Optics and Lasers in Engineering 82 (2016) 79–86

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

A novel color image encryption scheme using alternate chaotic mapping structure

Xingyuan Wang *, Yuanyuan Zhao, Huili Zhang, Kang Guo

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

ARTICLE INFO

Article history:
Received 14 April 2015
Received in revised form
18 December 2015
Accepted 18 December 2015

Keywords:
Image encryption
Chaotic
Color image
Alternate structure

ABSTRACT

This paper proposes an color image encryption algorithm using alternate chaotic mapping structure. Initially, we use the R, G and B components to form a matrix. Then one-dimension logistic and two-dimension logistic mapping is used to generate a chaotic matrix, then iterate two chaotic mappings alternately to permute the matrix. For every iteration, XOR operation is adopted to encrypt plain-image matrix, then make further transformation to diffuse the matrix. At last, the encrypted color image is obtained from the confused matrix. Theoretical analysis and experimental results has proved the cryptosystem is secure and practical, and it is suitable for encrypting color images.

1. Introduction

Along with the rapid development in digital image processing and network communication, information security has become increasingly important [1,2], and frequent Internet application has increased the requirement for security [3]. Chaos is a definitive and similar random procedure which appears in a nonlinear system [4,5]. In recent years, chaotic cryptography is a new research that aims at designing encryption algorithm, many cryptographic protocols have emerged in the scientific literature [6]. Chaotic systems have a lot of traits such as ergodicity, sensitivity to initial conditions, random-like behaviors, topological transitivity. These properties are very important for confusion and diffusion processes [7–9]. Therefore, encryption algorithms based on chaotic map are widely applied in cryptography fields. Britain mathematician Matthes [10] is the first one who adopted chaos theory to explore encryption technology. Since then, more and more researchers proposed lots of chaos-based encryption schemes.

Up to now, many chaos-based image encryption algorithms have been proposed [11–19], including algorithms for gray-level image [11–15] and algorithms for color image [16–19]. However, some of them have been proved insecure. The most serious problem in individual chaotic systems is that their chaotic dynamic properties degrade rapidly when they are realized with finite precision. Although some measures have been proposed to deal with such degradation of digital chaotic systems, such as increasing computing precision [20], cascading multiple chaotic systems [21], perturbing the chaotic systems [22] and switching multiple chaotic systems [23], but there should be more simple and effective measures for image encryption.

As for color image, each pixel value for the color image is composed of R, G and B components, each component directly determines the intensity of red, green or blue color. Because color images provide more information than gray-level images, they have attracted more and more attentions [24–26]. But most algorithms for color images used the same method to encrypt three components. They neglected the correlations between R, G, B components. To enhance the correlation between three components, this paper proposes a novel color image encryption algorithm based on chaos. One-dimension logistic and two-dimension logistic chaotic mapping are used to encrypt the color image, which make the three components affect each other and reduce the correlations between R, G and B components effectively, thus enhance the performance of encryption.

The remaining of the paper is organized as follows. In Section 2, the encryption algorithm is described. Section 3 provides simulation results and security analysis. Finally, this paper is concluded in Section 4.

2. Color image encryption algorithm

2.1. Logistic chaotic mapping

Two-dimension logistic chaotic map [27] and one-dimension logistic [28] can be defined as follows:

$$\begin{cases} x_{i+1} = x_i u_1 (1 - x_i) + \lambda_1 y_i^2 \\ y_{i+1} = y_i u_2 (1 - y_i) + \lambda_2 (x_i^2 + x_i y_i) \end{cases}, \quad (1)$$

* Corresponding author. Tel.: +86 0411 84707827
E-mail addresses: wangxy@dlut.edu.cn (X. Wang), yuanyuanzhao0319@126.com (Y. Zhao), zhanghui7873@foxmail.com (H. Zhang).

http://dx.doi.org/10.1016/j.optlaseng.2015.12.006
0143-8166/

$$z_{i+1} = uz_i(1-z_i), \tag{2}$$

where $2.75 < u_1 \le 3.4$, $2.75 < u_2 \le 3.45$, $0.15 < \lambda_1 \le 0.21, 3.56 < u \le 4$, $0.13 < \lambda_2 \le 0.15$, x_i, y_i, $z_i \in (0,1)$, the system works under a chaotic state. The complexity of the logistic map is low (almost zero) when the parameter u is within the range [3.82,3.85]. We can see that the parameter u is close to 4 [29–30]. The coefficients $u,u_1,u_2,\lambda_1,\lambda_2$ and the initial values of the iteration x_0,y_0,z_0 can be served as the keys for image encryption, which makes the key space very large.

