DOI 10.1007/s11071-011-9984-7

ORIGINAL PAPER

An image blocks encryption algorithm based on spatiotemporal chaos

Xingyuan Wang · Lin Teng

Received: 13 July 2010 / Accepted: 9 February 2011 / Published online: 17 March 2011

Abstract In this paper, the CML-based spatiotemporal chaos system is used for image blocks encryption, which gets higher security. The basic idea is to divide the image into blocks, and then use the block numbers as the spatial parameter of CML to iterate the chaos system. Each lattice generates a chaos sequence, and the number of chaos sequence values is equal to the pixels number of each block. The chaos sequences and the former block plaintext codecide the substitution and diffusion of each block. Simulation results show that the performance and security of the proposed encryption system can encrypt the image effectively and resist various typical attacks.

Keywords Image blocks encryption · Spatiotemporal chaos system · CML

1 Introduction

With the rapid development of computer network technology, a lot of sensitive information is transmitted over the network; information security becomes more and more important. Image information transmission has increased rapidly and image encryption technology has drawn more attention. Nowadays, image encryption schemes include two processes: substitution and diffusion [1]. The substitution stage permutes all the pixels as a whole, without changing their values. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in a pixel spreads out to as many pixels in the cipher-image as possible. The two processes can achieve a satisfactory level of security.

Image encryption is different from text encryption due to some inherent features such as bulk data capacity and high correlation among pixels. Therefore, traditional cryptographic techniques such as DES, IDES, and RSA are no longer suitable for image encryption. The properties of the chaotic maps such as sensitivity to initial conditions and random-like behavior have attracted the attention to develop image encryption algorithms. In recent years, some chaos-based image encryption algorithms have been developed, but a low-dimensional chaotic orbit will eventually become periodic in computer realizations with a finite precision; the drawback of small key space and weak security in one-dimensional chaotic cryptosystem are obvious. So, high dimensional chaotic systems are more suitable for image encryption.

A spatiotemporal chaos system is a complex chaos system, nonlinear dynamics in both space and time, not only sensitive to the initial conditions, but also sensitive to the boundary conditions. It is regarded

X. Wang · L. Teng (✉)
Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
e-mail: tenglin@mail.dlut.edu.cn

X. Wang
e-mail: wangxy@dlut.edu.cn

as better properties suitable for data protection than one-dimensional chaos systems, such as larger parameter space, better randomness, and more chaotic sequences.

In this paper, we use coupled map lattice (CML) as a spatiotemporal chaos system. Recently, CML-based spatiotemporal chaos system was used in pseudorandom sequence generation [2, 3], stream cipher encryption [4], image encryption [5–7], and hash function construction [8]. Moreover, in spatiotemporal chaos systems, many space units can be used for encryption and decryption in parallel, and that makes highly efficient performance. Therefore, spatiotemporal chaos systems may fully manifest the advantages of chaotic cryptography.

In this paper, an image blocks encryption algorithm based on spatiotemporal chaos is proposed. We divide the image into blocks, and then use the block numbers as the spatial parameter of CML to iterate the chaos system. The number of chaos sequences which each lattice generated is equal to the pixels number of each block. The chaos sequences and the former block plaintext codecide the substitution and diffusion of each block.

The rest of this paper is organized as follows. Section 2 describes the CML system and a block image encryption algorithm. Section 3 presents the experiments results. The security of the scheme is evaluated in Sect. 4. Section 5 concludes the paper.

2 An image blocks encryption algorithm

2.1 Coupled map lattice

A coupled map lattice (CML) is used as a spatiotemporal chaos system here, which is a dynamical system with discrete-time, discrete-space, and continuous states. It consists of nonlinear maps located on the lattice sites, named as local maps. Each local map is coupled with other local maps in terms of certain coupling rules. Because of the intrinsic nonlinear dynamics of each local map and the diffusion due to the spatial coupling among the local maps, a CML can exhibit spatiotemporal chaos. CML was introduced by Kaneko [9]; it can be described as

$$x_{n+1}(i) = (1-\varepsilon) f\big(x_n(i)\big) + \frac{\varepsilon}{2}\Big(f\big(x_n(i-1)\big) + f\big(x_n(i+1)\big)\Big), \qquad (1)$$

