Nonlinear Dyn (2015) 79:2449–2456
DOI 10.1007/s11071-014-1824-0

ORIGINAL PAPER

A novel image encryption scheme using chaos and Langton's Ant cellular automaton

Xingyuan Wang · Dahai Xu

Received: 5 September 2014 / Accepted: 20 November 2014 / Published online: 13 December 2014

Abstract The paper tries to give a new scheme for image encryption, which innovatively introduced the idea of Langton's Ant cellular automaton to scramble the image. We virtualize a chessboard with the size of the image, and let the ant crawls on it by following the rules which Langton gives and steps generated by intertwining logistic map, then to determine the position of the plain image's pixels in the scrambling image according to the position which the ant stay each time. Lastly, the PWLCM chaos map has been used to diffuse the image. Experimental results and security analysis show that our scheme is secure and can be used in image encryption and transmission.

Keywords Image encryption · Langton's Ant · Cellular automaton · Intertwining logistic map · PWLCM

1 Introduction

There are many ways to encrypt images, generally three types of forms are more obviously: ① Converting an image into one general stream of characters and using the traditional encryption methods, such as DES, AES [1], etc. But considering the large amount data of the image, such algorithms usually improve and optimize accordingly. ② The image has been regarded as a two-dimensional matrix, which a series of mathematical transformations will be carried out on. This is the main idea for encryption currently. Of course, the specific forms vary widely, and some algorithm will put the two-dimensional image into a one-dimensional sequence. But overall, most of them abandoned the traditional method of encryption, fully using the characteristics of the image, which brought a great increase in performance. ③ The combination of encryption and compression [2–5], in fact, no matter the compression is either before or after the encryption, the amount of resulting cipher text generally been cut ultimately, so just need to transfer less data in the transmission.

Encryption based on chaos [6–10,20–22] is one of the typical methods. Usually, these algorithms are designed to combine chaos with other ideas, its main advantage is that you can take advantage of the superior characteristics of chaos to meet the needs of encryption.

However, these algorithms usually have some problems: ① Chaos itself is flawed. As Arnold map's problems are often criticized, the number of its iterations is limited, which is <1,000 times. ② Some algorithms have poor versatility, and they tend to have stringent requirements about images. ③ The design of arithmetic logic is defective and cannot deal with common analysis attacks. Due to the presence of defects, many algorithms have been cracked [11–16].

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

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

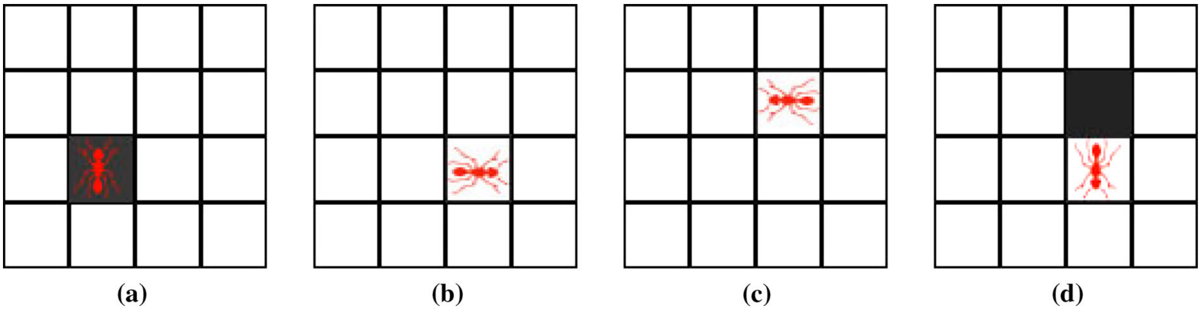

Fig. 1 Demonstration of the rules. **a** Start state of rule 1, **b** end state of rule 1, **c** start state of rule 2, **d** end state of rule 2

This paper try to using the idea of the Langton's Ant cellular automaton to make a new scheme for image encryption. We give the algorithm designed by applying it to scramble, the article uses two kinds of chaotic maps to confuse and diffuse the image.

The paper is organized as follows: the descriptions about Langton's Ant cellular automaton and chaos used in this paper is in Sect. 2. Section 3 gives a detailed description of our algorithm, and Sect. 4 is the experiment, the security analysis has been discussed in Sect. 5, and the conclusion in final.