2.2. Encryption process

Assume that the size of the color plain-image f is $M \times N$. Convert f into its R, G and B component matrix denoted as f^r f^g and f^b; the size of each component matrix is $M \times N$, and the pixel values range from 0 to 255. $f_k^r(k \in [0, M \times N-1])$ denotes the kth pixel of f^r; $f_k^g(k \in [0, M \times N-1])$ denotes the kth pixel of f^g; $f_k^b(k \in [0, M \times N-1])$ denotes the kth pixel of f^b

Step 1. Use the R, G and B component matrices $f^r f^g f^b$ to get the matrix B with size of $3 \times (M \times N)$.

${f_0}^r$	${f_1}^r$	$f_{M\times N-1}^r$
${f_0}^g$	${f_1}^g$	$f_{M\times N-1}^g$
${f_0}^b$	${f_1}^b$	$f_{M\times N-1}^b$

Step 2. $\varepsilon_1,\varepsilon_2,\varepsilon_3$ is determined by the color plain-image f.

$$\varepsilon_1 = \sum_{i \in [0, M\times N-1]} f_i^g/(M \times N \times 255) \tag{3}$$

$$\varepsilon_2 = \sum_{i \in [0, M\times N-1]} f_i^b/(M \times N \times 255) \tag{4}$$

$$\varepsilon_3 = + \sum_{i \in [0, M\times N-1]} f_i^r/(M \times N \times 255) \tag{5}$$

For different color plain-images, our proposed scheme have different secret keys $\varepsilon_1,\varepsilon_2$ and ε_3, so it could resist plaintext attack effectively. Then make transform for $\varepsilon_1,\varepsilon_2,\varepsilon_3$ to obtain

$$a = \left\lfloor \mathrm{mod}((\varepsilon_1+\varepsilon_2+\varepsilon_3) \times 10^{12}, 256) \right\rfloor, \tag{6}$$

$$b = \left\lfloor \mathrm{mod}(\frac{\varepsilon_1+\varepsilon_2+\varepsilon_3}{2} \times 10^{12}, 256) \right\rfloor, \tag{7}$$

$$c = \left\lfloor \mathrm{mod}(\frac{\varepsilon_1+\varepsilon_2+\varepsilon_3}{3} \times 10^{12}, 256) \right\rfloor. \tag{8}$$

Step 3. Iterate the Eqs. (1) and (2) $M \times N$ times by using u, u_1, u_2, λ_1, λ_2, x_0, y_0, z_0, three variables x_i,y_i,z_i can be got for each iteration.

$$m_1 = (x_k \times 10^{15}) \bmod 256. \tag{9}$$

$$m_2 = (y_k \times 10^{15}) \bmod 256. \tag{10}$$

$$m_3 = (z_k \times 10^{15}) \bmod 256. \tag{11}$$

$$S_k = \begin{cases} a-m_1, m_1 < a \\ m_1-a, m_1 > a \\ a, m_1 = a \end{cases}, \quad x_k = \begin{cases} (a-m_1)/256, m_1 < a \\ (m_1-a)/256, m_1 > a \\ a/256, m_1 = a \end{cases}, \tag{12}$$

$$S_{k+M\times N} = \begin{cases} b-m_2, m_2 < b \\ m_2-b, m_2 > b \\ b, m_2 = b \end{cases}, \quad y_k = \begin{cases} (b-m_2)/256, m_2 < b \\ (m_2-b)/256, m_2 > b \\ b/256, m_2 = b \end{cases}, \tag{13}$$

$$S_{k+M\times N\times 2} = \begin{cases} c-m_2, m_3 < c \\ m_3-c, m_3 > c \\ c, m_3 = c \end{cases}, \quad z_k = \begin{cases} (c-m_3)/256, m_3 < c \\ (m_3-c)/256, m_3 > c \\ c/256, m_3 = c \end{cases}, \tag{14}$$

S_k is the kth number of random matrix S(the size of $3 \times (M \times N)$), $k \in [1, M \times N]$, so the matrix S(the length is $3 \times (M \times N)$) can be got.

Step 4. Continue iterating Eqs. (1) and (2) alternately.

(1) Suppose $j(j \in [1, M \times N])$ denotes the iteration times, initially, $j = 1$.

