Sensors & Transducers, Vol. 160, Issue 12, December 2013, pp. 348-352

Sensors & Transducers

http://www.sensorsportal.com

A Novel Diffusion-Permutation Image Encryption Scheme Based on Spatiotemporal Chaos

Gang Xu, Xuna Miao, Yafeng Zheng
College of Computer and Information Engineering, Henan University of Economics and Law, Zheng Zhou, 450002, China
E-mail: xgtony@huel.edu.cn

Received: 30 November 2013 Accepted: 29 December 2013 Published: 30 December 2013

Abstract: The spatiotemporal chaos possesses better properties than simple chaotic system, which has attracted more and more attention by the researchers in the image encryption field. This paper presents a novel image encryption scheme based on spatiotemporal chaos. The algorithm uses the spatiotemporal chaos to diffuse plain image and an Arnold map shuffle the positions of pixels. Test results and security analysis not only show that the scheme is characteristic of excellent sensitivity to the original image and keys, large secret key space and high expansibility, but also has excellent effective encryption and strong anti-attacking performance. *Copyright © 2013 IFSA.*

Keywords: Image encryption, Spatiotemporal chaos, Diffusion, Permutation.

1. Introduction

With the rapid development of the Internet and digital multimedia techniques, image communication becomes more and more important. Images have their intrinsic properties, such as bulk data capacity and strong correlation among pixels, which is different from texts. Some traditional image encryption techniques appear in recently years [1, 2]. The major challenge in designing effective image encryption algorithms is that it is rather difficult to shuffle and diffuse image data efficiently by traditional cryptographic means. Because chaos has the good properties such as high security, low computational complexity and high sensitivity to the initial conditions and system parameters, the chaos based encryption algorithm provides a new way for digital image encryption.

Fridrich suggested that a chaos-based image encryption scheme should compose of the iteration of two processes: substitution and diffusion [3]. The whole substitution-diffusion process repeats for a number of times in order to achieve a satisfactory level of security. Several chaos-based image cryptosystems were designed under this architecture. Guan et al. used a 2D cat map for pixel relocating and the discretized Chen's chaotic system for pixel value masking [4]. Lian et al. [5] used a chaotic standard map in the substitution stage and a quantized logistic map in the diffusion stage. Yang et al. [6] presented a fast image encryption and authentication scheme based on chaotic maps. The hash value played the role of the key for encryption and decryption while the secret hash keys were used to authenticate the decrypted image. Pareek et al. [7] proposed a diffusion-substitution based gray image encryption scheme.

Spatiotemporal chaos is chaotic dynamics in spatially extended system, which has attracted much attention in the image encryption field. The spatiotemporal chaos is often created by local nonlinearity dynamics and spatial diffusion, and modeled by coupled map lattices (*CML*). The coupled map lattices (*CML*) based spatiotemporal chaotic system was proposed for self-synchronizing stream cipher [8-10]. Lian [11] proposed an image or video encryption system based on the spatiotemporal chaos. Wang et al. [12] proposed a block image encryption algorithm based on spatiotemporal chaos. Song et al. [13] introduced a new spatiotemporal map and proposed an image encryption algorithm based on the new chaotic map.

The spatiotemporal chaotic system possesses much better properties than simple chaotic system. First, it is found that the spatiotemporal chaos can solve the problems satisfactorily [14]. Second, the spatiotemporal systems have larger parameter space, more positive Lyapunov exponents, higher randomness and more chaotic sequences, so it is more difficult to predict the chaotic series generated by the spatiotemporal systems. Considering of this, the spatiotemporal chaos is more suitable for data protection. In this paper, we construct a new sequence by iterating two chaotic systems alternately, and then propose a novel image encryption scheme based on the spatiotemporal chaotic map.

The rest of this paper is organized as follows. Section 2 constructs a sequence by iterating spatiotemporal chaotic system. The spatiotemporal chaos based image encryption scheme is presented in Section 3. The experimental results and analysis are described in Section 4. Finally, Section 5 concludes the letter.