2 Preparation

2.1 Cellular automaton

Cellular automaton originally proposed by mathematician Stanislaw M. Ulam (1909–1984) and John von Neumann (1903–1957) in the 1940s [17]. It is a discrete dynamical system in terms of morphological manifestations. It is comprised of grids which followed some special rules, each grid can be seen as a cell, and each cell has some states, but only can have one state in a moment. Along with changing over time (we called "iteration" process), each cell in the grids change its state according to the states of peripheral cells by following the same rules, in other words, one cell's state is determined by the states of cells surrounded in the last moment. In view of artificial life, cellular automaton can be seen as a world which so many single-celled organisms' lives, after we set the initial state of the world, they will start the evolution by following the same rules.

A cellular automaton consists of several parts: determine the dimensions of the cell's living space, define the states the cells may have, define the rules how the cell change its state, set the initial state of each cells. Cellular automaton, in terms of living space, can be one dimensional, two dimensional, three dimensional, or higher dimensions.

2.2 Langton's Ant cellular automaton

Langton's Ant cellular automaton is an example of cellular automata. It is proposed by Christopher Langton [18]. Its main principle is as follows: The girds in the plane (we called "chessboard") are filled with black or white.

There is one ant in one of the girds. Its head toward one of the four directions (up, down. left, right). The ant crawls by following two rules: ① If the ant is in the black gird, it should turn right by 90°. Then change the black grid to white, and move forward by one step. ② If the ant is in the white gird, it should turn left by 90°. Then change the white gird to black, and move forward by one step. Figure 1 shows the demonstration of the rules.

2.3 Chaotic system

2.3.1 The intertwining logistic map

The intertwining logistic map can be described as below:

$$\begin{cases} x_{n+1} = [\mu \times k_1 \times y_n \times (1 - x_n) + z_n] \bmod 1 \\ y_{n+1} = \left[\mu \times k_2 \times y_n + z_n \times 1 \Big/ 1 + x_{n+1}^2\right] \bmod 1 \\ z_{n+1} = \left[\mu \times (x_{n+1} + y_{n+1} + k_3) \times \sin(z_n)\right] \bmod 1 \end{cases} . \quad (1)$$

where $0 < \mu \leq 3.999$, $|k_1| > 33.5$, $|k_2| > 37.9$, $|k_3| > 35.7$. The intertwining logistic map is much more chaotic than the logistic map; moreover, it has no blank windows and much even distribution [19].

2.3.2 The PWLCM map

Piecewise linear chaotic map:

$$x_i = F(x_{i-1}, \eta) = \begin{cases} \frac{x_{i-1}}{\eta}, & 0 < x_{i-1} < \eta \\ \frac{x_{i-1}-\eta}{2-\eta}, & \eta \leq x_{i-1} < 0.5 \\ F(1-x_{i-1}, \eta), & 0.5 \leq x_{i-1} < 1 \end{cases}. \quad (2)$$

where $x_i \in (0, 1)$, $\eta \in (0, 0.5)$. The PWLCM map is evenly distributed. It also has commendable ergodicity.

3 Algorithm

For $M \times N$ image P, we use the Langton's Ant cellular automaton and intertwining logistic map to scramble the image, and then diffuse it with PWLCM map.

Step 1 In order to resist attacks, we need to introduce the plaintext sensitivity. On the other hand, the chaos is sensitive to the initial value. So we can expressly use the plaintext to modify the initial value of the chaos.

$$x_0' = x_0 - \left(\delta/10^{14} - \left\lfloor \delta/10^{14} \right\rfloor\right) \Big/ 10^2. \quad (3)$$

where δ denotes the sum of all the pixels of the plain image, x_0 is the initial value given as a key, x_0' is the modified result.

Step 2 The intertwining chaotic system has been used to generate the chaotic sequences, we can get three sequences $(u_1 u_2 \ldots u_{MN})$, $(v_1 v_2 \ldots v_{MN})$ and $(w_1 w_2 \ldots w_{MN})$ by using the chaotic system (1) and the initial value x_0'.

Step 3 Preparatory work, the initial setup:

Step 3.1 Convert the original image P into a one-dimensional sequence $p_1 p_2 \ldots p_{MN}$. k denotes the pointer of p_i, $k = 1$.

Step 3.2 Initialize the scrambling image D, for $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$, $D(i, j) = -1$. -1 means that there is no scrambled result stored here.