(2) Firstly iterate Eq. (1) with $u_1,u_2,\lambda_1,\lambda_2,x_0,y_0$. For the jth iteration, x_j, $y_j$can be got, then make further transform:

$$t_1 = \mathrm{mod}(x_j \times 10^{15}, M \times N) \tag{15}$$

$$t_2 = \mathrm{mod}(y_j \times 10^{15}, M \times N) \tag{16}$$

$$t_3 = \mathrm{mod}((x_j+y_j - \lfloor x_j+y_j \rfloor) \times 10^{15}, M \times N) \tag{17}$$

$$z_0 = \mathrm{mod}(x_j+y_j, 1) \tag{18}$$

(3) Transform matrix S:

$$S(1,:) = cirshift(S(1,:), t_1). \tag{19}$$

$$S(2,:) = cirshift(S(2,:), t_2). \tag{20}$$

$$S(3,:) = cirshift(S(3,:), t_3). \tag{21}$$

$cirshift(e,r)$ denotes the right cyclic shift $r$bits operation for e.

(4) Encrypt matrix B with XOR operation.

$$G(:,j) = S(:,j) \oplus B(:,j). \tag{22}$$

G, S and B are represented in their binary format. Then $j=j+1$ and make sure whether the iteration times is enough or not. If $j = M \times N$, then go to step 5.

(5) Continue iterating Eq. (2) using u, z_0. Then we can obtain z_j:

$$t_1 = \mathrm{mod}(z_j \times 10^{15}, M \times N). \tag{23}$$

$$t_2 = \mathrm{mod}((1-z_j) \times 10^{15}, M \times N). \tag{24}$$

$$t_3 = \lfloor (t_1+t_2+c)/2 \rfloor. \tag{25}$$

$$x_0 = \mathrm{mod}(z_j+y_{j-1}, 1). \tag{26}$$

$$y_0 = \mathrm{mod}(z_j+x_{j-1}+y_{j-1}, 1) \tag{27}$$

$\lfloor x \rfloor$ means the max integer less than x or equal to x. Then go to step4.(c) and step4.(d). After transformation, then go to step4 (a) and process the subsequent encryption.

Step 5. Diffuse the gray value by Eq. (28) to obtain the finaltext C.

$$C(x,z) = (G(x,z)+C(x,z-1)) \bmod 256, \quad z \in [2, M \times N] \tag{28}$$

where $C(x,1) = G(x,1)$, $x \in \{1,2,3\}$,$C(x,z)$ denotes the gray value after transformation, and $C(x,z-1)$ denotes the previous gray value after transformation, $G(x,z)$ is current gray value which being processed.

3. Simulation results and security analysis

3.1. Simulation results

We used MATLAB 7.6.0 to run programs. The simulation results are shown in Figs. 1 and 2. The 170×170 color image "Lena" (Fig. 1(a)) is used as the plain image. Fig. 1(b)–(d) shows its R, G and B components respectively. The secret keys are set as follows: $u = 3.9989$, $u_1 = 3.399$, $u_2 = 3.4499$, $\lambda_1 = 0.21$,$\lambda_2 = 0.15$,$x_0 = 0.345$,$y_0 = 0.365$,$z_0 = 0.537$. Encrypted color image is shown in Fig. 2(a)–(d) shows the R, G and B components of the encrypted color image respectively.

3.2. Key space

The key space size characterizes the capability of resisting brute-force attack. In our algorithm, u, u_1, u_2, λ_1, λ_2, x_0, y_0, z_0, ε_1, ε_2, ε_3 are used as the secret keys. If the precision is 10^{-15}, the key space is almost 10^{165}, and the complexity of brute-force is great, so the key space is large enough for common applications to resist brute-force attack.

3.3. Distribution

The histogram of an image shows the distribution of pixel values. If it is not flat enough, certain amount of information can be guessed by the statistical attack opponents. This makes cipher-only attack easy by analyzing the statistic property of ciphered image.

Fig. 3 illustrates the histograms of the color plain-image "Lena". Fig. 3(a) shows histogram of the R component; Fig. 3(b) shows histogram of the G component; Fig. 3(c) shows histogram of the B component. As shown in Fig. 3, histograms of the plain-image are not flat.

Fig. 4 illustrates the histograms of the encrypted color image of "Lena". Fig. 4(a) shows histogram of the R component; (b) shows histogram of the G component; (c) shows histogram of the B component. It is clear from Fig. 4 that the proposed algorithm results in the flat distributions and statistical attack is not effective to our algorithm.

