Commun Nonlinear Sci Numer Simulat 20 (2015) 506–515

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

A novel image encryption algorithm based on chaos maps with Markov properties

Liu Quan [a,b,*], Li Pei-yue [a], Zhang Ming-chao [a], Sui Yong-xin [a], Yang Huai-jiang [a]

[a] State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China
[b] University of Chinese Academy of Sciences, Beijing 100039,China

ARTICLE INFO

Article history:
Received 2 September 2013
Received in revised form 17 April 2014
Accepted 1 June 2014
Available online 16 June 2014

Keywords:
Chaos
Markov
Complexity
Cipher

ABSTRACT

In order to construct high complexity, secure and low cost image encryption algorithm, a class of chaos with Markov properties was researched and such algorithm was also proposed. The kind of chaos has higher complexity than the Logistic map and Tent map, which keeps the uniformity and low autocorrelation. An improved couple map lattice based on the chaos with Markov properties is also employed to cover the phase space of the chaos and enlarge the key space, which has better performance than the original one. A novel image encryption algorithm is constructed on the new couple map lattice, which is used as a key stream generator. A true random number is used to disturb the key which can dynamically change the permutation matrix and the key stream. From the experiments, it is known that the key stream can pass SP800-22 test. The novel image encryption can resist CPA and CCA attack and differential attack. The algorithm is sensitive to the initial key and can change the distribution the pixel values of the image. The correlation of the adjacent pixels can also be eliminated. When compared with the algorithm based on Logistic map, it has higher complexity and better uniformity, which is nearer to the true random number. It is also efficient to realize which showed its value in common use.

1. Introduction

In recent years, more and more images are transmitted and stored on the internet. The confidentiality of the information becomes a prominent problem. While, the encryption algorithm make only the authorized users can access the image, which is considered a good solution to the problem. As the traditional encryption algorithms (DES, AES, IDEA and so on) were designed based on text-structure data, they were thought inappropriate applied on image encryption [1,2]. The traditional algorithms have an obvious drawback that the code image is still perceived after encryption. The main reason is that the image data has a special structure that the adjacent pixels have a strong correlation, which is different from text data.

To solve this problem, the chaotic encryption algorithm is attracting more and more attention [3–8]. According to the classification of chaotic systems, the chaotic encryption schemes, which have being proposed, can be divided into analog chaotic cryptosystems utilizing continuous dynamical systems [6,19] and digital chaotic cryptosystems utilizing discrete dynamical systems[3–5,7,8]. In 1998, Baptista [3] proposed a chaotic block cipher based on a lookup table which seemed simply and efficiency attracts many attentions. As the cipher-text may become longer than the plain-text and would not

* Corresponding author at: State Key Laboratory of Applied Optics, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China. Tel.: +86 13654373620.
E-mail address: lovefirespread@gmail.com (Q. Liu).

http://dx.doi.org/10.1016/j.cnsns.2014.06.005
1007-5704/

distribute uniformly, the algorithm is not widely used. At the same time, Fridrich proposed an image encryption algorithm structure model [4]. He divided the entire algorithm into two stages: permutation and diffusion. The permutation stage is used to rearrange the positions of pixels in the image. It will change the image structure and weaken the correlation of adjacent pixels. The diffusion stage is used to replace the image pixel values with random values so that the distribution of the cipher-text will not depend on the plain-text. The designs of image encryption algorithms almost always followed this model nowadays [4–8]. However, the proposed algorithm is broken [9] by Ercan Solak et al in 2010. The main drawback of Fridrich's algorithm is the diffusion function may be too simple to break. The image encryption algorithms similar to Fridrich's may have the same problem. The weaknesses of the existing chaotic image encryption algorithms are summarized as follows: poor statistical properties of chaotic maps, weak resistance to the CCA attack and CPA attacks, not sensitive enough to the plaintext and the keys, small key space, poor diffusion function and so on.

In this paper, a novel class of chaotic maps with Markov properties is proposed. It can be proved that the map generates a uniformly distributed sequence whose autocorrelation function is δ-like. It has no fixed point which can weaken the weak-key's affect. Through the selection of the parameters, it can avoid finite precision degradation problem similar to Tent map. By compared with Logistic map and Tent map on the complexity analysis, it shows that the sequence is closer to true random number [10]. In order to enlarge the key space, an improved coupled map lattice is proposed, which has better statistical properties. Finally, the diffusion function is redesigned to resist the CCA and CPA attacks.

This paper is organized as follows: firstly, a novel chaos is proposed and its properties are analyzed in Section 2. Then, the image encryption algorithm is described in Section 3. Thirdly, the system is tested in Section 4. Finally, the conclusion is drawn.

2. The chaotic system and its properties

2.1. A novel class of chaotic map with Markov properties

The chaotic map used in the paper is described as formula (1).

$$T(x,p,\sigma)=\begin{cases}\sigma x+\frac{(i+1)-i\sigma}{p} mod 1, x\in[\frac{i}{p},\frac{i+1}{p}), & i=0,1,\ldots,p-2\\ \sigma x+\frac{p-(p-1)\sigma}{p} mod 1, & x\in\left[\frac{p-1}{p},1\right]\end{cases} \tag{1}$$

The parameter $p(p \geqslant 7)$ is a prime number and $\sigma(2 \leqslant \sigma \leqslant p-1)$ is a positive integer. The x-domain is divided into p parts uniformly (denoted as $I_1, I_2, I_3, \ldots, I_p$) while each part can goes into the other parts after one step iteration which can construct a certain graph. When the parameter changed, the transition modes of the system states would change as shown in Fig. 1.

