Commun Nonlinear Sci Numer Simulat 18 (2013) 3075–3085

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A novel image encryption algorithm using chaos and reversible cellular automata

Xingyuan Wang *, Dapeng Luan

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China

ARTICLE INFO

Article history:
Received 18 July 2012
Received in revised form 12 November 2012
Accepted 7 April 2013
Available online 15 April 2013

Keywords:
Image encryption
Intertwining chaos map
Reversible cellular automata

ABSTRACT

In this paper, a novel image encryption scheme is proposed based on reversible cellular automata (RCA) combining chaos. In this algorithm, an intertwining logistic map with complex behavior and periodic boundary reversible cellular automata are used. We split each pixel of image into units of 4 bits, then adopt pseudorandom key stream generated by the intertwining logistic map to permute these units in confusion stage. And in diffusion stage, two-dimensional reversible cellular automata which are discrete dynamical systems are applied to iterate many rounds to achieve diffusion on bit-level, in which we only consider the higher 4 bits in a pixel because the higher 4 bits carry almost the information of an image. Theoretical analysis and experimental results demonstrate the proposed algorithm achieves a high security level and processes good performance against common attacks like differential attack and statistical attack. This algorithm belongs to the class of symmetric systems.

1. Introduction

With the development of internet, information security receives more and more attention. Generally encryption can effectively protect people's information transmitted through public channels. But traditional encryptions methods have limitation in encrypting images such as low efficiency, bulky data, and high correlation among pixels and so on [1–3]. Chaos, which is a complex nonlinear system [4,5], has favorable properties that are suitable for encryption such as high sensitivity to initial values and system parameters, unpredictability, pseudo-randomness and ergodicity [6,7]. So the chaos theory is increasingly applied to cryptosystems. In the last decade, many researchers have proposed many encryption schemes based on chaos [2,3,8–17], most of which are image encryption. Image encryption is usually divided into two subprocesses, confusion and diffusion stage. In the confusion stage, the image pixels are permuted using some transformation method like baker map [3], magic square [18], Arnold map-based [19], while the pixel values remain unchanged. Diffusion stage mainly masks each pixel after permutation sequentially.

In this paper, we combine cellular automata (CA) with chaos to propose a new image encryption. Cellular automata are highly parallel and distributed systems that can simulate complicated behaviors [20]. The large number of CA rules enables many ways to generate sequences. Further, cellular automata evolve by only simple logic computations, with pseudorandom and complex behavior. Cellular automata are also applied in symmetric cipher and public cipher. Public cipher based on cellular automata was first proposed by Guan [21], stream cellular automata stream cipher was proposed by Wolfram [22]. Later, many scholars proposed encryption algorithms based on cellular automata [23–26]. In [25] the authors used reversible cellular automata to implement block encryption algorithm. In our work, we take advantage of strongpoint of both chaos and

* Corresponding author. Tel.: +86 13074102070.
E-mail addresses: wangxy@dlut.edu.cn (X. Wang), dapengspace@163.com (D. Luan).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.04.008

cellular automata to design a new image encryption algorithm. All operations are executed on bit-level. In permutation stage, we use pseudorandom sequences generated by a chaotic map to shuffle the units constructing each pixel. It also changes pixel values besides permutation. In diffusion stage, reversible cellular automata are adopted to iterate on pixel bits many rounds to substitute pixels. The advantages of cellular automata in encryption are listed below:

(1) Large evolution rules space.
(2) Cellular automata only contain integer arithmetic or logic operations, simplifying the computation.
(3) Cellular automata also show complex behaviors, and have parallelism.

The paper is organized as follows. The next section, we briefly give the intertwining map and RCA description we used in this algorithm. In Section 3, the encryption algorithm is presented in detail. Section 4 gives the theory analysis and simulation results. The last Section concludes the paper.

2. Intertwining logistic map and reversible cellular automata

2.1. Intertwining logistic map

Logistic map, which is a simple and classic nonlinear model, is used in many image encryption algorithms [6,7,14–16] in the past few years. Logistic map is defined below:

$$x_{n+1} = px_n(1 - x_n),$$

where $0 < x_n < 1$ and $3.59 < p < 4$. Though the simplicity is the map, the sequences generated by logistic map are sensitive to the change of its initial value and the properties including pseudorandom capability and data irrelevance remains well. However, in general, the logistic map has some common weakness such as stable windows, blank windows, a weak key and relative small key space and uneven distribution of sequences. And these defects may 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 [27] which is defined as following:

$$\begin{cases} x_{n+1} = [u \times k_1 \times y_n \times (1 - x_n) + z_n] \bmod 1 \\ y_{n+1} = [u \times k_2 \times y_n + z_n \times 1/(1 + x_{n+1}^2)] \bmod 1 \\ z_{n+1} = [u \times (x_{n+1} + y_{n+1} + k_3) \times \sin(z_n)] \bmod 1 \end{cases}, \tag{1}$$

where u, k_i are the parameters and $0 < u \leqslant 3.999$, $|k_1| > 33.5$, $|k_2| > 37.5$, $|k_3| > 35.7$. The distribution of the sequences becomes better and importantly, blank windows are removed. The map's behavior and comparison are shown in Figs. 1 and 2.