3.4. Information entropy

The information entropy is a method to test uncertainty, namely, entropy reflects whether the distribution of gray-scale values is random or not [31]. The coarser the image is, the larger the entropy is. In contrary, more smoother the picture is, smaller the entropy is. The minimum entropy is zero while the maximum entropy is 8. That is, higher the value of entropy of encrypted image is, better the security will be. The formula for calculating information entropy is defined as [32]:

$$H(k) = -\sum_{j=1}^{2^N-1} P(k_j)\log_2 P(k_j). \tag{29}$$

here $P(k_j)$ represents the probability of symbol. When the probability is the same, the information entropy of the ciphered image should be close to 8 after encryption. The more it gets close to 8, the less possible to divulge information. Information entropies of the R, G and B components of the encrypted color image of "Lena" are listed in Table 1. From the table, test results based on the proposed algorithm are close to the ideal value 8. We can conclude that the encrypted image obtained by the proposed algorithm could hardly divulge information.

3.5. Correlation

Ciphered images should get rid of the drawback of high correlation between pixels. In order to test the correlations between two adjacent pixels by the proposed encryption method, we randomly select 1000 pairs of adjacent pixels in each direction from the R, G and B components of the encrypted color image of "Lena". Then calculate the correlation coefficient of each pair by Eq. (30), respectively, and the test results are listed in Table 2.

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{30}$$

where

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

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

From Table 2, correlation coefficients for the R, G and B components of the encrypted color image are all smaller than 0.01, which indicates a negligible correlation between adjacent pixels. It can be concluded that the proposed algorithm possesses high security against statistical attacks.

Moreover, we plot the correlation distributions of the R, G and B components of "Lena" and its encrypted color image in each direction, as illustrated in Figs. 5 and 6. Fig. 5(a)–(c) shows correlation distributions of the R component of "Lena" in each direction, Fig. 5(d)–(f) shows correlation distributions of the G component of "Lena" in each direction, Fig. 5(g)–(i) shows correlation distributions of the B component of "Lena" in each direction, Fig. 6(a)–(c) shows correlation distributions of the R component of the encrypted color image in each direction, Fig. 6(d)–(f) shows

Fig. 1. (a) Color plain-image "Lena" , (b) R component for plain-color image (a); (c) G component for plain color image (a); and (d) B component for plain color image (a). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

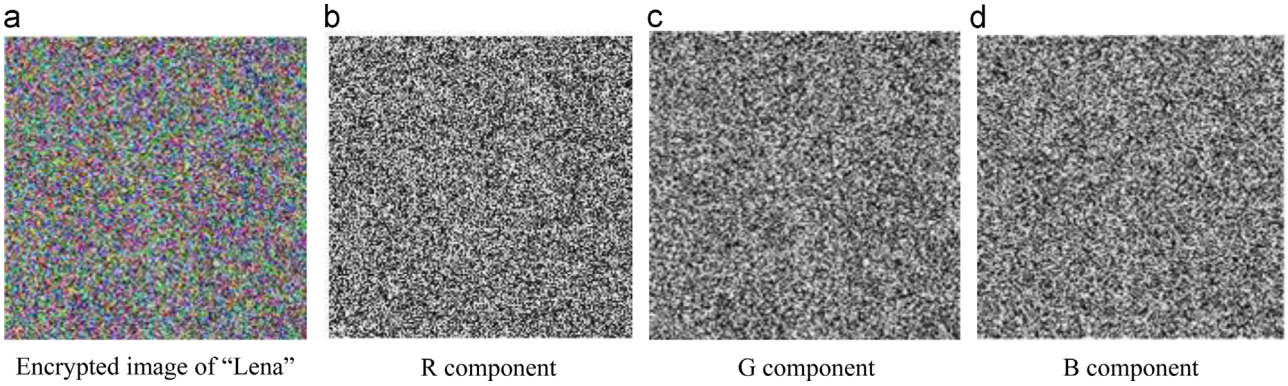

Fig. 2. (a) Encrypted color image 'Lena'; (b) R component for encrypted color image (a); (c) G component for encrypted color image (a); and (d) B component for encrypted color image (a).(For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