2. A Constructed Sequence and the Spatiotemporal Chaotic System

Spatiotemporal chaos is chaotic dynamics in spatially extended system. Comparing with the low-dimensional chaotic system, the spatiotemporal chaos has more complex behavior and more abundant characteristics. Spatiotemporal chaotic systems are often modeled by the coupled map lattices (*CML*). In the paper, *CML* is employed as the model of the spatiotemporal chaotic systems.

2.1. Intertwining Logistic Map

Logistic map is a simple and classic nonlinear model, which is used in many image encryption algorithms. Logistic map is defined below:

$$x_{i+1} = \mu x_i (1 - x_i) \tag{1}$$

where $0 < x < 1$ and $3.599456 < \mu \le 4$. The sequences generated by the logistic map are sensitive to the change of its initial value and the properties including pseudorandom capability and data irrelevance remains well. However, the logistic map has some weakness such as a weak key and relative small key space and uneven distribution of sequences, which can be utilized by the attackers.

For attaining better chaos behavior together so as to achieve a larger key space and overcome defects in logistic map, we adopt a new chaotic map called intertwining logistic map [15] which is defined as following:

$$\begin{cases} x_{i+1} = (u \times k_1 \times y_i \times (1 - x_i) + z_i) \bmod 1 \\ y_{i+1} = (u \times k_2 \times y_i + z_i \times 1/(1 + x_{i+1}^2)) \bmod 1 \\ z_{i+1} = (u \times (x_{i+1} + y_{i+1} + k_3) \times \sin z_i) \bmod 1 \end{cases}, \tag{2}$$

where u, k_i are the parameters and $0 < u \le 3.999$, $|k_1| > 33.5$, $|k_2| > 37.5$, $|k_3| > 35.7$. The distribution of the sequences becomes better and importantly. The intertwining logistic map has a more complicated behavior, a more uniform distribution of sequences than logistic map. The weaknesses logistic map caused are resolved in the meanwhile the key space[15] has increased greatly.

2.2. The Proposed Spatiotemporal Chaotic Map

A *CML* is a dynamical system with discrete time, discrete space and continuous state. It always serves as a prototype model of the spatiotemporal chaos to study the chaotic dynamics. The double-way coupled map lattice system can be defined as

$$x_{n+1}(i) = (1 - \varepsilon) f(x_n(i)) + \frac{\varepsilon}{2}[f(x_n(i+1)) + f(x_n(i-1))] \tag{3}$$

where $i = 1,2,\cdots,L$ is the lattice site index, L is the length of *CML*, $n = 1,2,\cdots$ is the time index, $\varepsilon \in (0,1)$ is a coupling constant, and $x_n(i) \in (0,1)$. The periodic boundary condition is $x_n(0) = x_n(L)$. $f(x)$ is a chaotic map such as the logistic map, tent map and so on.

Taking the advantages of the intertwining logistic map into account, we substitute the $f(x)$ with the intertwining logistic map Eq. (2). The system exhibits chaotic properties both in the time and space domains.

3. The Proposed Image Encryption Scheme

In the paper, we present an image encryption scheme based on two chaotic systems. The constructed spatiotemporal chaotic sequence is adopted to diffuse the image, and the Arnold map is used to permute the positions of the image pixels. An auxiliary key is brought in the algorithm to make the algorithm sensitive to the secret keys.

Without loss of generality, we assume the size of a plain image is *N*×*N*. The main key we selected is $K = \{k_1, k_2, \cdots, k_{32}\}$, where *K* is 256 bit and k_i means the i^{th} byte of *K*. The proposed image encryption scheme is summarized as follows.

Step 1: The image pixels are considered as a sequence $P = p_1, p_2, \cdots, p_i, \cdots, p_r \quad (i = 1,2,\cdots,r)$ in the order from left to right and then from top to bottom, where $P(i,j)$ is the pixel value of plain image. Pack the first 32 pixels in the sequence as the first block, then the next 32 pixels as the next block, and so on. If necessary, we use zero to fill in the block. Finally, a set of blocks is obtained.