From the Figs. 1 and 2, we can see that 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 has increased greatly.

To determine whether a map is chaotic or not, the simplest way is to look into the map's Lyapunov exponent. From Fig. 3, we can see that the Lyapunov exponent of intertwining logistic map is all positive, while logistic map's Lyapunov exponent exists negative. This shows a much more chaotic behavior of intertwining map. From analysis of the distribution of the sequences and Lyapunov exponents, intertwining chaotic map has been indicated as much more complex and randomness.

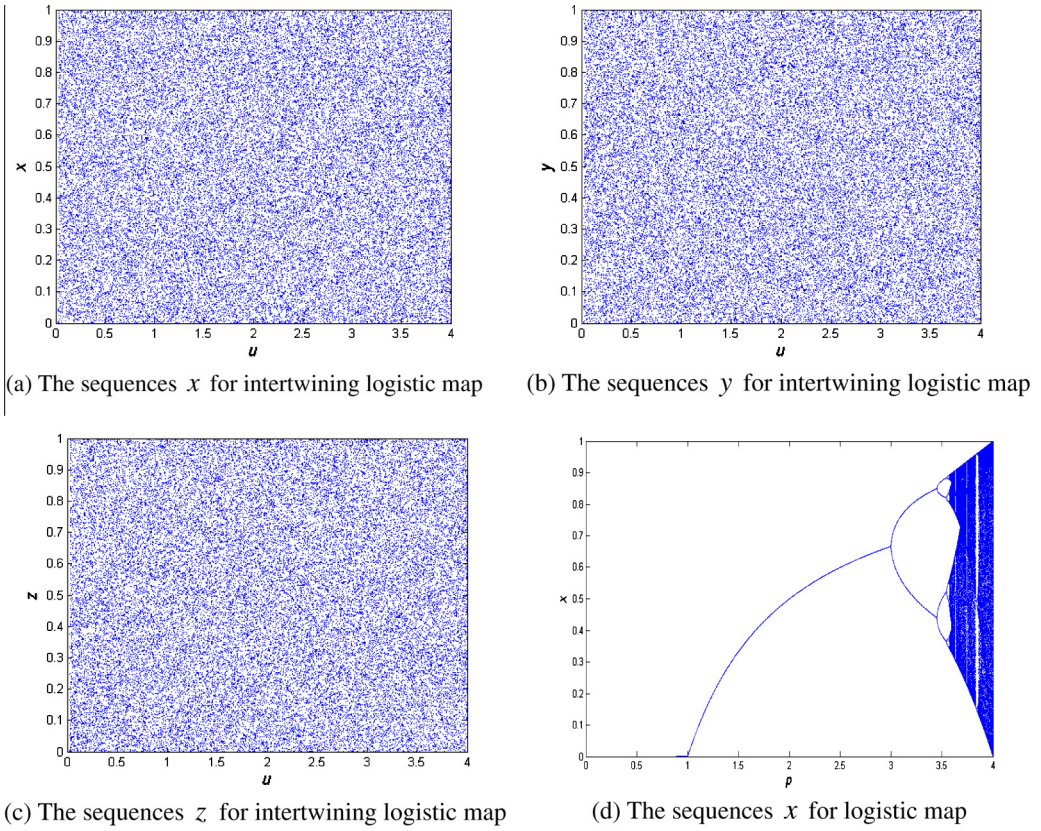
2.2. Reversible cellular automata

Cellular automata theory was first established to study possibility of robots self-replication by Von.Neumann. Now CA is described to be a dynamic system composed of cells with discrete, finite states in the cell space that evolutes in discrete time dimension in accordance with the given local rules. Generally, a CA can be defined as a 4-uplet: $CA = \{C, S, V, F\}$. C is the cell space, S is the discrete state sets, for the simplest case $S = \{0, 1\}$. V determines what cells are one cell's neighborhoods, which are used to determine cell's states in the next time. F is called the transfer function that means the rules according to which the next cell's state is going to be. Often all the cells' states at a certain time t are called a CA's configuration. CA can be classified by different dimensions, such as one-dimension CA, two-dimension CA and three-dimension CA and so on. Among those kinds of CA, the most classic and applied most is two-dimension CA because many objects to study in real life are two dimensional. As to the 2-dimensional characteristics of image, we choose the 2-dimensional CA in our work.