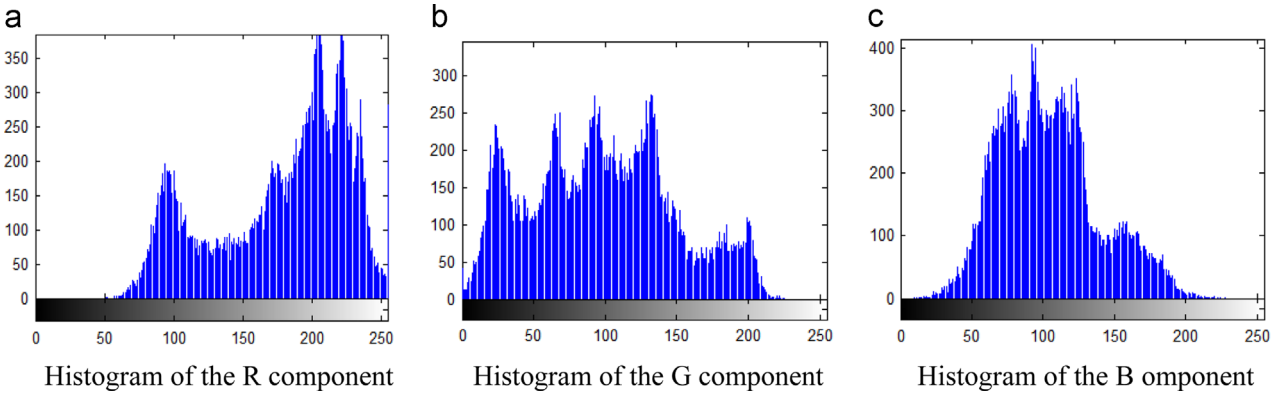

Fig. 3. (a) R component histogram for plain image; (b) G component histogram for plain image; and (c) B component histogram for plain image. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

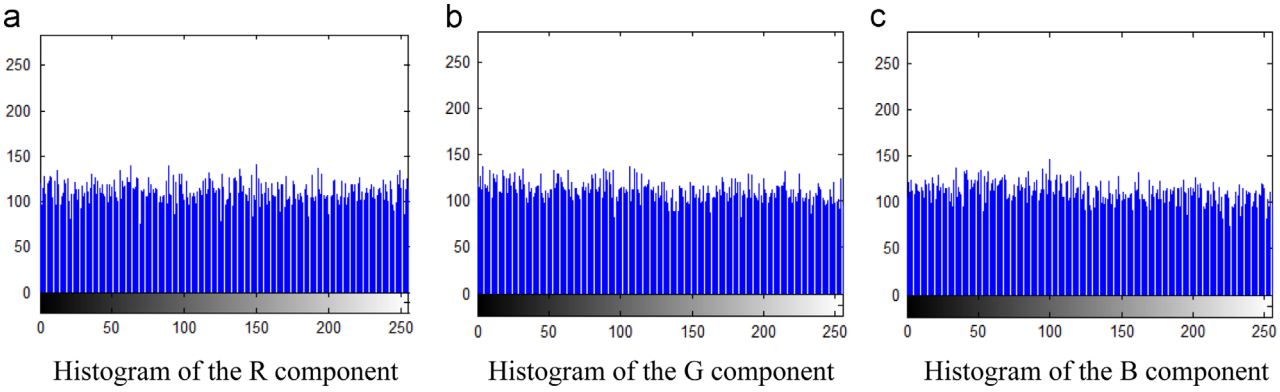

Fig. 4. Histograms of the R, G, B components of the encrypted color image of "Lena".

Table 1
Information entropies of the R, G and B components of the encrypted color image of "Lena".

Component	Information entropy
R component	7.9926
G component	7.9934
B component	7.9923

Table 2
Correlation coefficients of the R, G and B components of the encrypted color image of "Lena".

Component	Horizontal	Vertical	Diagonal
R component	0.0018	0.0016	0.0005
G component	0.0004	0.0021	−0.0007
B component	0.0029	0.0011	0.0037

correlation distributions of the G component of the encrypted color image in each direction, Fig. 6(g)–(i) shows correlation distributions of the B component of the encrypted color image in each direction. The strong correlation between adjacent pixels of the plain image is evident as the dots are congregated along the diagonal in Fig. 5. However, the dots are scattered over the entire