Step 3.3 Initialize the "chessboard" Cb which the Langton's Ant will crawl. We used two chaotic sequences $(u_1 u_2 \ldots u_{MN})$, $(v_1 v_2 \ldots v_{MN})$ generated by step 2 and reshape them to two-dimensional sequences (u_{ij} and v_{ij}) where $i = 1, 2, \ldots, M$, $j = 1, 2, \ldots, N$, if $u(i, j) > v(i, j)$, then $Cb(i, j) = 1$. Otherwise $Cb(i, j) = 0$. Here, 0 denotes the black box and 1 for the white.

Step 3.4 Initialize the starting coordinates i_{start}, j_{start} and direction d for the Langton's Ant. d is in the range of (0, 1, 2, 3), 0 for the upward direction, 1 for the right, 2 for the down, 3 for the left.

Step 3.5 Generate the random collection $s_1 s_2 \ldots s_{MN}$ of variable steps with the chaotic sequence $w_1 w_2 \ldots w_{MN}$ and Eq. (4).

$$s_i = \left(w_i \times 10^{14}\right) \bmod 4, \quad 3 \geq s_i \geq 0. \quad (4)$$

Step 4 The Langton's Ant crawls from the starting coordinates $i = i_{start}$, $j = j_{start}$ with the direction d for $M \times N$ steps.

(1) If $Cb(i, j) = 1$, then $Cb(i, j) = 0$. Otherwise $Cb(i, j) = 1$.
(2) If $D(i, j) = -1$, then $D(i, j) = p_k$, $k = k + 1$.
(3) The coordinates i, j and the direction d should be modified to ensure that the ant is in the range of the Cb according to the turning and moving rules (showed as in Table 1).

Step 5 We put the remaining pixels of the original image into the scrambling image.

Step 6 We use one piecewise linear chaotic map to diffuse.

$$\begin{cases} b_i = F(b_{i-1}, \eta) \\ d_i = (b_i \times 10^{14}) \bmod 256 \\ c_i = p_i \oplus d_i \oplus c_{i-1} \end{cases}. \quad (5)$$

where $i \in (1, 2, \ldots, MN)$, c_0 is a given value provided as a key. F means PWLCM map, b_0 is the PWLCM map's initial value (given in advance and $b_0 > 0.1$) and η is the parameter. p_i is the i-th pixel of the permuted image with the scanning order from left to right and up to down, c_i is the encrypted value of p_i.

4 Experiment

This paper conducted several experiments on multiple images, the images we have used are Lena. bmp, boat. bmp and peppers. bmp of size 512 × 512, all the

Table 1 The turning and moving rules

		d	i	j
$Cb(i, j) = 0$	$d = 0$	1	$i = \text{mod}(i + 1 + s_r, M)$	j
	$d = 1$	2	i	$j = \text{mod}(j + 1 + s_r, N)$
	$d = 2$	3	$i = \text{mod}(i - 1 + s_r, M)$	j
	$d = 3$	0	i	$j = \text{mod}(j - 1 + s_r, N)$
$Cb(i, j) = 1$	$d = 0$	3	$i = \text{mod}(i - 1 + s_r, M)$	j
	$d = 1$	0	i	$j = \text{mod}(j - 1 + s_r, N)$
	$d = 2$	1	$i = \text{mod}(i + 1 + s_r, M)$	j
	$d = 3$	2	i	$j = \text{mod}(j + 1 + s_r, N)$

experiments run on Matlab 2013a (64 bit), the configuration of our experimental machine are Microsoft Windows 7 operation system, 2.2 GHZ CPU, 4 GB memory. Table 2 shows the keys we adopted. Figures 2a, 3a and 4a show three plain images, Figs. 2b, 3b and 4b show the scrambled result, Figs. 2c, 3c and 4c are the cipher images.

Table 2 The key used in our scheme

Key name	Value	Meaning
x_0	0.36	The initial value of intertwining logistic map
y_0	0.25	
z_0	0.78	
k_1	35.5	The parameter of intertwining logistic map
k_2	38.2	
k_3	36	
μ	1.5	
b_0	0.2	The initial value of PWLCM map
η	0.3	The parameter of PWLCM
c_0	100	A given value to diffuse

5 Security analysis

5.1 Key space analysis

To make the key space large enough is necessary and important for an encryption algorithm. Its main significance is to make the brute-force attacks computationally infeasible, which has been a basic common sense. This paper utilize two chaotic systems, especially the intertwining logistic map, which have multiple initial values and parameters. All of that can make key space large enough. The keys we employed are showed in Table 2: the initial values and parameters x_0, y_0, z_0, μ, k_1, k_2, k_3 of the intertwining logistic map, b_0, η of PWLCM map. The ciphered image can be decrypted unless we know x_0, y_0, z_0, μ within error 10^{-16} and k_1, k_2, k_3 within error 10^{-15}, b_0 within error 10^{-16}, η within error 10^{-16}, the key space is larger than 10^{141}. So it is obvious that the key space is large enough to resist the brute-force attack.

