the correct plain-image. As a result, differential attack would become very inefficient and practically useless.

3.2 Correlation analysis of two adjacent pixels

To test the correlation between two vertically adjacent

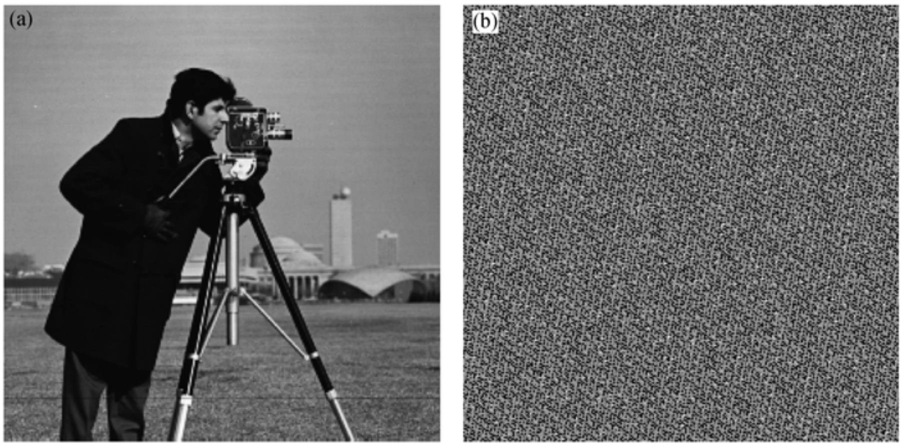

Figure 5 The experimental results of (a) plain image and (b) encrypted image.

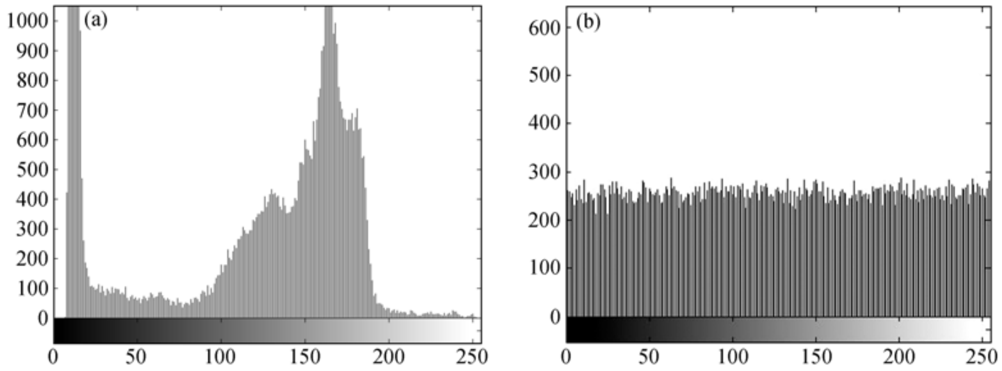

Figure 6 Histograms of (a) the plain-image and (b) encrypted image.

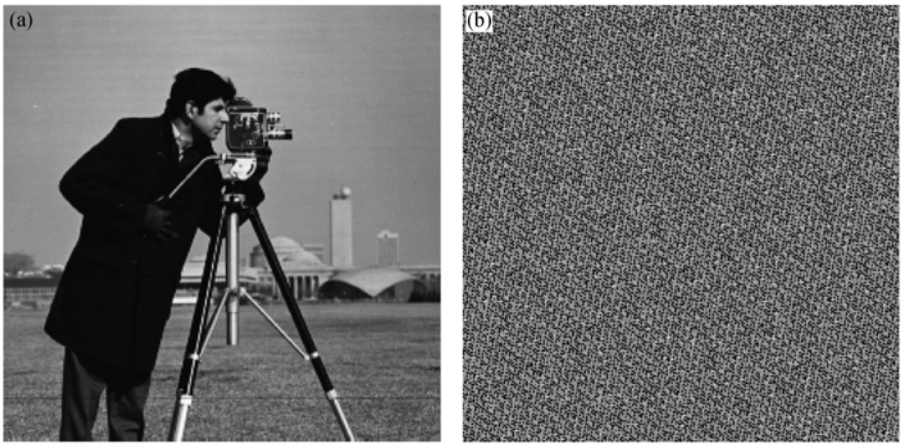

Figure 7 Decrypted image. (a) Decrypted image by correct key; (b) decrypted image by wrong key, $K = (x_{0,0} = y_{0,0} = z_{0,0} = 0.98;\ \omega = -0.05;\ \mu_1 = 1.6,\ \mu_2 = 1.75,\ \mu_3 = 1.7800000000000001)$.

pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels, respectively, in a cipher-image, the following procedure was carried out. 1000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-image and cipher-image were randomly selected and the correlation coefficients were calculated by the following formulas:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{12}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{13}$$