The chaotic system proposed above have some useful properties [11] as shown in the following four theorems.

Theorem 1. *$T(x,p,\sigma)$ is sensitive to the initial value x.*

Proof. Let L(x, f) denote the Lyapunov exponent of $T(x,p,\sigma)$. The set A denote the first class of break points of the map,

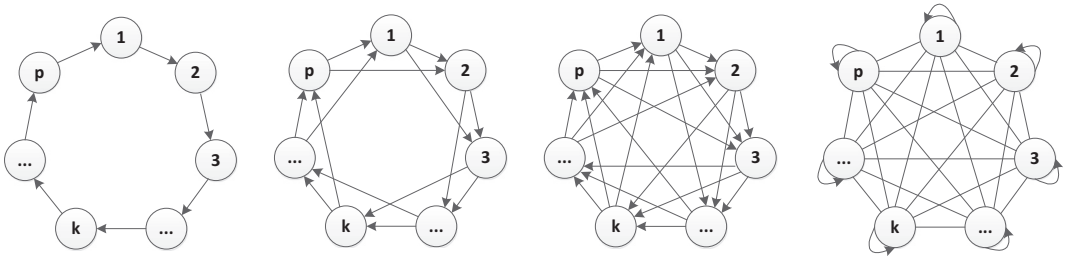
$$A=\{x:\lim_{x\to x^-}T(x,p,\sigma)\neq\lim_{x\to x^+}T(x,p,\sigma),\ \text{the left and right limit of T}(x,p,\sigma)\ \text{on x exists}\},$$

If $x \notin A$, then $|T'(x)| = \sigma$.

So that if $x^j = f^j(x_0) \notin A$, then $L(x,f) = \ln(\sigma) \geqslant \ln(2) > 0$. The map has a positive Lyapunov exponent, which means it is sensitive to the initial value of x. □

Theorem 2. *$I_1, I_2, I_3, \ldots, I_p$ is a Markov portion of $T(x,p,\sigma)$.*

Proof. According to the formula (1), $I_1, I_2, I_3, \ldots, I_p$ is a portion of the x-domain.



(a) $\sigma = 1$ (b) $\sigma = 2$ (c) $\sigma = 3$ (d) $\sigma = p$

Fig. 1. System states transition models with different parameters.

For each i, $\overline{f(I_i)} = \bigcup_{j=1}^{\sigma} I_{i+j}, i = 1, \ldots, p$, while $I_{i+j} = I_{(i+j) mod \sigma}$ and if $(i+j) mod \sigma = 0$, then $I_{i+j} = I_p$.

For each i and j, $\overline{f(I_j)} I_i$, if $f(int(I_j)) \cap^{int} (I_i) \neq \emptyset$.

This means that each interval will goes into the finite p-intervals after iteration once. Then the transform of the states could generate a Markov chain. According to reference [12], $I_1, I_2, I_3, \ldots, I_p$ will be a Markov portion of $T(x, p, \sigma)$. □

Theorem 3. *The period of $T(x, p, \sigma)$ is no shorter than $[p/\sigma] + 1$.*

Proof. Let the symbol $\{s_1, s_2, s_3, \ldots, s_p\}$ denote the Markov portion intervals. If a trajectory goes through the intervals $I_{a_1}, I_{a_2}, I_{a_3}, \ldots, I_{a_l}$ where $I_{a_k} \in \{I_j : j = 1, \ldots, p\}, k = 1, \ldots, l$, the corresponding symbol sequence can be denote as $s_{a_1}, s_{a_2}, s_{a_3}, \ldots, s_{a_l}$. If a trajectory was periodic, the symbol sequence would be periodic. The period of the trajectory would be no longer than the least period of the symbol sequence. Take the state 1 as an example: The shortest way to go back to state 1 is $\{s_1, s_{1+\sigma}, s_{1+2\sigma}, \ldots, s_{1+t\sigma}, s_1\}$ where $t = \left[\frac{p}{\sigma}\right]$, as shown in Fig. 1.

If $2 \leqslant \sigma \leqslant p - 1$ the least period of the chaos would be no shorter 2, which means that the chaotic maps have no fixed points. □

Theorem 4. *The limit invariant distribution of $T(x, p, \sigma)$ is uniform.*

Proof. According to Lasota–Yorke's theory [12–14], calculating the limit invariant distribution of $T(x, p, \sigma)$ requires to know the transition matrix firstly. As the chaotic map has Markov properties, the transition of the portions construct Markov chain. The transition matrix $M = (a_{ij})_{p,p}$ is shown in formula (2) which is satisfying $\sum_{j=1}^{p} a_{ij} = 1$.

$$M = \begin{bmatrix} 0 & 1/\sigma & 1/\sigma & 0 & \cdots & 0 \\ 0 & 0 & 1/\sigma & 1/\sigma & \ddots & 0 \\ \cdots & \cdots & \ddots & \ddots & \cdots & \cdots \\ 0 & 0 & \ddots & \ddots & 1/\sigma & 1/\sigma \\ 1/\sigma & 0 & \ddots & \ddots & \ddots & 1/\sigma \\ 1/\sigma & 1/\sigma & 0 & \cdots & \cdots & 0 \end{bmatrix}_{p \times p} \tag{2}$$