Step 2: Set the chaotic maps initial value and the parameters. To achieve good chaotic behavior, We choose the chaotic system's parameters of Eq. (2) as $x_0 = y_0 = z_0 = 0.565437$, $\mu = 3.815637$ and $k_1 = k_2 = k_3 = 38.5$.

Step 3: Construct an auxiliary key $\delta \in (0,1)$ as follows

$$\delta = \frac{1}{256}[(\sum_{i=1}^{N}\sum_{j=1}^{N} P(i,j) + \sum_{i=1}^{32} k_i) \bmod 256], \quad i, j \in [1, N] \tag{4}$$

In our algorithm, the auxiliary key is used to regulate the initial value of chaotic system and parameters. We respectively multiply x_0, y_0, z_0 and μ by δ to achieve new initial value and the parameters, which can be denoted by x_0', y_0', z_0' and μ'.

Step 4: Iterate Eq. (2) with the initial value x_0', y_0', z_0', μ' for 1000+*D* times. The iterations *D* is sensitive to the main key, which can be defined as follows

$$D = (\sum_{i=1}^{32} k_i) \bmod 256$$

The iterations 1000+*D* are used to avoid the harmful effect of the transition procedure, and form a new sequence. A chaotic sequence is generated according to Eq. (2) by using this method.

Step 5: Let $L = r$. By utilizing the sequence obtained in Step 4, every *CML* model can generate a chaotic sequence. Take out the last 32 state values from the sequence to encrypt the plain image block. Denote the j th of 32 state value as $\{z_1^j, z_2^j, \cdots, z_{32}^j\}$, where $j = 1,2,\cdots,L$. The number of times to evolution the Eq.(3) is $N_1 = 1000 + D$.

Step 6: Translate the state value into decimal number by

$$\overline{P}_t^j = \left\lfloor \left| z_t^j \right| \times 256 \right\rfloor,$$

where $t = 1,2,\cdots,32$. Then put the 32 decimal number in order $\{\overline{P}_1^j, \overline{P}_2^j, \cdots, \overline{P_{32}}^j\}$ and convert them to binary representation $\overline{\overline{P}}^j$. A sequence of 256 bits is formed. The encryption algorithm can be described as follow

$$C_j = \overline{\overline{P}}^j \oplus P_j .$$

Step 7: Encrypt the *r* blocks respectively and obtain the encrypted message $\{C_1, C_2, \cdots, C_r\}$. The encrypted message are transformed to matrix *C* using the function reshape( ) in MATLAB.

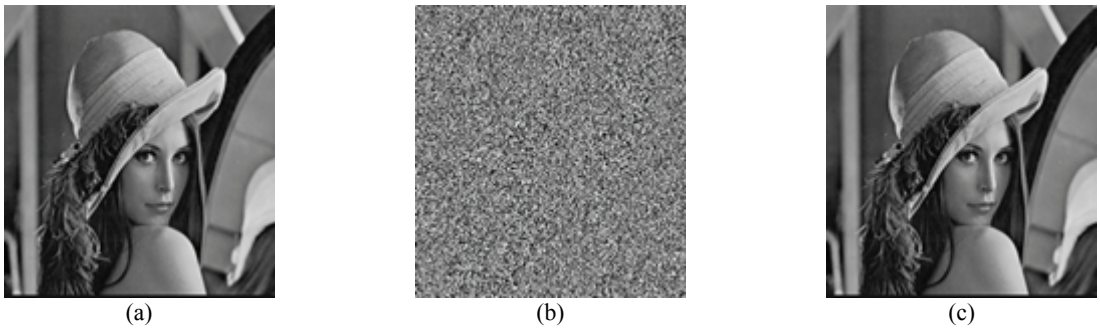
Step 8: Change the position of the matrix *C* by the means of chaotic Arnold map, which can be defined as

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod N \tag{5}$$

Consider the pixel coordinates (i, j) as the initial value (x_0, y_0) in Eq. (5). After iteration of Arnold map, a new pixel coordinates (x_1, y_1) is generated. So we switch the two positions.