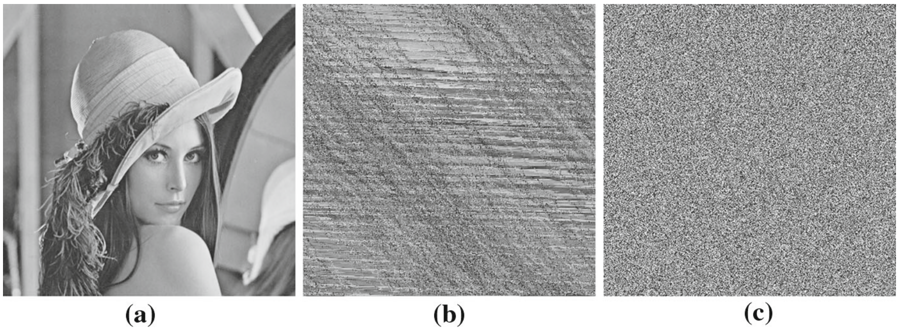

Fig. 2 Experimental result of lena.bmp. **a** Original image, **b** scrambled image, **c** encrypted image

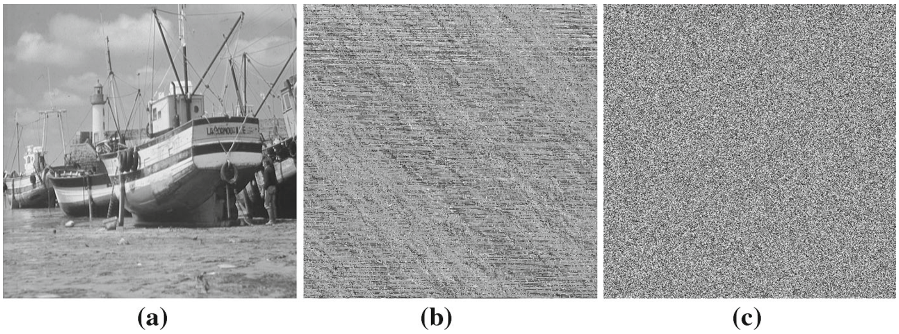

Fig. 3 Experimental result of boat.bmp. **a** Original image, **b** scrambled image, **c** encrypted image

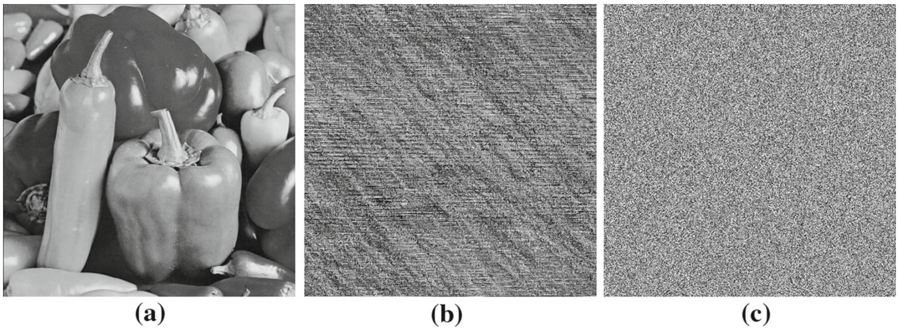

Fig. 4 Experimental result of peppers.bmp. **a** Original image, **b** scrambled image, **c** encrypted image

5.2 Statistical analysis

Statistical analysis attack is a traditional measure to crack, which is useful for some classical encryption. A good encryption algorithm should make the cipher image confusing enough so that an attacker cannot get any useful information from a statistical point of view. This requires the algorithm has good randomness, and chaos can be a nice choice to meet that. Here, we elaborate statistical analysis from three indicators: the histograms, correlations of two adjacent pixels and the information entropy.