The limit distribution of the map is the standardized eigenvector of the matrix corresponding to the eigenvalue 1, which is $V_p = \left(\frac{1}{p}, \frac{1}{p}, \ldots, \frac{1}{p}\right)$. The density function of the map is formula (3), which means the distribution of the chaotic map is uniform.

$$\rho(x) = \chi_{[0,1]}(x) = \begin{cases} 0, & x \in R \setminus [0, 1] \\ 1, & x \in [0, 1] \end{cases} \tag{3}$$

□

2.2. An improved couple map lattice

Generally, the key space of the low-dimensional chaotic system is small and the phase space structure is simple which could lead to security vulnerabilities. The article [15] proposed a chaotic system named couple map lattice which can solve this problem. The stability of the couple map lattice is analyzed in [16]. A K-order couple map lattice can be described in the formula (4), which can be used to cover the phase space system structure and enlarge the key space.

$$\begin{cases} y_{n+1}(1) = (1 - \varepsilon) f(y_n(1)) + \varepsilon g_n \\ y_{n+1}(i) = (1 - \varepsilon) f(y_n(i)) + \varepsilon f(y_n(i + 1)) \\ g_n = f(y_n(2)), \quad i = 2, \ldots, K \ (n = 0, 1, 2, \ldots) \end{cases} \tag{4}$$

The boundary condition satisfies $y_n(K + 1) = y_n(1)$. When iterated n-times, the state of the ith node is denoted as $y_n(i)$. The parameter $\varepsilon (0 \leqslant \varepsilon \leqslant 1)$ denotes the weight of the certain node and K denotes the number of the nodes. The initial states of the K-nodes represent as $(y_0(1), \ldots, y_0(K))$ which can be used as the key of the chaotic system. The output sequence is denoted as g_n used as key stream in the cryptosystem. The base function $f(x)$ is a Logistic map originally, which is replaced by $T(x, p, \sigma)$ here.

3. The proposed image encryption algorithm

3.1. Algorithm framework

The encryption algorithm proposed in the paper still follows Fridrich's structure as shown in Fig 2. It can be divided into two phases: permutation and diffusion. The two phases both require the key stream generated by the chaotic system. The

chaotic system composed of two parts: couple map lattice and our chaotic map. The keys of the system include the initial states of the map and the system parameter. A true Random number is used to manage the keys, which makes the keys different when used every time. The proposed algorithm has three parts: the key stream generation algorithm, encryption algorithm and decryption algorithms.

3.2. Key stream generation algorithm

The key stream generation algorithm has four steps.

Step 1: The parameters p and σ of the chaotic system $T(x, p, \sigma)$ are selected. The order of the coupled map lattice and the weight of the trajectory are initialized.

Step 2: The initial values $(X_1, X_2, \ldots, X_K)$ of the couple map lattice are assigned by the keys $(\overline{X_1}, \overline{X_2}, \ldots, \overline{X_K})$ and the true random number RND (uniformly distributed in [0,1]), which satisfying $X_i = \overline{\overline{X_i} + RND}(\mathrm{i} = 1, 2, \ldots, \mathrm{K})$. The true random number RND can be generated in many ways, which makes the encryption algorithm have a one-time pad effect.

Step 3: The key stream $(k_1, k_2, \ldots, k_m, \ldots)$ can be generated by iterating the chaotic maps several times, which can be used to generate the permutation matrix and the key of the diffusion function. The permutation matrix is used to permutated the rows and the columns of the plain-text images as shown in Fig 3. It can be got by the column vector $(p_1, p_2, \ldots, p_M)$ used to permutated the column and the row vector $(q_1, q_2, \ldots, q_N)$ used to permutated the row. The vector $(p_1, p_2, \ldots, p_M)$ is generated from the order of the M-different values $(k_1, k_2, \ldots, k_M)$ of the sequence $(k_1, k_2, \ldots, k_m, \ldots)$. For example, if the sequence $(0.25, 0.82, 0.67, 0.32, 0.49)$ is the key stream, $M = 5$, the column vector would be $(1, 5, 4, 2, 3)$, which means change the column $(1, 2, 3, 4, 5)$ of the image into the column $(1, 5, 4, 2, 3)$. The row vector is got by the same way.

Step 4: The key stream $(k_1, k_2, \ldots, k_m, \ldots)$ requires to be quantified into Byte stream $(k_1, k_2, \ldots, k_m, \ldots)$ by $K_n = [k_n \times 256] \mathrm{mod} 256$, where [x] means the greatest integer $\leqslant$ x.

3.3. Image encryption algorithm

Step 1: The original plain image is denoted as $\mathrm{I} = (I_{ij})_{M\times N}$, while the permutation image and the code image are denoted as $\mathrm{P} = (\mathrm{p}_{ij})_{M\times N} = P^{rc}(I)$ and $\mathrm{D} = (\mathrm{D}_{ij})_{M\times N} = D^{Encrypt}(I)$. The permutation image P is transfer into data stream denote as $(m_1, m_2, \ldots, m_t, \ldots, m_s)$, where $m_t = \mathrm{p}_{ij}, t = (i-1) * M + j, 1 \leqslant t \leqslant s$

Step 2: The code image can be got by the following two rounds as shown in formula (5). $(D_1, D_2, \ldots, D_t, \ldots, D_s)$ is the code data stream while $(C_1, C_2, \ldots, C_t, \ldots, C_s)$ is the temporary data stream. The parameter C_0 of the encryption algorithm is used as key. The code stream is transferred into code image after the two rounds encryption, while $\oplus$ defined as exclusive or and $\overline{(A+B)} \triangleq (A+B) mod 1$.