Step 9: After the diffusion and permutation, output the cipher image *C'*.

The decryption process is the inverse process of the encryption.



(a) (b) (c)

Fig. 1 Experimental results: (a) plain image, (b) cipher image and (c) decrypted image.

4. Performance and Security Analysis

The image for testing is the standard 256×256 Lena image with 8-bit gray-scale, which is shown in Fig. 1(a). The key set is {*K*, x_0, y_0, z_0, μ, δ, *D*}. The main key is selected as follows: *K*='schemebasedonspatiotemporalchaos'. The cipher image is shown in Fig. 1(b). Fig. 1(c) is the decrypted image. It can be seen that the image is perfectly decrypted without any distortion.

4.1. Key Space Analysis

The key space of any encryption algorithms should be sufficiently large to make brute-force search infeasible. In our proposed scheme the key lies in both confusion and diffusion stage. The keys consist of the following: (1) the initial values of chaotic maps, (2) the main key and (3) the auxiliary key and iteration rounds.

Because the inherent high sensitivity to initial values and parameters, the chaotic map's precision is

considered as 10-16. So the key space is calculated as $2^{256} \times 255^2 \times 10^{61} \approx 10^{142}$, which is large enough to make the brute-force attack infeasible.

4.2. Key Sensitivity Test

A good cryptosystem should be sensitive to its key in order to guarantee the brute-force attack. A slight change of a pixel of the plain image and key can cause great change in the cipher image. We encrypt the plain-image with the slightly changed key $x_0 = 0.565437000000001$, the cipher image is shown in Fig. 2(a), and the differential image between Fig. 2(a) and the original cipher image Fig. 1(b) is shown in Fig. 2(b). The difference between two cipher images is 99.59%. Then we change the pixel $P(11,4)$ of the plain image Lena from 128 to 127. The differential image is shown in Fig. 2(c). Therefore the method is of high key sensitivity.

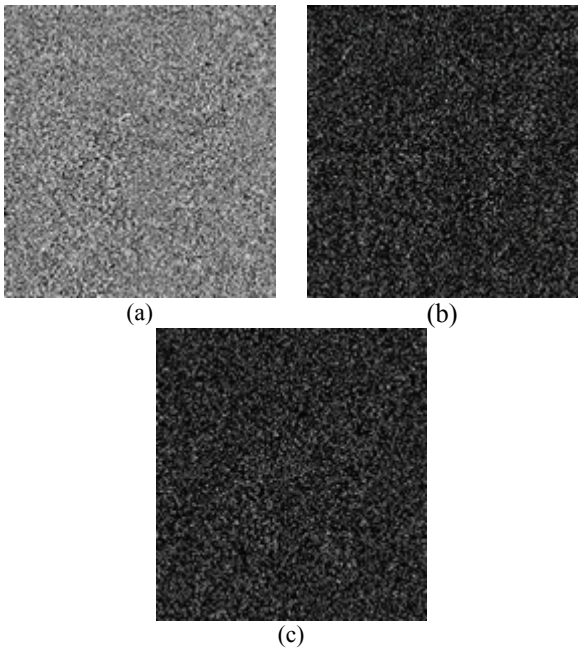


Fig. 2. Key sensitivity analysis: (a) cipher image (x_0=0.565437000000001) (b) and (c) differential image.

4.3. Information Entropy Analysis

Information entropy is thought to be one of the most important features of randomness. Information entropy $H(M)$ is calculated by the following formula:

$$H(M) = -\sum_{i=0}^{2^N-1} p(m_i) \log_2(p(m_i))$$

where M is the message. $p(m_i)$ represents the probability of symbol mi and N is the number of bits to represent symbol. The ideal entropy for a random image with 256 gray levels is 8. The entropy of the cipher image is 7.9967, which is very close to the ideal value. So the scheme is secure enough to resist the entropy attack.