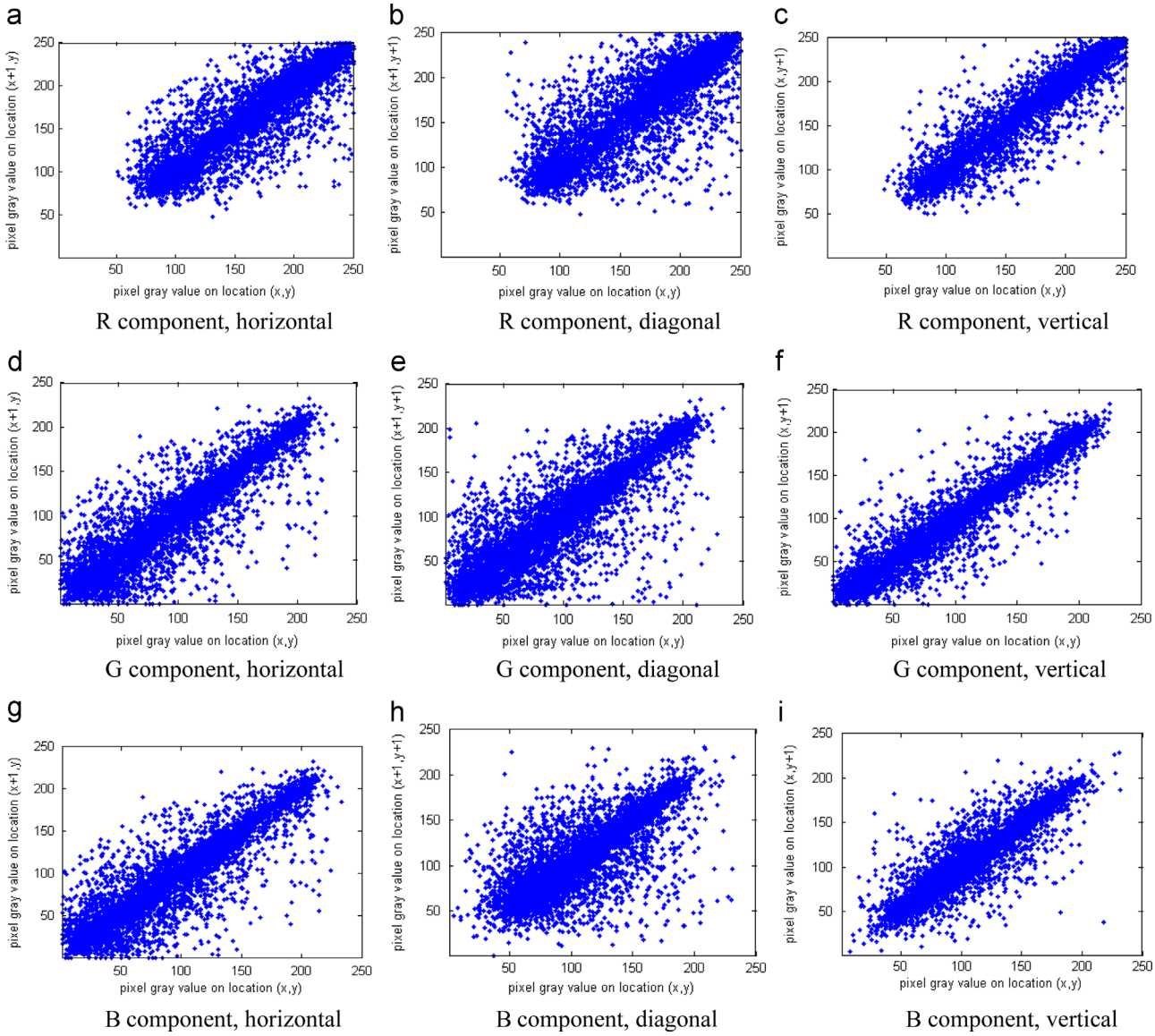

Fig. 5. Correlation distributions of "Lena" in each direction.

plane in Fig. 6, which indicates that the correlation is greatly reduced in the encrypted image.

3.6. NPCR and UACI

NPCR (Number of Pixels Change Rate) stands for the number of pixels change rate while one pixel of plain image changed. And UACI (Unified Average Changing Intensity) represents the average intensity of differences between the plain image and ciphered image. If NPCR gets more close to 100%, which indicates the cryptosystem is more sensitive to the alteration of plain image and it is helpful to resist plaintext attack, while UACI gets more close to 33.33%, which denotes the capability of resisting differential attack of the cryptosystem is better, according to Eqs. (31) and (32):

$$\mathrm{NPCR} = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100\%, \tag{31}$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%, \tag{32}$$

where W and H represent the width and height of the image, respectively, C_1 and C_2 are the ciphered image before and after one pixel of the plain image is changed. For the pixel at position $(i,\ j)$, if $C_1(i,j) \neq C_2(i,j)$, then $D(i,j) = 1$; else $D(i,j) = 0$. NPCR and UACI of R, G and B components of "Lena" are listed in Table 3. The results show that the proposed algorithm could resist plaintext attack and differential attack effectively.