$$Round1: \begin{cases} C_1 = \overline{(m_1 + K_2)} \oplus \overline{(C_0 + K_1)} \\ C_2 = \overline{(m_2 + K_3)} \oplus \overline{(C_1 + K_2)} \\ \ldots \\ C_s = \overline{(m_s + K_{s+1})} \oplus \overline{(C_{s-1} + K_s)} \end{cases} \tag{5}$$

$$\mathrm{Round2}: \begin{cases} D_1 = \overline{(C_1 + K_2)} \oplus \overline{(C_s + K_1)} \\ D_2 = \overline{(C_2 + K_3)} \oplus \overline{(D_1 + K_2)} \\ \ldots \\ D_s = \overline{(C_s + K_{s+1})} \oplus \overline{(D_{s-1} + K_s)} \end{cases}$$

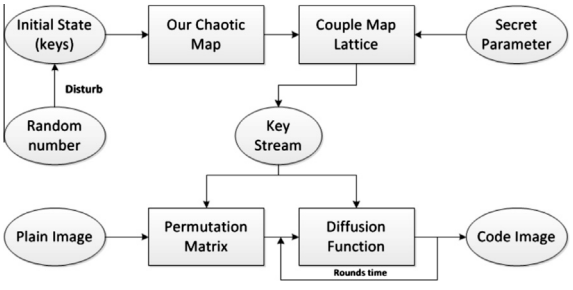


Fig. 2. Framework of the image encryption algorithm.

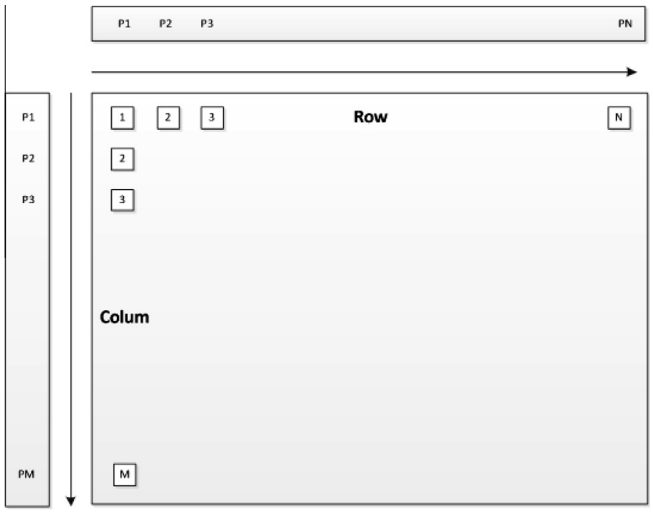


Fig. 3. The permutation matrix.

3.4. Decryption algorithm

The image encryption algorithm is a symmetric algorithm which means the decryption key is the same with the encryption key including the true random number RND. The decryption algorithm is the inverse operation of encryption. The temporary image $(C_1, C_2, \ldots, C_s)$ can be got from $(D_1, D_2, \ldots, D_s)$ first. Then, the image stream $(m_1, m_2, \ldots, m_s)$ could be calculated. Finally, the plain image can be got by the inverse permutation matrix.

4. Security test

The key of the algorithm is composed of four parts: the chaotic system parameters, coupled map lattice parameters, encryption system startup parameter and true random number. The size of the key space can be adjust by the order of the couple map lattice which means the size can be as large as you want.

In this paper, the keys are defined as follows: $\mathrm{p} = 29, \sigma = 28, \mathrm{K} = 6, \varepsilon = 0.99, \mathrm{RND} = 0.01/6, \mathrm{C} = 29$ and the initial value $(0.9/6, 1.9/6, 2.9/6, 3.9/6, 4.9/6, 5.9/6)$ which is used to test the performance of the algorithm. The plain image is chosen 8bit Lena (size of $256 * 256$).

4.1. The statistical properties of the chaos system

As known from Theorem 4, the map $T(x, p, \sigma)$ is uniformly distributed. The cumulating distribution function of the map $T(x, 29, 28)$ is test as an example as shown in Fig. 4(a), which is uniform like. The autocorrelation coefficients of the map are δ like as shown in Fig. 4(b), which means the sequence is ideal random like. The complexity of Tent map, Logistic map and ours are compared through symbol entropy as shown in Fig. 4(c). The complexity of our map is higher than the other two, which can achieve as high as 3.3288.

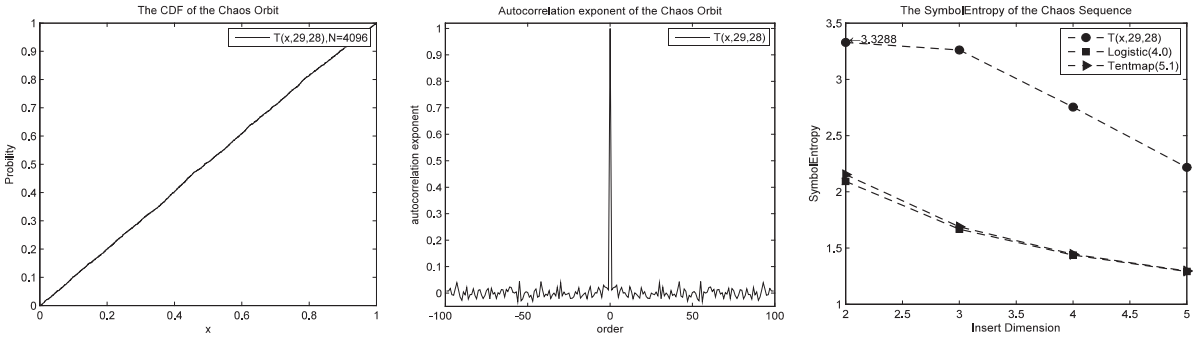
The statistical properties of the improved couple map lattice are also tested as shown in Fig. 5. The phase space of the original couple map lattice (OCML) is distributed random-like but not uniform as shown in Fig. 5(a), which is thicker in edge than the center. While, the improved couple map lattice (ICML) is uniformly random like as shown in Fig 5(b). The phase space test shows that the original chaos and its improved version would not quickly come into the regular patterns, but the improved one has better distribution from the viewpoint of cryptography. The uniform properties of the system are also confirmed through their cumulative distribution functions as shown in Fig. 5(c) and (d).