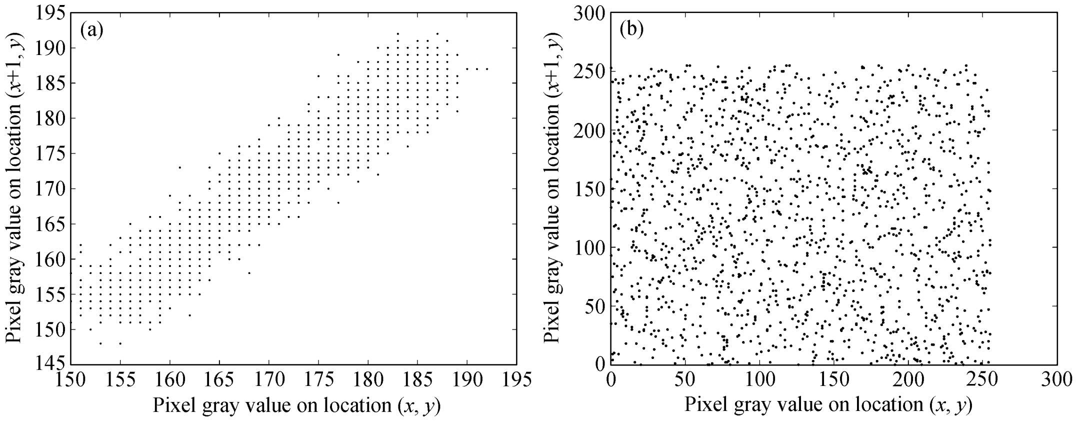

Figure 8 Correlations of two horizontally adjacent pixels for (a) the plain-image and (b) cipher-image.

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)), \tag{14}$$

where x and y are grey-scale values of two adjacent pixels in the image. Figures 8(a) and (b) show the correlation distribution of two horizontally adjacent pixels in the plain-image and that in the cipher-image. The correlation coefficients are shown in Table 1. These correlation analyses prove that the chaotic encryption algorithm satisfies zero co-correlation.

Table 1 Correlation coefficient of two adjacent pixels in plain-image and cipher-image

	Plain-image	Cipher-image
Horizontal	0.994948	2.44573×10^{-7}
Vertical	0.961046	-9.1226×10^{-8}
Diagonal	0.956190	9.2465×10^{-8}

3.3 Key space analysis

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. In this algorithm, the initial conditions and parameters of three equations may be used as keys. If the precision is 10^{-14}, the key space may reach 10^{126}. One may see the key space is large enough to resist the attacks.

3.4 Differential attack

As a general requirement for all the image encryption schemes, the encrypted image should be greatly different from its original form. To satisfy this requirement, two common measures, including the number of pixel change rate (NPCR) and unified average changing intensity (UACI), can be adopted. NPCR stands for the number of pixels change rate while one-pixel of plain image is changed. UACI measures the average intensity of differences between the plain-image and cipher-image. For calculation of NPCR and UACI, assume two cipher-images C_1 and C_2 whose corresponding plain-images have only one-pixel difference. The grey-scale values of the pixels of the cipher-image C_1 and C_2 at grid (i,j) are labeled as $C_1(i,j)$ and $C_2(i,j)$, respectively. Take an array $D(i,j)$ with the same size as image C_1 and C_2. Then, $D(i,j)$ is determined by $C_1(i,j)$ and $C_2(i,j)$. So, if $C_1(i,j)=C_2(i,j)$, then $D(i,j)=$ 1; otherwise, $D(i,j)=0$. NPCR and UACI are defined through the following formulas:

$$\text{NPCR}=\frac{\sum_{ij}D(i,j)}{W\times H}\times100\%, \tag{16}$$

$$\text{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times100\%, \tag{17}$$

where W and H are the width and height of C_1 or C_2. Tests have been performed on the proposed scheme, about the one-pixel change influence on a 256 grey-scale image of size 256×256. We obtained NPCR = 0.3870% and UCAI = 0.3042%. The results show that a small change in the original image will result in a significant shift in the cipher-image, so the algorithm proposed has a good ability to anti differential attack.

3.5 Other attacks

As for known-plaintext and chosen-plaintext attacks, the illegal users are assumed to have obtained several plain-image and cipher-image pairs, and both pairs share a common key K. In these cases, the outlaws can analyze these pairs to obtain the common key K, and correctly decrypt the next cipher-image if the sender still encrypts his next original image by K. To prevent these attacks, we define that our private key is disposable, i.e., it is requested to change the secret key frequently between each section of communication. Since no common key exists in our cryptosystem, no one may break our cryptosystem with the known-plaintext or the chosen-plaintext attack.

4 Conclusions

This paper presents a new encryption algorithm, which is to use spatial chaotic map to finish the encryption process. The proposed algorithm overcomes the drawbacks of small key space and weak security in the widely used 1D chaotic system. The statistical analysis, key sensitivity analysis, and key space analysis demonstrate that the encryption algorithm is effective and highly secure. Although the spatial chaotic system presented in this paper aims at 2D image encryption, it is not just limited to this area and may be widely applied in other fields such as 3D image encryption.