A 2-dimensional CA is defined in a 2-dimensional space. Theoretically, the cell space is infinite, but in practice, it usually attaches boundary conditions to simulate the infinite situation without losing any properties. Eq. (2) is the boundary conditions.

$$S_{i,j}^t = S_{u,v}^t \Longleftrightarrow i \equiv u(\bmod\ r) \text{ and } j \equiv v(\bmod\ c), \tag{2}$$

where i, j, u, v are coordinates in a 2-dimensional cell space(a rectangle) of $r \times c$. The states each cells have are defined as: $S = \{0, 1\}$. In 2-dimensional plane, the common neighborhood models are given in the following from Fig. 4:



(a) The sequences x for intertwining logistic map (b) The sequences y for intertwining logistic map

(c) The sequences z for intertwining logistic map (d) The sequences x for logistic map

Fig. 1. Distribution comparison of intertwining logistic map and logistic map.

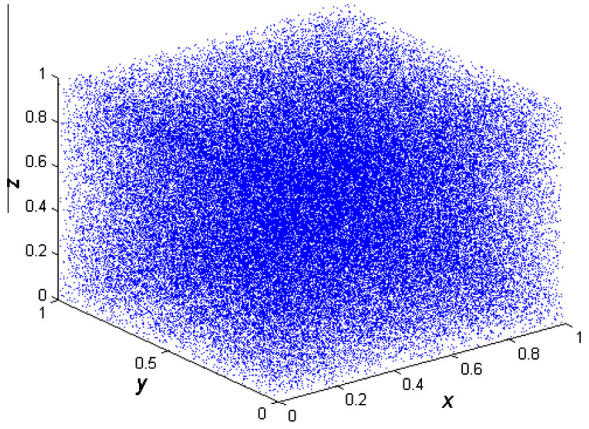


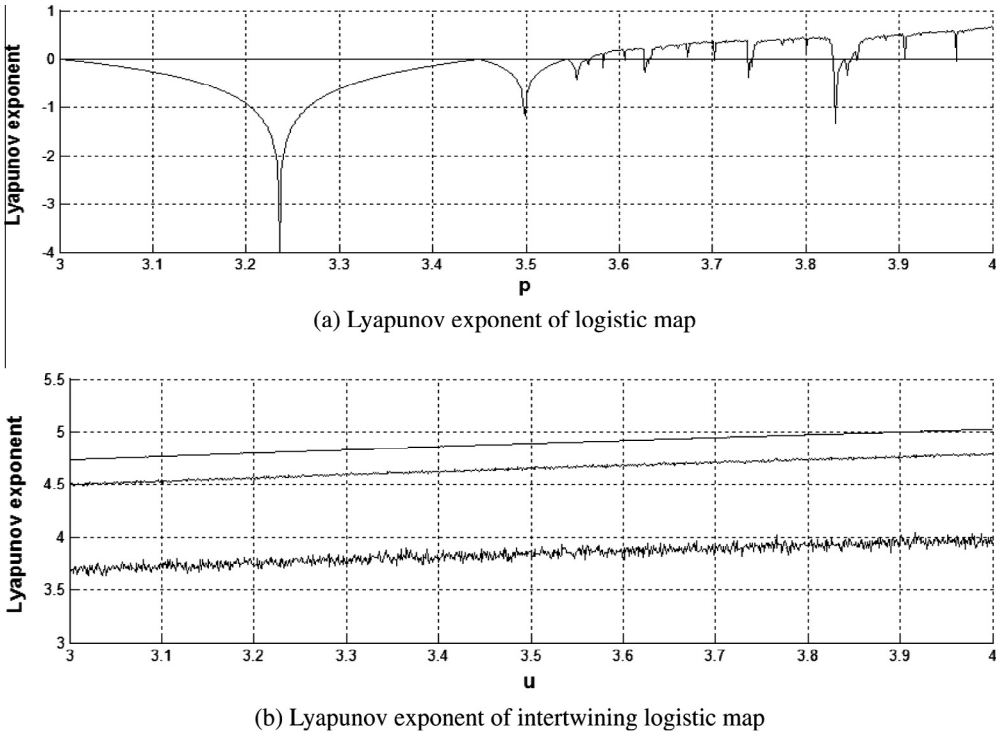
Fig. 2. Sequences of intertwining logistic map.

In our proposed algorithm, we choose the simplest Von.Neumann type as our neighborhood model. Despite the simplicity, we will later see that it has as complex behaviors as others have. What is special is the transfer function F. As we given above, F can be formalize as follows:

$$F : C^t \to C^{t+1}.$$

To be specific:

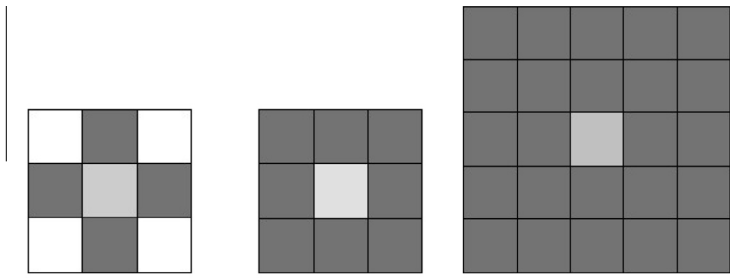
$$F : S_{ij}^{t+1} = f(S_{i-rj-r}^t, \ldots, S_{ij}^t, \ldots, S_{i+rj+r}^t).$$



(a) Lyapunov exponent of logistic map

(b) Lyapunov exponent of intertwining logistic map

Fig. 3. Lyapunov exponents comparison.