4.2. Random Test with sp800-22 test suite

The key stream generated by the above algorithm passed sp800-22 [17] as shown in Table 1. From the table, it is known that the random number generated by our maps passed all the sixteen tests.

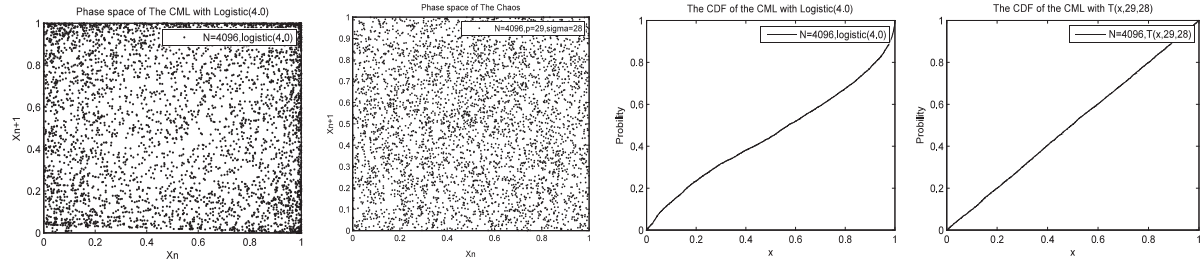
4.3. Histogram of the encrypted image

The histogram of the original image called Lena is shown in Fig 6(b1). The cipher image encrypted by the couple map lattice with Logistic map is shown in Fig 6(a2), while the couple map lattice with our map is shown in Fig 6(a3). The



(a) The cumulating distribution function (b) The autocorrelation coefficient (c) The comparison of symbol entropies

Fig. 4. Statistics properties of the sequences.



(a) The phase space of the original (b) The phase space of the improved (c) The CDF of the original (d) The CDF of the improved

Fig. 5. Comparison with the original couple map lattice.

histogram of the encrypted images is shown in Fig 6(b2) and (b3). From the comparison of the histogram of the encrypted images, it is known that the distributions of the encrypted images changed a lot with the two different encrypt algorithms. Another thing should be mentioned is that the pixel distribution of the cipher image encrypted by our maps is uniform which is better than the image encrypted by the Logistic map.

4.4. Correlations of adjacent pixels

The correlation of adjacent pixels can be evaluated by the correlation exponents of the three different directions, horizontal, vertical and diagonal. The correlation exponents can be calculated by formula (6), where N is number of groups of the points and x_i, y_i is the pixels value of the ith point of group X and y.

Table 1
Key stream sp800-22 test suite (LEN = 262,144).

Statistical test	Parameter	*P*-value	Result
Frequency		0.630894	SUCCESS
Block frequency	M = 128	0.207628	SUCCESS
Runs		0.118276	SUCCESS
Long runs of one's		0.763895	SUCCESS
Binary matrix Rank		0.218168	SUCCESS
Spectral DFT		0.248399	SUCCESS
No overlapping templates	M = 32,768, N = 8, M = 9	0.574039	SUCCESS
Overlapping templates	M = 9, M = 1032, N = 254	0.906134	SUCCESS
Universal		0.383475	SUCCESS
Lempel ziv complexity		0.280646	SUCCESS
Linear complexity	M = 500, N = 524	0.225654	SUCCESS
Serial	m = 16, p_value1	0.830423	SUCCESS
	m = 16, p_value2	0.670414	SUCCESS
Approximate entropy	m = 10	0.127352	SUCCESS
Cumulative sums	Forward	0.661654	SUCCESS
	Reverse	0.906386	SUCCESS
Random excursions	x = −1	0.203411	SUCCESS
Random excursions variant	X = −1	0.597936	SUCCESS
Total (16Test)			100% Pass

$$\gamma = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \sum_{i=1}^{N}(y_i - \bar{y})^2}} \tag{6}$$

For a plain image, the correlation exponents between two adjacent pixels are always high either in horizontal, vertical or diagonal directions, while the encryption algorithm should break the correlations. When simulated on the MATLAB platform, sixty-four pixels at intervals of eight are selected to do the test on each direction and the result is shown in Fig 7. Fig 7(a1)–(a3) described the correlation of the encrypted images on the direction of diagonal, horizontal and vertical, while Fig 7(b1)–(b3) described the original ones. It is clear that the encryption algorithm with our maps could change the relationship of the adjacent pixels of the image dramatically. This is mainly because the value of the original image pixel changed little between adjacent pixels, but the cipher image changed a lot after encryption.