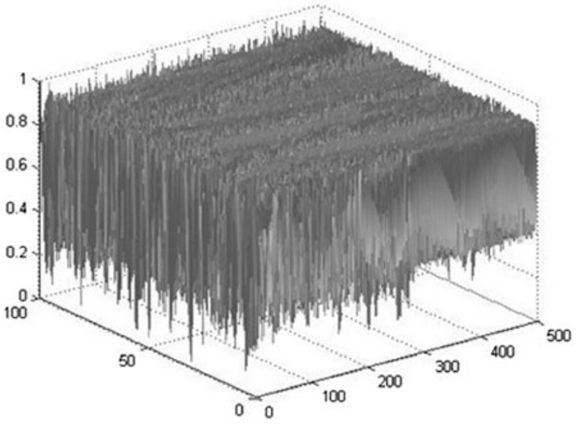


Fig. 1 Chaotic behavior of CML system when $a = 3.9$, $\varepsilon = 0.1$

where n is the time index, i $(i = 1, 2, \ldots, L)$ is the lattice site index, $\varepsilon \in (0, 1)$ is a coupling constant; $x_n(i)$ represents the state variable for the ith site at time n $(n = 1, 2, \ldots)$. The periodic boundary condition $x_n(0) = x_n(L)$ is assumed.

The local mapping function $f(x)$ is chosen to be the logistic map:

$$x_{n+1} = a x_n (1 - x_n), \qquad (2)$$

with parameter $a \in (3.5699456, 4]$, $x_n \in (0, 1)$, the system is in chaotic state.

The chaotic behavior of CML system is demonstrated in Fig. 1.

2.2 Preprocessing of plain-image and chaotic sequence

Without loss of generality, we assume that the size of the plain-image A is $M \times N$, and the pixels' values range from 0 to 255. A is divided into $m \times n$ $(m, n > 5)$ blocks, the size of each block is $M/m \times N/n$ (M, N are divisible by m, n respectively). Each block is represented as matrix $\boldsymbol{P}_i$ $(0 \le i < m \times n)$.

The number of CML lattice L is set to $m \times n$ which is equal to the block number of the divided image. Initialize the system with the parameters a, ε and value sequences $\{x_0(1), x_0(2), \ldots, x_0(m \times n - 1)\}$ to iterate the chaotic system $500 + M/m \times N/n$ times, discard the former 500 values to avoid harmful effect. Each lattice generates $M/m \times N/n$ values, so the chaotic system generates $L \times M/m \times N/n = M \times N$ values totally.

The output sequences of CML $0 \le x_n(i) \le 1$ are transformed into integer sequences $x'_n(i) \in [0, 255]$ as follows:

$$x'_n(i) = x_n(i) \times 10^{14} \mod 256. \tag{3}$$

Then arrange the integer sequence $x'_n(i)$ generated by each lattice i from left to right, from top to bottom to consist a matrix $\boldsymbol{X}_i$ $(0 \le i < m \times n)$ of size $M/m \times N/n$.

2.3 Substitutions of image blocks

The last output value $x_{M\times N}(i)$ of each lattice i and the last pixel value of the $(i-1)$th block are codeciding the substitution of the ith block. Use

$$\theta = \big(x_{M\times N}(i) + \boldsymbol{P}_{i-1}[M/m-1][N/n-1]/256\big) \mod 1$$

as reference, if $\theta > 0.5$, the corresponding block $\boldsymbol{P}_i$ is permuted by row transformation; if $\theta \le 0.5$, the corresponding block $\boldsymbol{P}_i$ is permuted by column transformation. After permuted, the block $\boldsymbol{P}_i$ is changed to $\boldsymbol{P}'_i$.

The row transformation and column transformation are described as follows:

(1) Row transformation: We take out M/m values $\{x_{501}(i), x_{502}(i), \dots, x_{500+M/m}(i)\}$ from the output sequence of the ith lattice, and ordering for this M/m values and getting $\{\bar{x}_{501}(i), \bar{x}_{502}(i), \dots, \bar{x}_{500+M/m}(i)\}$. We find the position of values $\{\bar{x}_{501}(i), \bar{x}_{502}(i), \dots, \bar{x}_{500+M/m}(i)\}$ in $\{x_{501}(i), x_{502}(i), \dots, x_{500+M/m}(i)\}$ and mark down the transform positions $TM = \{t_1, t_2, \dots, t_{M/m}\}$. Then rearrange the row of ith image block according to TM, that is, move the t_1 row of to the first row, t_2 row to the second row.