(a)Von.Neumann Type (b)Moore Type (c)Extended Moore Type

Fig. 4. Different types of neighborhood of a cell.

We also consider the cell's previous state when generate the next state when CA evolutes. So the transfer function F becomes like:

$$F : S_{ij}^{t+1} = f(S_{i-r,j-r}^{t}, \ldots, S_{ij}^{t}, \ldots, S_{i+r,j+r}^{t}, S_{ij}^{t-1}), \tag{3}$$

Eq. (3) makes a CA invertible and this type of CA is called reversible cellular automata [22]. RCA can be used as cryptosystems in natural way. In our algorithm, we use RCA with particular rules to achieve diffusion. The transfer function is given in Table 1.

3. Proposed algorithm

Our proposed algorithm composes of two parts: confusion and diffusion stage. In the confusion stage, we shuffle image on unit-level which is a much smaller level than pixels by using chaotic maps. The reversible cellular automata is performed on higher half pixel bits many rounds in diffusion stage. After confusion and diffusion, we get the cipher image. The whole procedure is shown in Fig. 5.

Table 1
The local rules of our RCA.

$S^t_{i,j-1}S^t_{i-1,j}S^t_{i,j}S^t_{i+1,j}S^t_{i,j+1}$	$S^{t+1}_{i,j}$		$S^t_{i,j-1}S^t_{i-1,j}S^t_{i,j}S^t_{i+1,j}S^t_{i,j+1}$	$S^{t+1}_{i,j}$	
	$S^{t-1}_{i,j}=0$	$S^{t-1}_{i,j}=1$		$S^{t-1}_{i,j}=0$	$S^{t-1}_{i,j}=1$
00000	1	0	10000	0	1
00001	1	0	10001	0	1
00010	1	0	10010	0	1
00011	1	0	10011	0	1
00100	0	1	10100	0	1
00101	0	1	10101	0	1
00110	1	0	10110	1	0
00111	1	0	10111	1	0
01000	0	1	11000	0	1
01001	0	1	11001	0	1
01010	0	1	11010	1	0
01011	0	1	11011	1	0
01100	1	0	11100	0	1
01101	1	0	11101	0	1
01110	1	0	11110	0	1
01111	1	0	11111	0	1

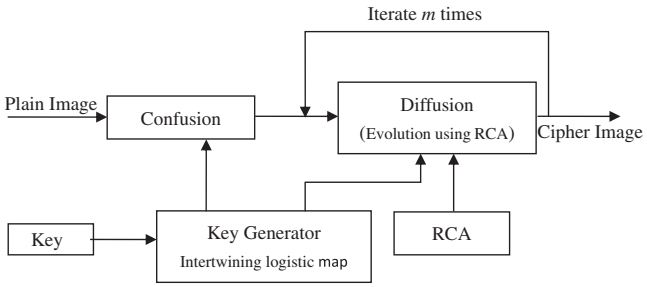


Fig. 5. The proposed image cryptosystem flow.

3.1. Image permutation

Without loss of generality, we assume the size of the plain-image P as $M \times N$, and the pixels' values range from 0 to 255. Each pixel's value is represented by this:

$$p = \sum_{i=0}^{7} 2^i,$$

where i is the value at different position when a pixel is expressed in bit. That means a bit contains different amount of information depending on its position. For example '1' in the highest position (7th) represents 128, but the lowest bit only 1. Based on different information amount depending on position, in our work the permutation of image is achieved using the sequences generated by intertwining logistic map. In addition to lessen the correlation of adjacent pixels, we also reach diffusion to some extent in the permutation stage. The permutation procedure is listed below in detail:

(1) Divide each pixel into two parts each of which contains 4 bits. Then the image is stretched to be $M \times N \times 2$, we call it P'.

(2) Iterate intertwining logistic map to generate three sequences: $\{x_k\}$, $\{y_k\}$, $\{z_k\}$, and discretize the $\{x_k\}$, $\{y_k\}$, $\{z_k\}$:

$$\{\hat{x}_k\} = \lfloor \{x_k\} \times 10^{13} \rfloor \bmod M,$$

$$\{\hat{y}_k\} = \lfloor \{y_k\} \times 10^{13} \rfloor \bmod 2N,$$

$$\{\hat{z}_k\} = \lfloor \{z_k\} \times 10^{13} \rfloor \bmod 2.$$

(3) From the top left corner unit (4 bits) to the bottom right corner unit, we exchange the $P'_{i,j}$ and $P'_{\hat{x}_i,\hat{y}_j}$, where $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, 2N$. And the permuted image (Lena image size of 512×512) is shown below in Fig. 6:

Fig. 6. Permuted image of Lena.