5.2.1 Histograms of corresponding images

We can obtain a visual impression of statistics from histograms. Generally, the histogram of the plain image will be clear statistically significant, which exposed some characteristic features of the image. After encrypted, these features should not be obtained. Cipher text should show non-obvious features and be almost statistically equal for the 256 gray-scale image. Figure 5 shows the histograms of the original and encrypted image of lena.bmp. We can see that the histogram has been much uniform after encrypted.

5.2.2 Correlations of two adjacent pixels

There is an expressly strong correlation between the pixels of the plain image, which is a reflection of its features. So in the cipher text, these correlations should be weakened. The paper randomly chose 1,000 pairs of pixels separately in horizontal, vertical and diagonal direction from the image lena.bmp and calculate the coefficients as follows:

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

where

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

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

where, x and y stand for the gray-scale values of two adjacent pixels;

Table 3 shows the correlation coefficients of two adjacent pixels in three directions, the coefficients of the original image is almost to 1, after encrypted, they

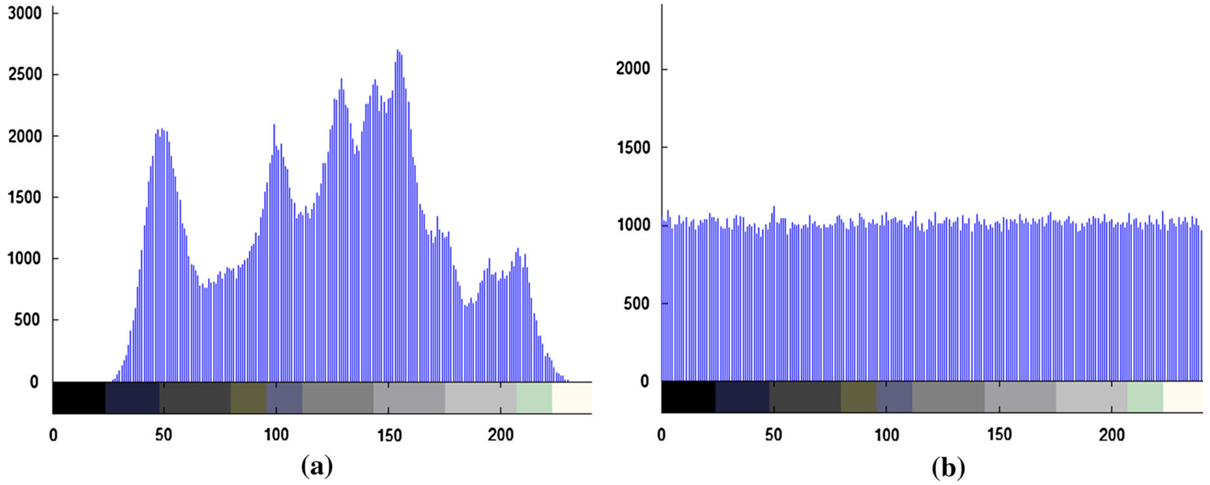

Fig. 5 Histograms analysis. **a** Histogram of original image, **b** histogram of ciphered image

Table 3 The correlation coefficients of two adjacent pixels in three directions

Directions	Original image	Cipher image
Horizontal	0.973928780957292	0.001270468595904
Vertical	0.984469820084225	0.001694253624902
Diagonal	0.960657093678514	−0.001541295546719

have been cut down to nearly 0. Figure 6 gives the correlation of two horizontally adjacent pixels. So this paper has remarkable achievements.

5.2.3 Information entropy

Information entropy is a very important concept in information theory, it can describe the degree of disorder of a system. As we have said in front, the cipher text should be confusing enough to resist the statistical analysis attack. Here, we can use the information entropy to calculate, the more the entropy is to 8, the more confusing the cipher text is.

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i)\log_2 \frac{1}{p(s_i)}, \tag{7}$$