(2) Column transformation: We take out N/n values $\{x_{501}(i), x_{502}(i), \dots, x_{500+N/n}(i)\}$ from the output sequence of the ith lattice, and order for these N/n values and get $\{\bar{x}_{501}(i), \bar{x}_{502}(i), \dots, \bar{x}_{500+N/n}(i)\}$. We find the position of values $\{\bar{x}_{501}(i), \bar{x}_{502}(i), \dots, \bar{x}_{500+N/n}(i)\}$ in $\{x_{501}(i), x_{502}(i), \dots, x_{500+N/n}(i)\}$ and mark down the transform positions $TN = \{p_1, p_2, \dots, p_{N/n}\}$. Then rearrange the column of ith image block according to TN, that is, move the t_1 column of to the first column, t_2 column to the second column.

2.4 Diffusion of image block

Use the transformed integer matrix $\boldsymbol{X}_i$ to diffuse the permuted block $\boldsymbol{P}'_i$; the corresponding elements of these matrixes are processed. $\boldsymbol{C}_i$ is the ciphered image block matrix. The encryption transformation is

$$\begin{aligned} &\boldsymbol{C}_i = (\boldsymbol{P}'_i + \boldsymbol{X}_i + \boldsymbol{C}_{i-1} + \boldsymbol{P}'_{i-1}) \mod 256, \\ &\boldsymbol{C}_{-1} = 0, \qquad \boldsymbol{P}'_{-1} = 0. \end{aligned} \tag{4}$$

After diffusions, arrange the ciphered image blocks to consist the encrypted image.

The image encryption scheme is shown in Fig. 2.

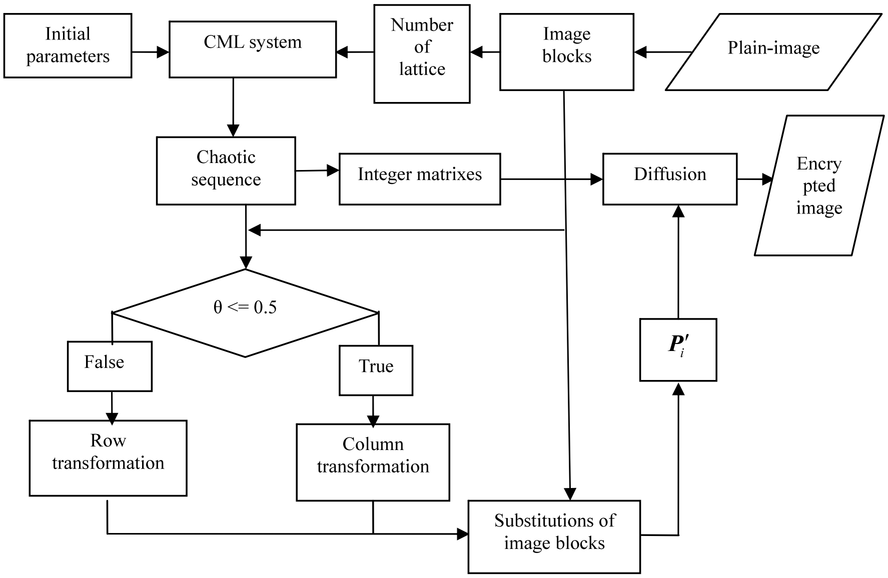
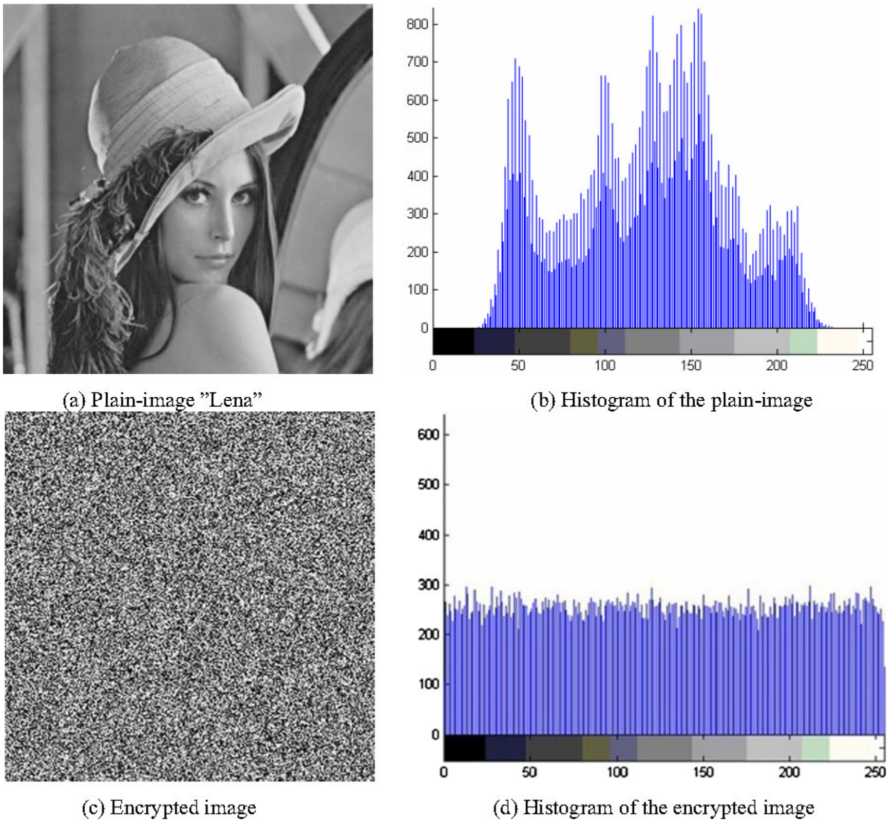