Table 2
Percentage of pixel information contributed by different bits.

Bit position i	Percentage $p(i)$ of an information pixel
0	0.3922
1	0.7843
2	1.5686
3	3.1373
4	6.2750
5	12.5500
6	25.1000
7	52.2000

3.2. Image diffusion

In diffusion process, RCA evolve on pixel bits to change pixel properties. As we talked about that the bit in a higher position owns more information of pixel, in order to save space and time while keep well encryption effect, we only consider the first higher 4 bits in one pixel. From Table 2, we can see that more than 90% information is occupied by the higher 4 bits. So the RCA's cell space is defined as a square constructed by units of the higher 4 bits of each pixel. We name the rectangle as *PC*. It should be like Fig. 7 shown below:

The local rules are given in Table 1, the model chosen is Von.Nueuman type and the boundary condition is defined by Eq. (2). The RCA's evolution is proceeding in discrete time dimension, and we denote the cell space at different time by C^t. And *PC* is C^{t_1}. Note that in the RCA evolution according to Eq. (3), a previous state C^{t_0} is needed. C^{t_0} is constructed by the discretized sequence $\{\hat{z}_k\}$ generated in permutation stage. So the diffusion flow is illustrated below in the Fig. 8.

After r rounds of iteration, the C^{t_r}, where r is the number of iteration. C^{t_r} together with the lower 4 bits that are derived from image permutation stage construct the cipher image.

One thing we must be aware of is that for some images whose information mostly being concentrated on the last 4 bits, the process described above is useless as the cipher has not considering lower 4 bits in one pixel. For this situation, extra an operation need to be added in each of round of RCA evolution.

$$c_i = c_{i-1} \oplus p'_i \oplus \mathrm{mod}(\lfloor z_i \times 10^{13} \rfloor, 256)$$

where $i = 1, 2, ..., M \times N$, c_i, p'_i stand for cipher pixel and the pixel after permutation, respectively. c_{-1} is given in advance.

4. Performance and security analysis

4.1. Key space analysis and sensitivity analysis

Any image encryption algorithm thought to be secure should have a large key space that makes brute attack ineffective. In our proposed algorithm the key lies in both confusion and diffusion stage. The keys consist of the following: (1) the initial values of intertwining logistic maps $x_0, y_0, z_0, u, k_1, k_2, k_3$, (2) the number of the RCA's local rules and (3) the iteration rounds r and c_{-1} .

Because the inherent high sensitivity to initial values and parameters, the chaotic map's precision is considered as 10^{-16} [17,28]. So the key space is calculated:

$$\begin{matrix} b_{1,1}^7 b_{1,1}^6 b_{1,1}^5 b_{1,1}^4 b_{1,2}^7 & \cdots & \cdots & b_{1,N-1}^4 b_{1,N}^7 b_{1,N}^6 b_{1,N}^5 b_{1,N}^4 \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ b_{M,1}^7 b_{M,1}^6 b_{M,1}^5 b_{M,1}^4 b_{M,2}^7 & \cdots & \cdots & b_{M,N-1}^4 b_{M,1}^7 b_{M,1}^6 b_{M,1}^5 b_{M,1}^4 \end{matrix}$$

Fig. 7. RCA's cell space from image.

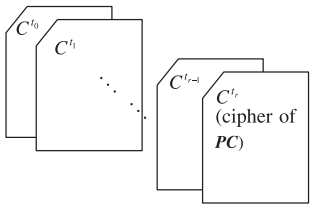


Fig. 8. RCA performed to image.

Table 3
Key space size of proposed algorithm and other different scheme.

Scheme	Proposed	Ref. [15]	Ref. [16]
Key size	2^{280}	2^{128}	2^{157}

$$S = 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^3 \times 2^{2^6} \gg 2^{128},$$

which is large enough to resist brute force attacks. From Table 3, the proposed algorithm's key size is larger than other encryption schemes. Fig. 9 shows the sensitivity to the key, Fig. 6(a) is cipher encrypted by key ($u = 1.5, x = 0.36, y = 0.25, z = 0.78, k_1 = 35.5, k_2 = 38.2, k_3 = 36.1, r = 6, c_{-1} = 168$), while Fig. 9(b) is decrypted by the key ($u = 1.5000000000001$) with a tiny difference while keep other parameters all the same. Fig. 9(c) is the image decrypted by the right key, and Fig. 9(d) is the image encrypted using the key ($u = 1.5000000000001$). By comparing the two encrypted images using the same key and key with only tiny differences, there is a 99.7295% difference between them (Fig. 9(a), Fig. 9(d)). It shows that our algorithm has a high level sensitivity to initial key.