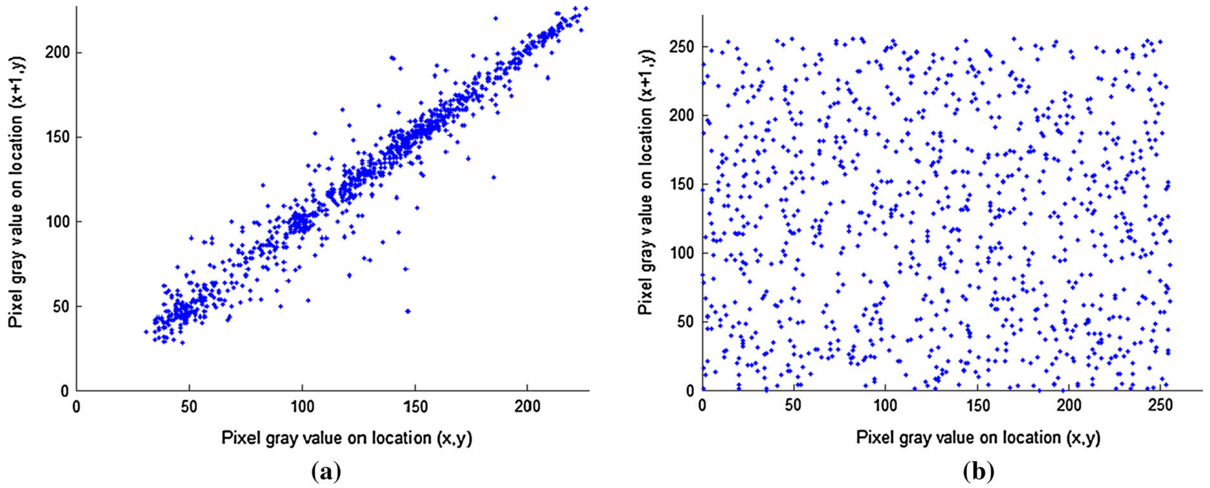

Fig. 6 Correlation of two horizontally adjacent pixels. **a** Correlation of original image, **b** correlation of ciphered image

Table 4 Information entropies

Test image	Original image	Cipher image
Lena.bmp (512 × 512)	7.445567570340059	7.999317955870737
Boat.bmp (512 × 512)	7.191370218069238	7.999296628450773
Peppers.bmp (512 × 512)	7.571477564161731	7.999297667485719

where $p(s_i)$ denotes the probability of symbol s_i.

Table 4 gives the information entropies of three images. After encrypted, we can see that the information entropies have been enlarged and almost to 8, which means the cipher text is confusing enough.

5.3 Sensitivity analysis

In order to find clues to crack, attackers often observe changes in the cipher text by making small changes to the keys or plaintext. That requires our algorithm must be sensitive to the key and the plaintext. When tiny change of the plaintext or key occur, the cipher text should be able to vary greatly, so do not let the attacker succeeded.

5.3.1 Key sensitivity

We decrypt the ciphered image Fig. 2c using $b_0 = 0.25 + 10^{-16}$ with other keys the same, Fig. 7b shows the image which has been decrypted by the wrong key, while Fig. 7a gives the right result.

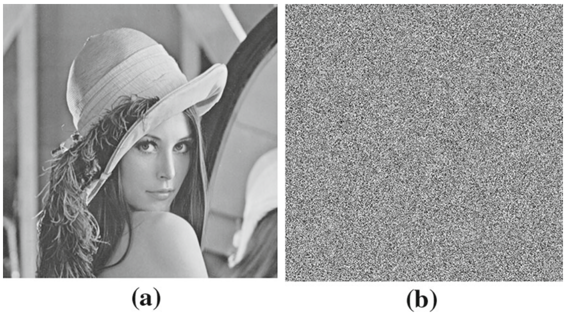

Fig. 7 Sensitivity analysis. **a** Decrypted with correct key, **b** decrypted with wrong key

5.3.2 Plaintext sensitivity

In order to cope with the differential attack, when a slight change of plaintext happen, cipher text should change greatly, so that the attacker cannot obtain any meaningful association between the plaintext and cipher text. Here are the formulas to calculate NPCR (number of pixels change rate) and UACI (unified average changing intensity) according to Eqs. (8) and (9).

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100, \tag{8}$$

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100, \tag{9}$$

where c_1 and c_2 are two images with the same size $W \times H$. If $c_1(i,j) \neq c_2(i,j)$, then $D(i,j) = 1$, otherwise, $D(i,j) = 0$.

Table 5 gives the mean NPCR and UACI of ciphered images when there is one bit different between the plain images. After encrypted, almost all the pixels of the test images have been changed. It is clear that the disparity between the corresponding pixels became larger. So the algorithm is sensitive to the plaintext.