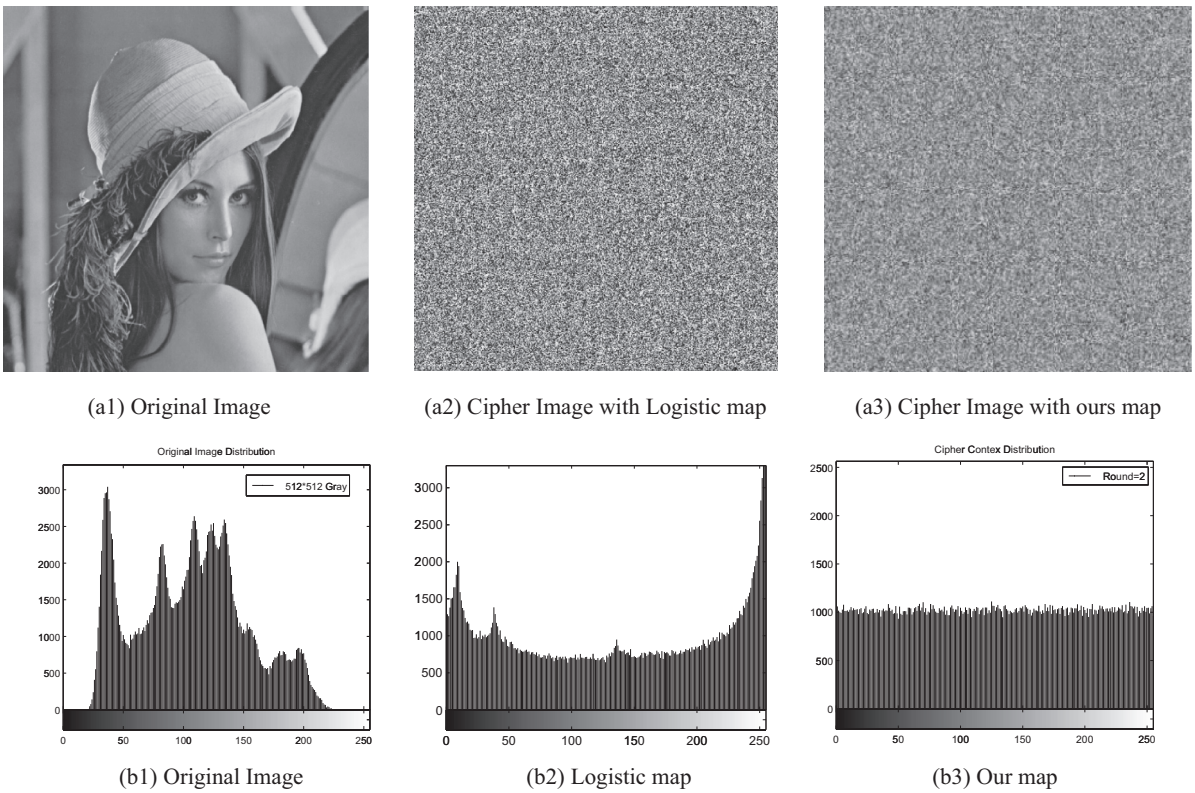
In Table 2, the original image, the encrypted image with Logistic map and our map are compared. From the table, it can be concluded that both the Logistic map and ours can change the structure of the image conspicuously and the correlation of the image can be eliminated clearly.

4.5. Differential attack analysis

From the cryptography theory, a good cryptographic algorithm should be sensitive to changes in the plaintext. This sensitivity is closely related to its ability to resist differential attacks. The sensitivity of the plaintext encryption algorithm is evaluated by the NPCR (Number of Pixels Change Rate, NPCR) of the image or the UACI (Unified Averaged Changed Intensity) of the image. The NPCR is calculated by the formulate (7).

$$P_{\mathrm{NPCR}} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \mathrm{D}(\mathrm{i},\mathrm{j}) \times 100\% \tag{7}$$

A hundred points are selected from the left top to the right bottom in the intervals of five of the plain image to test the sensitivity of the image. During each test the NPCR is calculated when each point changed a bit every time. As shown in Fig 8, the mean value of the NPCRs is quite near to the theory limit value 99.6094% in both Logistic map test and ours, which means the two encryption algorithms have a strong ability to resist the differential analysis. However, the changes of the NPCRs of the algorithm with Logistic map are not stable where the variance becomes larger when the pixels are nearer to right bottom.



(a1) Original Image (a2) Cipher Image with Logistic map (a3) Cipher Image with ours map

(b1) Original Image (b2) Logistic map (b3) Our map

Fig. 6. Comparison of the image before and after encryption.