4.2. Statistical analysis

According to Shannon's theory, it is possible to solve many kinds of ciphers by statistical analysis. Confusion and diffusion are introduced to increasing the difficulty of statistical analysis. 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) Histogram of encrypted images. Select several 256 gray-level images with size of 512×512 that have different contents and then calculate their histograms. Our results (Lena) are shown in Fig. 10. From the histogram we can see that the histogram has fairly uniformed distribution.
(2) Correlation of two adjacent pixels. To test the correlation of pixels (vertical, horizontal, diagonal), we randomly select 3000 pairs of adjacent pixels both from plain image and encrypted image, and calculate the correlation coefficients of pixels according the following formula:

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4}$$

where

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i, D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2.$$

Fig. 11 shows the horizontal correlation of pixels of plain image, cipher image, respectively. From the Fig. 11 we see that our algorithm reduces the correlation between adjacent pixels effectively.

Table 4 gives more tests on correlations. The result indicates that our proposed encryption effects are rather well.

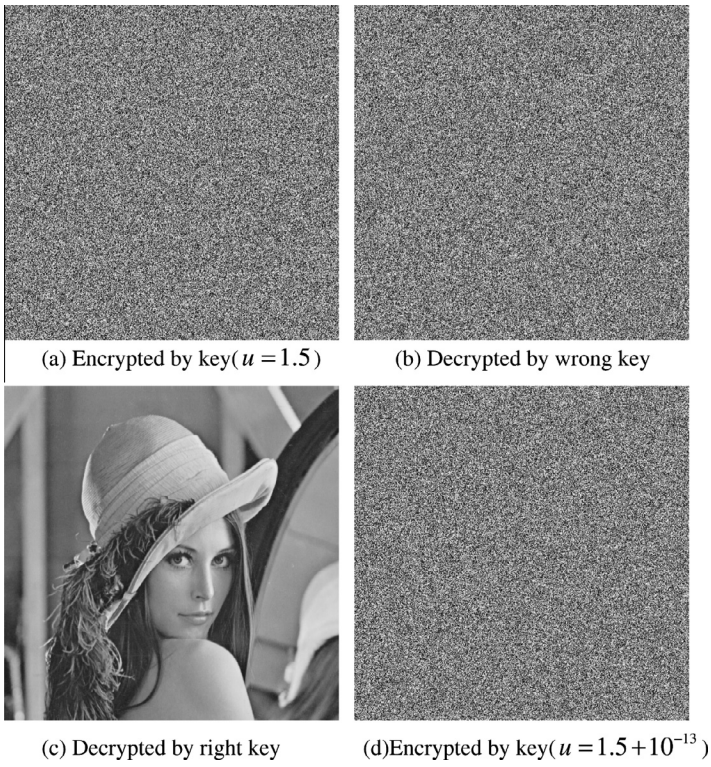


Fig. 9. The algorithm's sensitivity to key.

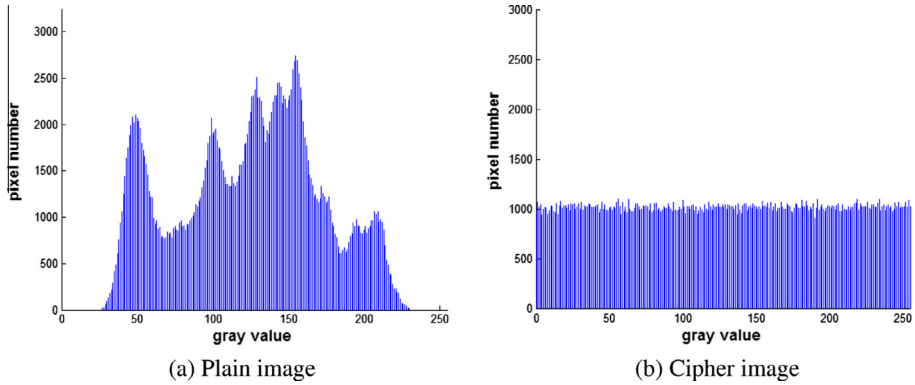


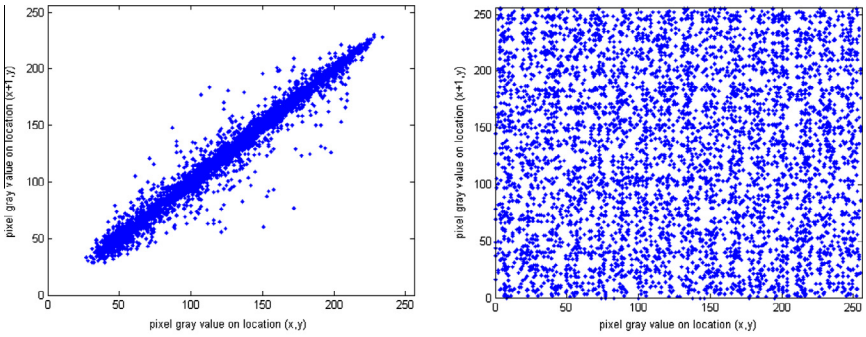
Fig. 10. Histogram of images.