1 Hao B L. Starting with Parabolas: An Introduction to Chaotic Dynamics. Shanghai: Shanghai Scientific and Technological Education Publishing House, 1993

2 Brown R, Chua L O. Clarifying chaos: Examples and counterexamples. Int J Bifurcat Chaos, 1996, 6(2): 219—242[DOI]

3 Lasota A, Mackey M C. Chaos, Fractals, and Noise Stochastic Aspects of Dynamics. 2nd ed. New York: Springer, 1994

4 Yan S L, Chi Y Y, Chen W J. Chaotic laser synchronization and its application in optical fiber secure communication. Sci China Ser F-Inf Sci, 2004, 47(3): 332—347[DOI]

5 Dai J H. Chaotic application in information encryption. Chin Sci Bull, 1996, 41(5): 402—405

6 Zhang Y, Yu J M, Du G H. Continuous feedback chaotic synchronization and its application in secure communication. Chin Sci Bull, 1998, 43(17): 1831—1835

7 Zhou C S, Lai C H. Extracting messages masked by chaotic signals of time-delay systems. Phys Rev E, 1999, 60: 320—323[DOI]

8 Chang H K C, Liu J L. A linear quadtree compression scheme for image encryption. Signal Process-Image Commun, 1997, 10(4): 279—290[DOI]

9 Lu H P, Wang S H, Li X W, et al. A new spatiotemporally chaotic cryptosystem and its security and performance analyses. Chaos, 2004, 14(3): 617—629[DOI]

10 Yen J C, Guo J I. A new chaotic key-based design for image encryption and decryption. In: Proc IEEE Int Symposium on Circuits and Systems. Geneva: IEEE, 2000, 4: 49—52

11 Chen G R, Mao Y B, Chui C K. A symmetric image encryption scheme based on 3D chaotic cat maps. Int J Bifurcat Chaos Solitons Fractals, 2004, 21: 749—761[DOI]

12 Pareek N K, Patidar V, Sud K K. Cryptography using multiple one-dimensional chaotic maps. Commun Nonlinear Sci Number Simul, 2005, 10(7): 715—723[DOI]

13 Garcia P, Parravano A, Cosenza M G, et al. Coupled map networks as communication schemes. Phys Rev E, 2002, 65: 045201[DOI]

14 Zhou H, Ling X T. Problems with the chaotic inverse system encryption approach. IEEE Trans Circ Syst I, 1997, 44(3): 268—271[DOI]

15 Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map. Image Vision Comput, 2006, 24(9): 926—934[DOI]

16 Li P, Li Z, Halang W A, et al. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. Phys Lett A, 2006, 349: 467—473[DOI]

17 Wang S H, Liu W R, Lu H P, et al. Periodicity of chaotic trajectories of single and coupled maps in realizations of finite computer precisions. Int J Mod Phys B, 2004, 18(17-19): 2617—2622[DOI]

18 Parker A T, Short K M. Reconstructing the keystream from a chaotic encryption scheme. IEEE Trans Circuits Syst I, 2001, 48(5): 104—112

19 Wang K, Pei W J, Zou L H, et al. Security of public key encryption technique based on multiple chaotic systems. Phys Lett A, 2006, 360: 259—262[DOI]

20 Kaneko K, Tsuda I. Complex Systems: Chaos and Beyond. Tokyo: Asakura, 1996

21 Yang W M. On the largest exponent for coupled surjective map lattice with weak diffusive coupling. Chaos Solitons Fractals, 1991, 1: 389—396[DOI]

22 Liu S T, Wu S. Uniformity of spatial physical motion systems and spatial chaos behavior in the sense of Li-Yorke. Int J Bifurcation Chaos Appl Sci Eng, 2006, 16(9): 2697—2703[DOI]

23 Liu S T, Chen G. On spatial lyapunov exponents and spatial chaos. Int J Bifurcation Chaos Appl Sci Eng, 2003, 13(5): 1163—1181[DOI]

24 Liu S T, Wu S. Spacial chaos behavior of molecular orbit. Chaos Solitons Fractals, 2007, 31: 1181—1186[DOI]

25 Liu S T. Nuclear fission and spatial chaos. Chaos Solitons Fractals, 2006, 30: 453—462[DOI]

26 Liu S T, Chen G. Nonlinear feedback-controlled generalized synchronization of spatial chaos. Chaos Solitons Fractals, 2004, 22(4): 35—46[DOI]

27 Liu S T, Chen G. Asymptotic behavior of delay 2-D discrete logistic systems. IEEE Trans Circuits Syst I, 2002, 49(11): 1677—1682[DOI]

28 Chen G, Liu S T. On spatial periodic orbits and spatial chaos. Int J Bifurcation Chaos Appl Sci Eng, 2003, 13(3): 867—876

29 Chen G, Liu S T. On generalized synchronization of spatial chaos. Chaos Solitons Fractals, 2003, 15(2): 311—318[DOI]