3.7. Sensitivity

An excellent cryptosystem should be sensitive to the secret keys as well as the plaintext. Taking secret key x_0 for example, sensitivity test on the R component of "Lena" is performed. Fig. 7 (a) shows the cipher-image when x_0 is changed from 0.345 to

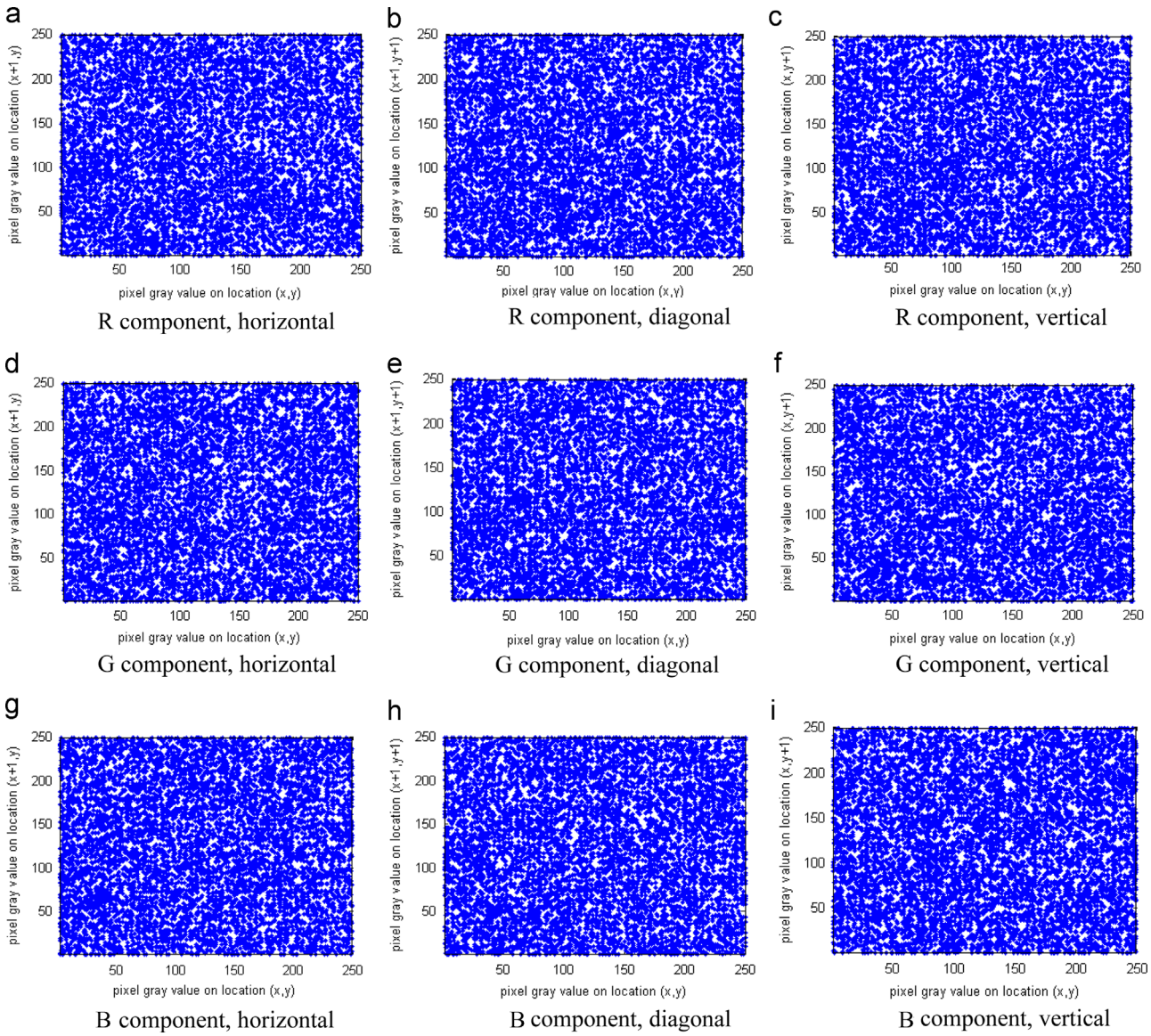

Fig. 6. Correlation distributions of the encrypted color image in each direction. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 3
NPCR and UACI of R, G and B components of "Lena".