Table 5 The mean NPCR and UACI of ciphered images with one bit different between the plain images

Test image	NPCR (%)	UACI (%)
Lena.bmp (512 × 512)	99.6307373046875	33.5663978726360
Boat.bmp (512 × 512)	99.6128082275391	33.4661745557705
Peppers.bmp(512 × 512)	99.6196746826172	33.4530415254591

6 Conclusion

This paper proposes an encryption algorithm using Langton's Ant cellular automaton to scramble and chaos to diffuse. The main idea is to combine the two-dimensional structural characteristics of the image with the "chessboard" Langton's Ant crawls on. According to the result of each step of the automaton, we can get the scrambled image gradually. In order to increase the randomness, the paper made change to the cellular automaton by using the chaos map to generate steps with random length. Experimental results and analysis show that the tested indicators of our algorithm are good, it is able to resist common attacks. In practice, our algorithm does not have rigid requirements for image itself and no overly complex logic design and is easy to understand and use. In conclusion, the proposed scheme is secure and practical.

Acknowledgments This research is supported by the National Natural Science Foundation of China (Nos. 61370145, 61173183, and 60973152), the Doctoral Program Foundation of Institution of Higher Education 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. Xiao, H.J., Qiu, S.S., Deng, C.L.: Image encryption scheme based on AES and chaotic series encryption. Comput. Eng. **33**(23), 154–155 (2007)
2. Alfalou, A., Brosseau, C.: Optical image compression and encryption methods. Adv. Opt. Photonics **1**(3), 589–636 (2009)
3. Maniccam, S.S., Bourbakis, N.G.: Lossless image compression and encryption using SCAN. Pattern Recognit. **34**(6), 1229–1245 (2007)
4. Yang, H.Q., Liao, X.F., Wong, K.W.: SPIHT-based joint image compression and encryption. Acta Phys. Sin. **61**(4), 040505 (2012)
5. Zhu, H.G., Zhao, C., Zhang, X.D.: A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. Signal Process. Image Commun. **28**(6), 670–680 (2013)
6. Kanso, A., Ghebleh, M.: A novel image encryption algorithm based on a 3D chaotic map. Commun. Nonlinear Sci. Numer. Simul. **17**(7), 2943–2959 (2012)
7. Gao, T.G., Chen, Z.Q.: A new image encryption algorithm based on hyper-chaos. Phys. Lett. A **372**(4), 394–400 (2008)
8. Patidar, V., Pareek, N.K., Sud, K.K.: A new substitution diffusion based image cipher using chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simul. **14**(7), 3056–3075 (2009)
9. Sun, F.Y., Liu, S.T., Li, Z.Q.: A novel image encryption scheme based on spatial chaos map. Chaos Solitons Fractals **38**(3), 631–640 (2008)
10. Singh, N., Sinha, A.: Optical image encryption using fractional Fourier transform and chaos. Opt. Lasers Eng. **46**(2), 117–123 (2008)
11. Wang, J., Jiang, G.P.: Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version. Acta Phys. Sin. **60**(6), 060503 (2011)
12. Wang, X.Y., He, G.X.: Cryptanalysis on an image block encryption algorithm based on spatiotemporal chaos. Chin. Phys. B **21**(6), 060502 (2012)
13. Liu, J.M., Qiu, S.S., Liu, W.P.: Cryptanalysis of image encryption algorithm based on hyper-chaotic system. Appl. Res. Comput. **27**(3), 1042–1044 (2010)
14. Ozkaynak, F., Ozer, A.B., Yavuz, S.: Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun. **285**(24), 4946–4948 (2012)
15. Li, C.Q., Zhang, D., Chen, G.R.: Cryptanalysis of an image encryption scheme based on the Hill Cipher. J. Zhejiang Univ. Sci. A **9**(8), 1118–1123 (2008)
16. Wang, X.Y., Liu, L.T.: Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos. Nonlinear Dyn. **73**(1–2), 795–800 (2013)
17. Wikipedia. http://en.wikipedia.org/wiki/Cellular_automaton
18. Wikipedia. http://en.wikipedia.org/wiki/Langton%27s_ant.s
19. Shatheesh, S.I., Devaraj, P., Bhuvaneswaran, R.S.: An intertwining chaotic maps based image encryption scheme. Nonlinear Dyn. **69**(4), 1995–2007 (2012)
20. Huang, X.L., Ye, G.D.: An efficient self-adaptive model for chaotic image encryption algorithm. Commun. Nonlinear Sci. Numer. Simul. **19**(12), 4094–4104 (2014)
21. Zhu, H.G., Zhao, C.: A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. Signal Proces. Image Commun. **28**(6), 670–680 (2013)
22. Zhang, X.P., Zhao, Z.M.: Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dyn. **75**(1–2), 319–330 (2014)