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:

$$H(m) = -\sum_{i=0}^{2^n-1} p(m_i)\log_2 \frac{1}{p(m_i)}, \tag{5}$$

where m is the message. $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. To a message of which a symbol is encoded by 8 bits, when ideally random, entropy should be 8, in general, the entropy value of the message is smaller than 8, but ought to be close to be ideal. As shown in Table 5, we notice that the values obtained in the proposed scheme are very closer to 8, better than other schemes. This indicates that the scheme has hidden information randomly, and information leakage in encryption process is negligible.



(a)Horizontal correlation (Lena) (b)Horizontal correlation(cipher Lena)

Fig. 11. Correlation of plain image and cipher image.

Table 4
Correlation test.

Image	Ref. [26]	Ref. [29]	Proposed
Lena			
Horizontal	−0.015166	−0.002902	0.001117
Vertical	0.013962	−0.015075	0.019254
Diagonal	0.021808	0.012912	0.004548
Sailboat			
Horizontal	0.029174	0.016378	0.012510
Vertical	−0.018017	−0.005022	0.002329
Diagonal	0.030255	0.021685	0.013534
Pepper			
Horizontal	0.013137	0.014982	0.014360
Vertical	0.020275	0.002165	0.004224
Diagonal	−0.013955	−0.024071	−0.002939

Table 5
Entropy of ciphered images.

Image	Proposed	Ref. [26]	Ref. [29]
Lena	7.9992	7.9368	7.9997
Sailboat	7.9973	7.9643	7.9957
Pepper	7.9993	7.9487	7.9961

4.4. Differential attack

In addition to brute attack in cryptanalysis, there is another important method, which is called differential attack, to crack the encryption algorithm. Often the attacker usually make a tiny change in the plain image (e.g., modify only one pixel) to observe changes in the cipher image. By comparing the difference, the cryptanalyst may find out the subtle relationship between plain image and cipher image. A good encryption algorithm should satisfy that over 50% differences between the cipher images even if a minor change takes place in the plain images. This can be measured by means of two criteria, i.e., the number of pixel change rate (NPCR) and the unified averaged changing intensity (UACI) which are computed in formula Eqs. (6) and (7).

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{6}$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255}\right] \times 100\%, \tag{7}$$

where W and H represent the width and height of the image, respectively. $C(i,j)$ and $C'(i,j)$ are the ciphered images before and after one pixel of the plain image is changed. For position (i,j), if $C(i,j) \neq C'(i,j)$, then $D(i,j) = 1$; else $D(i,j) = 0$. Table 6 shows the NPCR and UACI results according our proposed encryption tested on several images. From the results we can

Table 6
NPCR and UACI of ciphered image.

Test	Proposed	Ref. [26]	Ref. [29]
NPCR (%)	99.79	99.96	99.61
UACI (%)	33.35	33.44	33.47

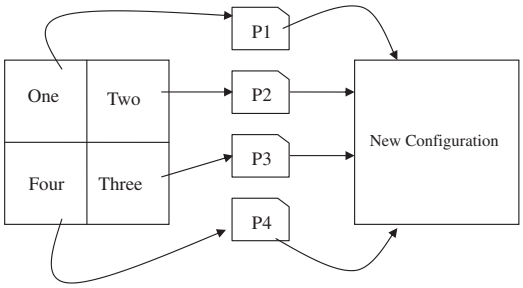


Fig. 12. Evolution on multiprocessor.

see that the NPCR is over 99% and UACI is very close to 33.33%. Therefore, the proposed algorithm is very sensitive to plain image, even if a very tiny difference due to intertwining logistic map and cellular automata. Comparing to other schemes from Table 6, our scheme shows a more competitive ability to resist differential attack.

4.5. RCA parallelism

The parallelism derives from the way the reversible cellular automata evolutes in every round. So the encryption efficiency can be improved by dividing the image into several parts, each of which will be processed by a single processor or a thread, in every round on multiprocessor computer. And in the end, all the subimages make up the final cipher image. For example, the image can be divided into two parts to process, the left part and the right part in every round, the RCA evolutes in each part independently, after completed; both of them construct a new intermediate image for the next round. And repeat the process until all the rounds have done. The process can be described below:

In Fig. 12, the image is divided into 4 subimages after permutation, each subimage can be processed by one processor using the same key except that c_{-1} is unique to each processor. After each evolution completed, the 4 images reconstruct the cipher image.