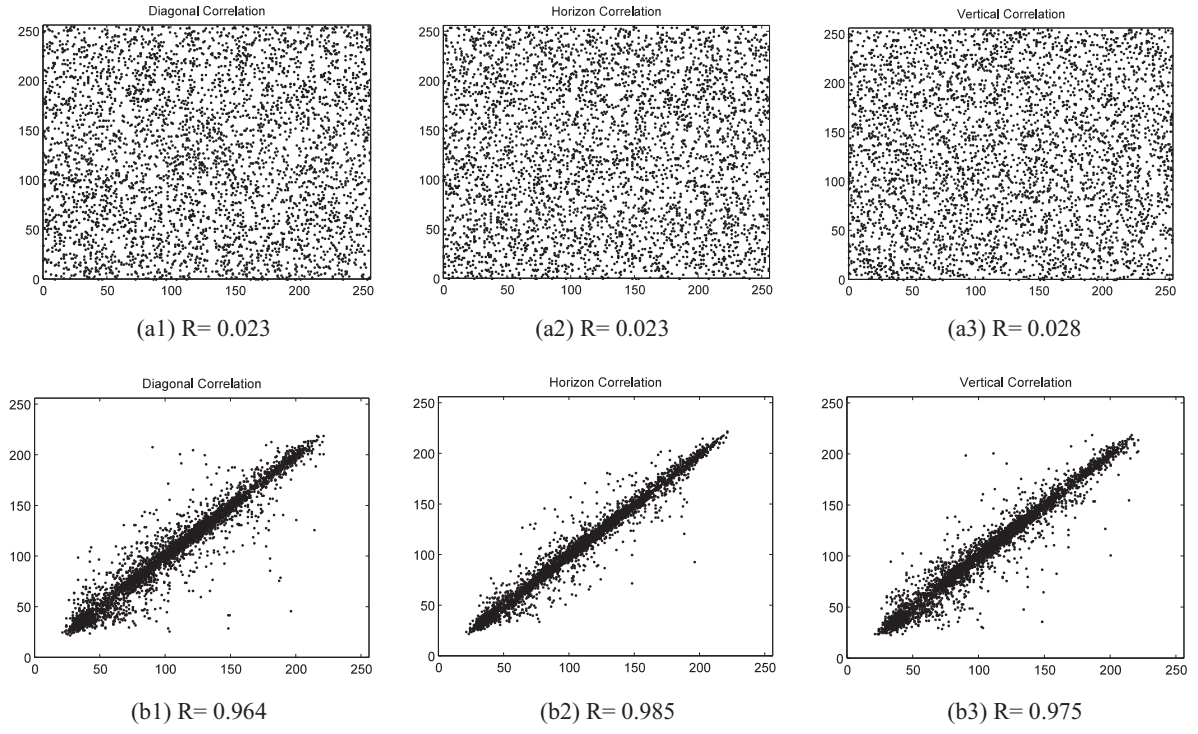


Fig. 7. Comparisons of correlation coefficients between adjacent pixels of three directions.

Table 2
Correlation coefficient of the image before and after encryption.

	Horizon	Vertical	Diagonal
Original image	0.985	0.975	0.964
Cipher with logistic map	−0.001	−0.014	−0.019
Cipher with our map	0.023	0.028	0.023

This is mainly because the pixels nearer to the bottom may iterated less times, which means it need more rounds or a new permutation function to eliminate the influence of the different positions of the image. The changes of NPCRs of our map are stable, which is better than the former.

4.6. Key sensitivity test

A good cryptographic algorithm is also sensitive to the key [18]. When the key of the initial value or the key of the random number changed a bit, the cipher image should change dramatically. When the original key is changed to $(0.9/6, 1.9/6, 2.9/6, 3.9/6, 4.9/6, 5.91/6)$ the NPCR of the code image is 99.6103% which is near the theory limit value. When the key changed a little, the cipher image changed a lot compared with the original cipher image. The changes of the first 200 pixels of the cipher image are described as shown in Fig 9(a) and (b), which is random like in the interval of $[-255, 255]$. The same conclusion could be drawn when other keys changed. From the comparison of Logistic map and ours, it can be told that they are almost the same.

4.7. Algorithm efficiency

The hardware of the experimental environment is the PC of the Pentium (R) Dual-Core 2.6 GHz CPU, 2G-memory. The software environment is the Windows XP operating system and Matlab2009 platform. When compared with the continuous chaotic maps such as Hyper-chaotic system and Lorenz system, the algorithm proposed in this paper can achieve better performance. When generate 4096 bits data stream, the Hyper-chaotic system and Lorenz system needs 43.4375 s and 10.8096 s, while ours just needs 0.1563 s. In addition, the couple map lattice-based system has a parallel structure which can have better performance when implemented on FPGA platform.

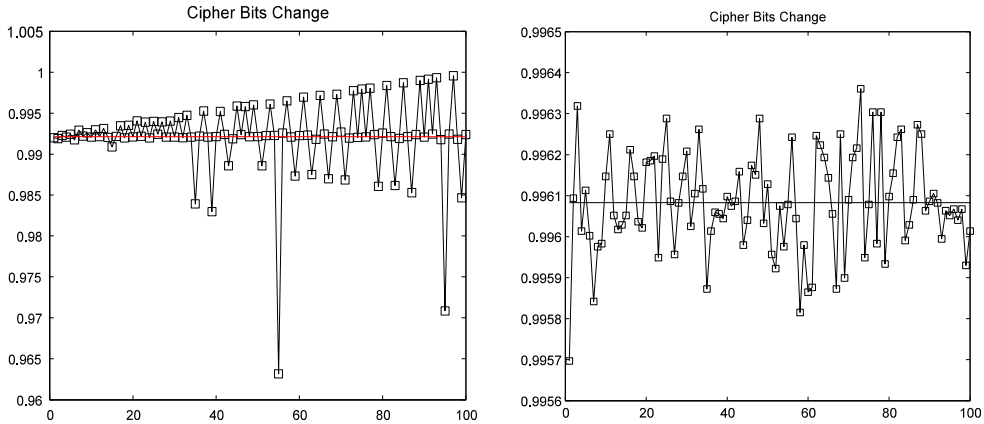


Fig. 8. Differential attack analysis.