4.4. Differential Attack

Differential attack would become ineffective if a tiny change in the plain image causes a significant difference in the cipher image. To measure this capability quantitatively, the following measures are usually used: number of pixels change rate (*NPCR*) and unified average changing intensity (*UACI*).

NPCR is used to measure the number of different pixels in two images and defined as follows:

$$\gamma_{\mathrm{NPCR}} = \frac{\sum_i \sum_j Q(i,j)}{N \times N} \times 100\%,$$

where N is the width and length of the image, respectively. Let $C_1(i, j)$ and $C_2(i, j)$ be the i[th] row and j[th] column pixels of two cipher images C_1 and C_2, respectively. $Q(i, j)$ is determined as follows:

$$Q(i,j) = \begin{cases} 1 & C_1(i,j) \neq C_2(i,j), \\ 0 & C_1(i,j) = C_2(i,j). \end{cases}$$

UACI is defined as

$$\gamma_{\mathrm{UACI}} = \frac{1}{N \times N}\left[\sum_i \sum_j \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%,$$

which measures the change rate of the pixels between C_1 and C_2. For two completely random images, the theoretical value of *NPCR* and *UACI*[16] are 99.60937% and 33.46354%, respectively. The *NPCR* and *UACI* calculated in our proposed scheme are γ_{NPCR} = 99.6192% and γ_{UACI} = 33.4723%, which are very close to the theoretical value. The result demonstrates the algorithm is very sensitive to the plaintext.

4.5. Statistical Analysis

According to Shannon's theory, a secure cryptographic scheme should be strong enough to resist statistical attack. To frustrate the powerful attacks based on statistical analysis, he suggested that diffusion and confusion should be employed in the cryptosystem.

As to image encryption, histogram of the cipher images and the correlations of adjacent pixels in the cipher image are the two primary measurements to statistical property. Therefore, we will demonstrate that our cipher image has good statistical properties through proposed confusion and diffusion stage.

1) Histograms of the plain-image and the cipher-image.

Histograms of the plain-image and the cipher-image are shown in Fig. 3. The latter histogram is fairly uniform and does not reveal any statistical information of the former.

2) Correlation of two adjacent pixels.

To test the correlation of pixels (vertical, horizontal, diagonal), we randomly select 4000 pairs of adjacent pixels both from plain image and cipher image, and calculate the correlation coefficients of pixels according the following formula:

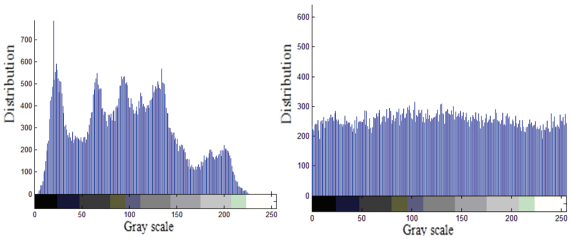
$$\mathrm{cov}(X,Y) = E(X - E(X))(Y - E(Y)),$$

$$r_{xy} = \frac{\mathrm{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}},$$

$$E(X) = \frac{1}{L}\sum_i X_i \,,\; D(X) = \frac{1}{L}\sum_i (X_i - E(X))^2 \,,$$

$$\mathrm{cov}(X,Y) = \frac{1}{L}\sum_i (X_i - E(X))(Y_i - E(Y)),$$

where X and Y are gray-scale values of two adjacent pixels in the image.



(a) (b)

Fig. 3. Histogram analysis: (a) histogram of the plain image and (b) histogram of the cipher image.

The measured correlation coefficients of the plain-image are close to 1 while those of the cipher-image are nearly 0 in Table 1. This indicates that the proposed scheme has successfully removed the correlation of adjacent pixels in the plain-image so that neighbor pixels in the cipher-image virtually have no correlation.