5. Conclusion

In this paper, we propose an image encryption algorithm that based on chaos combined with reversible cellular automata which show complex behaviors and have large rule space. The pixels are permuted by the intertwining logistic at the same time change values of pixels. Through reversible cellular automata, the cipher is generated after many rounds on bit-level. Experimental results and security analysis for the proposed algorithms 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 secure and hence more suitable for image encryption for applications. As future work, the plan is to study parallelism cryptosystem.

Acknowledgements

This research is supported by the National Natural Science Foundation of China (Nos.: 61173183, 60973152, and 60573172), the Superior University Doctor Subject Special Scientific Research Foundation of China (No.: 20070141014), Program for Liaoning Excellent Talents in University (No.: LR2012003), the National Natural Science Foundation of Liaoning province (No.: 20082165) and the Fundamental Research Funds for the Central Universities (No.: DUT12JB06).

References

[1] Chen GR, Mao YB, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004;21(3):749–61.
[2] Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption. Chaos Solitons Fractals 2009;40(1):309–18.
[3] Mao YB, Chen GY, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurcation Chaos 2004;14(10):3613–24.
[4] Zhang HG, Ma TD, Huang GB, Wang ZL. Robust global exponential synchronization of uncertain chaotic delayed neural networks via dual-stage impulsive control. IEEE Trans Syst Man Cybern B Cybern 2010;40(3):831–44.

[5] Zhang HG, Fu J, Ma TD, Tong SC. An improved impulsive control approach to nonlinear systems with time-varying delays. Chin Phys B 2009;18(3):969–74.
[6] Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations. Chaos Solitons Fractals 2009;40(5):2557–68.
[7] Dutta D, Bhattacharjee JK. Period adding bifurcation in a logistic map with memory. Physica D 2008;237(23):3153–8.
[8] Xiang T, Liao XF, Tang GP, Chen Y, Wong K. A novel block cryptosystem based on iterating a chaotic map. Phys Lett A 2006;349(1–4):109–15.
[9] Wang XY, Jin CQ. Image encryption using Game of Life Permutation and PWLCM chaotic system. Opt Commun 2011;285(4):412–7.
[10] Ye RS. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Opt Commun 2011;284(22):5290–8.
[11] Liu HJ, Wang XY. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284(16–17):3895–903.
[12] Huang CK, Nien HH. Multi chaotic systems based pixel shuffle for image encryption. Opt Commun 2009;282(11):2123–7.
[13] Behnia S, Akhshani A, Ahadpour S, Mahmodi H, Akhavan A. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Phys Lett A 2007;366(4–5):391–6.
[14] Wang Z, Huang X, Li N, Song XN. Image encryption based on a delayed fractional-order chaotic logistic system. Chin Phys B 2012;21(5):050506.
[15] Patidar V, Pareek NK, Sud KK. A new substitution diffusion based image cipher using chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul 2009;14(7):3056–75.
[16] Patidar V, Pareek NK, Purohit G, Sud KK. Modified substitution-diffusion image cipher using chaotic standard and logistic maps. Commun Nonlinear Sci Numer Simul 2010;15(10):2755–65.
[17] Khan MK, Zhang JS, Alghathbar K. Challenge-response-based biometric image scrambling for secure personal identification. Future Gen Comput Syst 2011;27(4):411–8.
[18] Shen JB, Jin XG, Zhou C. A color image encryption algorithm based on magic cube transformation and modular arithmetic operation. Adv Multimedia Inf Process 2005;3768:270–80.
[19] Guan ZH, Huang FJ, Guan WJ. Chaos-based image encryption algorithm. Phys Lett A 2005;346(1–3):153–7.
[20] Sarkar P. A brief history of cellular automata. ACM Comput Surv 2000;32(1):80–107.
[21] Guan P. Cellular automata public-key cryptosystem. Complex Syst 1987;1:51–6.
[22] Wolfram S. Cryptography with cellular automata in advances in cryptology. In: Advances in cryptology-Crypto's 85 Proceedings, vol. 218; 1986. p. 429–32.
[23] Chen RJ, Lai JL. Image security system using recursive cellular automata substitution. Patter Recognit 2007;40(5):1621–31.
[24] Seredynski F, Bouvry P, Zomaya AY. Cellular automata computations and secret key cryptography. Parallel Comput 2004;30(5–6):753–66.
[25] Seredynski M, Pienkosz K, Bouvry P. Reversible cellular automata based encryption. Netw Parallel Comput 2004;3222:411–8.
[26] Abdo AA, Lian SG, Ismail IA, Amin M, Diab H. A cryptosystem based on elementary cellular automata. Commun Nonlinear Sci Numer Simul 2013;18(1):136–47.
[27] Shatheesh Sam I, Devaraj P, Bhuvaneswaran R. An intertwining chaotic maps based image encryption scheme. Nonlinear Dyn 2012;69(4):1995–2007.
[28] Xiao D, Liao XF, Deng SJ. Parallel keyed hash function construction based on chaotic maps. Phys Lett A 2008;372(26):4682–8.
[29] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul 2012;17(7):2943–59.