Fig. 2 Block diagram



(a) Plain-image "Lena"

(b) Histogram of the plain-image

(c) Encrypted image

(d) Histogram of the encrypted image

Fig. 3 Image encryption and decryption experimental results

2.5 Image decryption

The decryption procedure is similar to that of the encryption procedure illustrated above.

Divide the encrypted image into blocks as the way which the plain-image is divided, the CML system is processed as the encryption process. The decryption transformation of the block pixels is

$$\begin{aligned} &\boldsymbol{P}'_i = (\boldsymbol{C}_i - \boldsymbol{X}_i - \boldsymbol{C}_{i-1} - \boldsymbol{P}'_{i-1}) \mod 256, \\ &\boldsymbol{C}_{-1} = 0, \qquad \boldsymbol{P}'_{-1} = 0. \end{aligned} \tag{5}$$

Use

$$\begin{aligned} \theta = \bigl(&x_{M\times N}(i) \\ &+ \boldsymbol{P}_{i-1}[M/m-1][N/n-1]/256\bigr) \mod 1 \end{aligned}$$

as reference, if $\theta > 0.5$, $\boldsymbol{P}'_i$ is permuted by reversed row transformation; if $\theta \le 0.5$, $\boldsymbol{P}'_i$ is permuted by reversed column transformation. Then arrange the image blocks to consist of the decrypted image.