Table 1. Correlation coefficients of two adjacent pixels in the image.

	Vertical	Horizontal	Diagonal
Plain-image	0.986648	0.980657	0.964588
Cipher-image	-0.015168	-0.002497	0.017656

5. Conclusions

This paper introduces a novel image encryption scheme based on the spatiotemporal chaotic system. Experimental results and security analysis show that our scheme has perfect information protection ability, and satisfied the confusion and diffusion request in cryptosystem. Simulation experiments prove that the algorithm is more suitable for image encryption for potential applications in other multimedia data.

Acknowledgements

This work was supported by the National Natural Science Foundations of China (Grant Nos. 61170037, 61374079, 61309033, 11202068) and the Science and Technology Department of Henan Province Foundation (Grant No. 132300410438).

References

[1]. Pareek, Narendra K., Vinod Patidar, and Krishan K. Sud, Diffusion-substitution based gray image encryption scheme, *Digital Signal Processing,* 23, 3, 2013, pp. 894–901.

[2]. Chen W, Chen X., Space-based optical image encryption, *Optics Express,* 18, 26, 2010, pp. 27095-27104.

[3]. Fridrich J., Symmetric ciphers based on two-dimensional chaotic maps, *International Journal of Bifurcation and Chaos,* 8, 06, 1998, pp. 1259-1284.

[4]. Guan Z. H., Huang F., Guan W., Chaos-based image encryption algorithm, *Physics Letters A,* 346, 1, 2005, pp. 153-157.

[5]. Lian S, Sun J, Wang Z., A block cipher based on a suitable use of the chaotic standard map, *Chaos, Solitons & Fractals,* 26, 1, 2005, pp. 117-129.

[6]. Yang H, Wong K. W., Liao X., et al., A fast image encryption and authentication scheme based on chaotic maps, *Communications in Nonlinear Science and Numerical Simulation,* 15, 11, 2010, pp. 3507-3517.

[7]. N. K. Pareek, V. K. Patidar, K. Sud, Diffusion-substitution based gray image encryption scheme, *Digital Signal Processing,* 23, 3, 2013, pp. 894-901.

[8]. Pareek N. K., Patidar V., Sud K. K., Image encryption using chaotic logistic map, *Image and Vision Computing,* 2006, 24, 9, pp. 926-934.

[9]. Li C, Li S, Chen G, et al., Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, *Image and Vision Computing,* 27, 8, 2009, pp. 1035-1039.

[10]. Rhouma R., Solak E., Belghith S., Cryptanalysis of a new substitution–diffusion based image cipher, *Communications in Nonlinear Science and Numerical Simulation,* 15, 7, 2010, pp. 1887-1892.

[11]. Lian S., Efficient image or video encryption based on spatiotemporal chaos system, *Chaos, Solitons & Fractals,* 40, 5, 2009, pp. 2509-2519.

[12]. Wang X., Teng L., An image blocks encryption algorithm based on spatiotemporal chaos, *Nonlinear Dynamics,* 67, 1, 2012, pp. 365-371.

[13]. C. Song, Y. Qiao, X. Zhang, An image encryption scheme based on new spatiotemporal chaos, *Optik - International Journal for Light and Electron Optics,* 124, 18, 2013, pp. 3329-3334.

[14]. Wang Y, Wong K W, Liao X, et al., A new chaos-based fast image encryption algorithm, *Applied Soft computing,* 11, 1, 2011, pp. 514-522.

[15]. Wang X, Luan D., A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata, *Communications in Nonlinear Science and Numerical Simulation,* 18, 11, 2013, pp. 3075-3085.

[16]. Kwok H. S., Tang W. K. S., A fast image encryption system based on chaotic maps with finite precision representation, *Chaos Solitons & Fractals,* 32, 4, 2007, pp. 1518-1529.