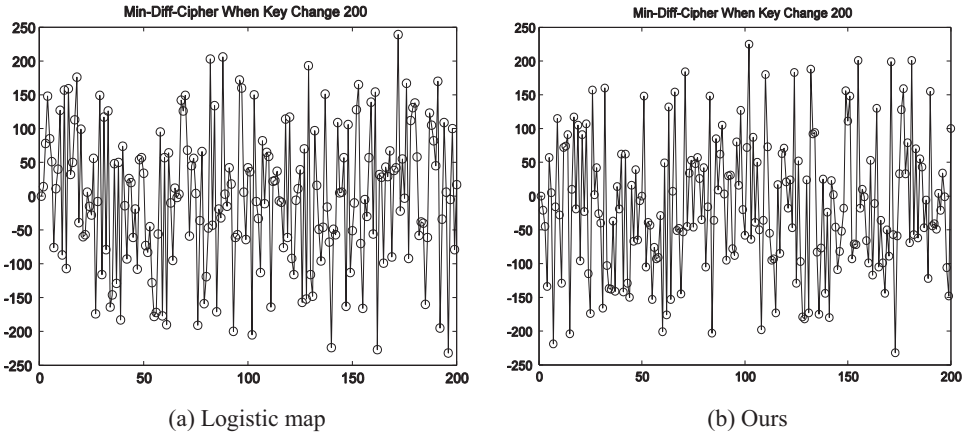


Fig. 9. Sensitivy test.

5. Summary

This paper constructs a class chaos with Markov properties. From the tests, it is known that the system generates a sequence which is uniformly distributed and has higher complexity than Logistic map ($r = 4.0$) and the skew Tent map ($p = 0.51$). An improved couple map lattices with our map is employed to conceal the phase space structure of the chaos and also to increase the key space, which keeps the original property of the uniformity of sequence and the autocorrelation function (δ-like). It has better property than the original one. The key stream generator is constructed then using the couple map lattices with our maps which passed all the sixteen test of sp800-22. A novel image encryption algorithm is also proposed based on the generator, which has dynamical permutation matrix and key streams when using a random number to disturb the key. A carefully designed round function with calculations in different groups is proposed which made the algorithm can resist the CPA and CCA attack. From the test of the image encryption algorithm, it is known that the algorithm can change the image pixels distribution into uniform, which is better than the algorithm with Logistic map. The algorithm is sensitive to the initial key and the plain image from the test. The algorithm is also very efficient when compared with the algorithm with chaos which is represented in ordinary differential equation form and can achieve better performance when implemented in the FPGA platform.

Acknowledgements

This work was supported by National Basic Research Program of China (Grant No. 2007CB311201), the Open Foundation of State Key Laboratory of Applied Optics (Grant No. Y1Q03FQK02) and the Project Development Plan of Science and Technology of Jilin Province (Grant No. 20130522120JH).

References

[1] Socek D, Magliveras S, C'ulibrk D, Marques O, Kalva H, Furht B. Digital video encryption algorithms based on correlation-preserving permutations. EURASIP J Inform Secur 2007.
[2] Ji WY, Hyoungshick K. An image encryption scheme with a pseudo-random permutation based on chaotic maps. Commun Nonlinear Sci Numer Simul 2010;15:3998–4006.
[3] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240:50–4.
[4] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 1998;8(6):1259–84.
[5] Tong XJ. Design of an image encryption scheme based on a multiple chaotic map. Commun Nonlinear Sci Numer Simul 2013;18:1725–33.
[6] Wang H, Han ZZ, Xie QY, Zhang W. Finite-time chaos synchronization of unified chaotic system with uncertain parameters. Commun Nonlinear Sci Numer Simul 2009;14:2239–47.
[7] Guan ZH, Huang FJ, Guan WJ. Chaos-based image encryption algorithm. Phys Lett A 2005;346:153–7.
[8] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul 2012;17:2943–59.
[9] Ercan S, Cahit C, OLCAY TY. Cryptanalysis of Fridrich's chaotic image encryption. Int J Bifurcation Chaos 2010;20(5):1405–13.
[10] Azad RK, Rao JS, Ramakrishna R. Information-entropic analysis of chaotic time series: determination of time delays and dynamical coupling. Chaos Solitons Fractals 2002;2002(14):633–41.
[11] Liu Q, Li PY, Zhang MC, Sui YX, Yang HJ. Construction of a class of chaos systems with Markov properties. Acta Phys Sin 2013;62(17):170505:1–5:8.
[12] Robinson RC. An introduction to dynamical systems: continuous and discrete. Prentice Hall Press; 2004. pp. 459–64.
[13] Lasota A, Yorke J. On the existence of invariant measures for piecewise monotonic transformations. Trans Am Math Soc 1973;186:481–8.
[14] Li T, Yorke J. Period three implies chaos. Am Math Mon 1975;82:985–92.
[15] Li P, Li Z, Halang WA, Chen GR. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. Phys Lett A 2006;349:467–73.
[16] Ding MZ, Yang WM. Stability of synchronous chaos and on-off intermittency in coupled map lattices. Phys Rev E 1997;56:4009–25.
[17] http://csrc.nist.gov/publications/PubsSPs.html#800-22.
[18] Wang XY, Xie YX. Cryptanalysis of a chaos-based cryptosystem with an embedded adaptive arithmetic coder. Chin Phys B 2011;20:080504:1–4:9.
[19] Volos Chk, Kyprianidis IM, Stouboulos IN. Image encryption process based on chaotic synchronization phenomena. Signal Process 2013;93:1328–40.