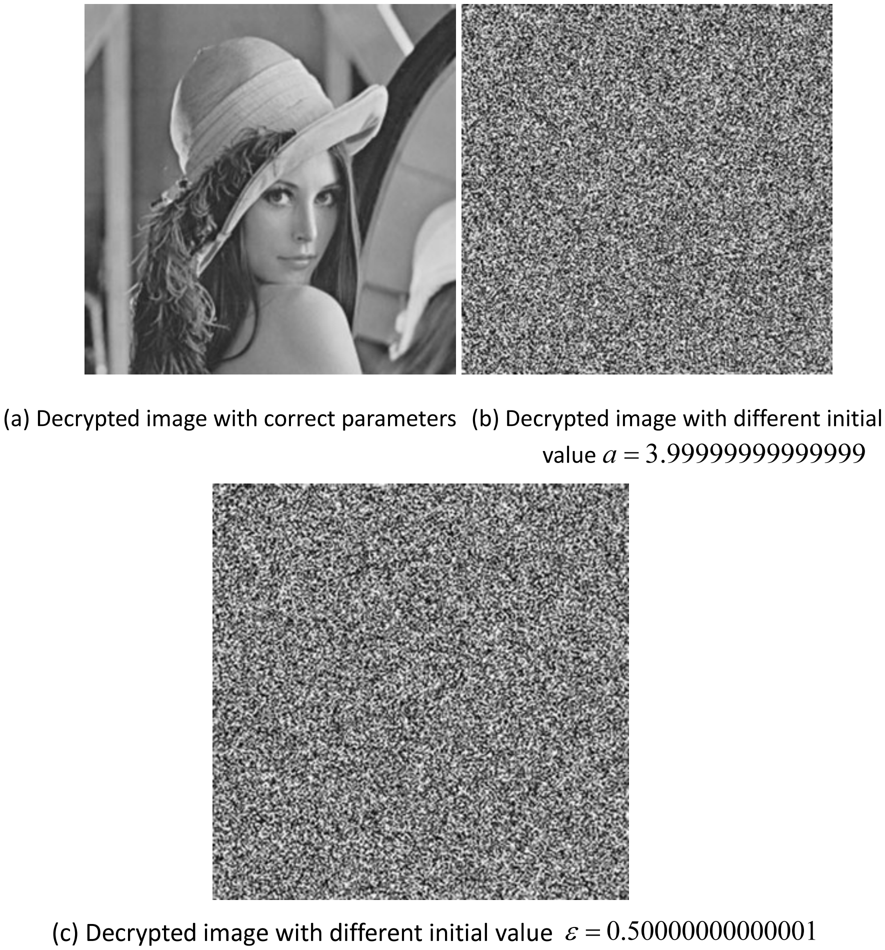
3 Experimental results

The plain-image "Lena" with the size 256 × 256 is shown in Fig. 3(a) and the histogram of the plain-image is shown in Fig. 3(b). We let $m = n = 8$, that is dividing the image into 64 blocks and each block size is 32 × 32. The initial parameters and initial values of CML are $a = 4$, $\varepsilon = 0.5$, $x_0(i) = 0.23456789876543 \times i \mod 1$, $L = m \times n = 64$. The encrypted image is shown in Fig. 3(c), and Fig. 3(d) is the histogram of encrypted image. From the figure, we can see that the histogram of the encrypted image is fairly uniform and is significantly different from that of the original image.

4 Security analysis

In this section, the proposed image encryption scheme is analyzed in detail. We have made several tests to check the security of the cryptosystem. The results show that the scheme have higher security, bigger key space, and can resist various typical attacks, such as

Fig. 4 Key sensitivity analysis



(a) Decrypted image with correct parameters

(b) Decrypted image with different initial value $a = 3.99999999999999$

(c) Decrypted image with different initial value $\varepsilon = 0.50000000000001$

brute-force attack, statistical analysis, differential attack, and chosen-plaintext/ciphertext attack.

4.1 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 values $x_0(i)$ and parameters a, ε as well as the way which plain-image is divided, that is, the block numbers m, n can be used as keys. If the precision is 10^{-14}, the key space size can reach to $10^{14(L+2)}$, where L is the number of initial values $x_0(i)$ and $L > 16$. The key space is large enough to resist the brute-force attacks.

4.2 Key sensitivity analysis

Several key sensitivity tests are performed. Figure 4(a) shows the encrypted image of Lena with the correct encryption key $a = 4, \varepsilon = 0.5$. Figures 4(b) and 4(c) show the encrypted image of Lena with the wrong encryption key $a = 3.99999999999999, \varepsilon = 0.50000000000001$, respectively. So, it can be concluded that the proposed 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 Correlation analysis of two adjacent pixels

It is well known that adjacent image pixels are highly correlated in the plain image. In order to resist statistical attack, we must decrease the correlation of two adjacent pixels in the ciphered image [10]. To test the correction between two adjacent pixels in plain image and ciphered image, the following procedure was carried out. First, randomly select 2,000 pairs of two adjacent pixels from an image. Then calculate the correction coefficient of each pair by using the following formulas:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{6}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\bigl(x_i - E(x)\bigr)^2, \tag{8}$$

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

where x and y are grey-scale values of two adjacent pixel in the image, $E(x)$ is expectation of x, and $D(x)$ the variance. N denotes the total number of samples.

The correlation of two adjacent pixels in plain image Lena is 0.935832, and in ciphered image is 0.012401. It proves that the chaotic encryption algorithm satisfy zero co-correlation.

4.4 Information entropy analysis

Information theory is a mathematical theory of data communication and storage founded by Shannon in 1949 [11]. An important theory in information theory is entropy. The entropy $H(m)$ of a message source m can be calculated as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)}, \tag{10}$$

where $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Actually, given that a real information source seldom transmits random messages, in general, the entropy value of source is smaller than the ideal one. However, when these messages are encrypted, their ideal entropy should be 8. If the output of such a cipher emits symbols with entropy of less than 8, then there would be a possibility of predictability which threatens its security. The value obtained is very close to the theoretical value 8. This means that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack. Using the above mentioned formula, we have obtained the entropy $H(m) = 7.995351$.

4.5 Classical types of attacks

When cryptanalyzing a cryptosystem, the general assumption made is that the cryptanalyst knows exactly the design and working of the cryptosystem under study, he knows everything about the cryptosystem except the secret key. This is an evident requirement in today's secure communications networks, usually referred to as Kerckhoff's principle [12]. There are four classical types of attacks:

(1) Ciphertext only: the opponent possesses a string of ciphertext.
(2) Known plaintext: the opponent possesses a string of plaintext, and the corresponding ciphertext.
(3) Chosen plaintext: the opponent has obtained temporary access to the encryption machinery. Hence, he can choose a plaintext string, and construct the corresponding ciphertext string.
(4) Chosen ciphertext: the opponent has obtained temporary access to the decryption machinery. Hence, he can choose a ciphertext string, and construct the corresponding plaintext string.

Obviously, chosen plaintext attack is the most powerful attack. If a cryptosystem can resist this attack, it can resist other types of attack.

In the proposed cryptosystem, the parameter of chaotic system would be different if the image blocks are divided in the different way. Moreover, encrypted image blocks are not only related to plain-image blocks and the key but also related to the former plain-image blocks, that is, in the substitution stage, θ is related to $\boldsymbol{P}_{i-1}[M/m-1][N/n-1]$; in the diffusion stage, $\boldsymbol{C}_i$ is related to $\boldsymbol{P}'_i$. So, the different plain-image generates totally different θ and $\boldsymbol{C}_i$. So, the proposed cryptosystem can effectively resist the chosen plaintext/ciphertext attack.

5 Conclusions

In this paper, an image blocks encryption algorithm is presented, which is based on the spatiotemporal chaos system. Firstly, we divide the image into blocks, and then use the block numbers as the spatial parameter of CML system to iterative the chaos system. The chaos sequences and the former block plaintext codecide the substitution and diffusion of each plain-image block. Simulation results show that the performance and security of the proposed encryption system can encrypt image effectively and resist various typical attacks. The algorithm is also suitable for color image encryption.

Acknowledgements This research is supported by the National Natural Science Foundation of China (Nos: 60573172, 60973152), the Superior University Doctor Subject Special Scientific Research Foundation of China (No: 20070141014) and the Natural Science Foundation of Liaoning province (No: 20082165).

References

1. Wang, S.H., Kuang, J.Y., Li, J.H., Luo, Y.L., Lu, H.P., Hu, G.: Chaos-based communication in a large community. Phys. Rev. E **66**(6), 1–4 (2002)
2. Li, P., Li, Z., Halang, W.A., Chen, G.: A multiple pseudo-random-bit generator based on a spatiotemporal chaotic map. Phys. Lett. A **349**(6), 467–473 (2006)
3. Sun, F., Liu, S.T.: Cryptographic pseudo-random sequence from the spatial chaotic map. Chaos Solitons Fractals **41**(5), 2216–2219 (2009)
4. Li, P., Li, Z., Halang, W.A., Chen, G.R.: A stream cipher based on a spatiotemporal chaotic system. Chaos Solitons Fractals **32**(5), 1867–1876 (2007)
5. Sun, F.Y., Liu, S.T., Li, Z.Q., Lü, Z.W.: A novel image encryption scheme based on spatial chaos map. Chaos Solitons Fractals **38**(3), 631–640 (2008)
6. Rhouma, R., Meherzi, S., Belghith, S.: OCML-based colour image encryption. Chaos Solitons Fractals **40**(1), 309–318 (2009)
7. Rhouma, R., Belghith, S.: On the security of a spatiotemporal chaotic cryptosystem. Chaos **17**(3), 1–5 (2007)
8. Ren, H.J., Wang, Y., Xie, Q., Yang, H.Q.: A novel method for one-way hash function construction based on spatiotemporal chaos. Chaos Solitons Fractals **42**(4), 2014–2022 (2009)
9. Kaneko, K.: Spatiotemporal intermittency in Coupled Map Lattices. Prog. Theor. Phys. **74**(5), 1033–1044 (1985)
10. Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**(2), 408–419 (2008)
11. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
12. Pareek, N.K., Patidar, V., Sud, K.K.: Cryptography using multiple one-dimensional chaotic maps. Commun. Nonlinear Sci. Numer. Simul. **10**(7), 715–723 (2005)