Component	NPCR	UACI
R component	99.63%	33.43%
G component	99.59%	33.39%
B component	99.67%	33.51%

0.345000000001 while the other keys are the same. So it can be concluded that the proposed scheme is sensitive to the secret keys. Fig. 7(b) shows the cipher-image when 1 bit of the pixel data of the R component of "Lena" is changed, so it can be concluded that the proposed scheme is sensitive to the plaintext. A tiny change in the plain image leads to dramatic changes in the ciphered image. The high sensitivity to plaintext ensures the cryptosystem could resist plaintext attack. Fig. 8 shows the histograms of Fig. 7 in different situations. It is clear from Fig. 8 that the proposed algorithm results in very flat distributions.

4. Conclusion

In this paper, a color image encryption algorithm is proposed. Firstly, we use the R, G and B components of the color plain-image to obtain a matrix. Then one-dimension and two-dimension logistic chaotic mapping are adopted to generate a matrix. The one-dimension logistic chaotic mapping and two-dimension logistic chaotic mapping are employed to permute the matrix generated by them. Last, XOR operation is used to encrypt plain image. The proposed scheme is quite simple, so it is easy to implement. Many experiments are performed to test the security performance, the simulation results and theoretical analysis show that the scheme is able to resist differential attack, brute-force

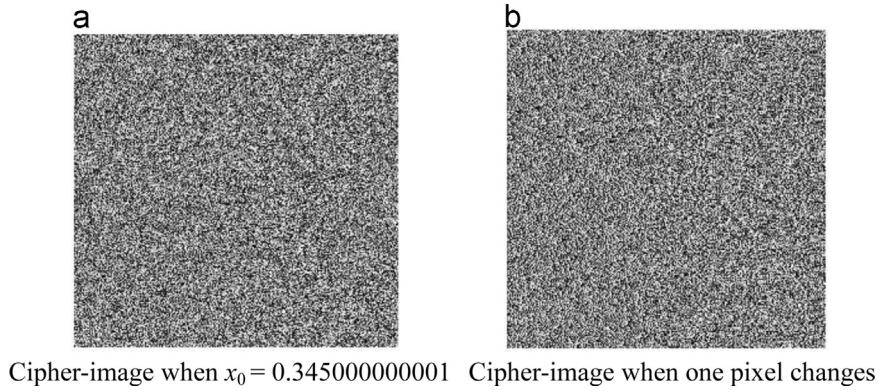

Fig. 7. Sensitivity tests.

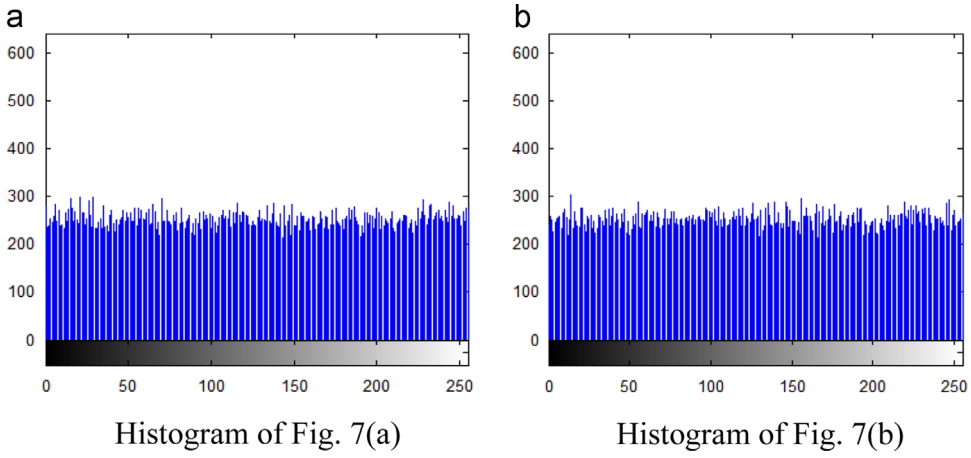

Fig. 8. Histograms of Fig. 7 in different situations.

attack, statistical attack and plaintext attack, so it has high security. It is expected to attract more researchers in this field.

Acknowledgment

This research is supported by the National Natural Science Foundation of China, 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] Gao TG, Chen ZQ. Image encryption based on a new total shuffling algorithm. Chaos Solitons Fractals 2008;38(1):213–20.
[2] Pisarchik AN, Zanin M. Image encryption with chaotically coupled chaotic maps. Phys Lett A 2008;237(20):2645–52.
[3] Chen WM, Lai CJ, Wang HC, Chao HC, Lo CH. H.264 video watermarking with secret image sharing. IET Image Process 2011;5(4):349–54.
[4] Deng Y, Hu H, Xiong N, et al. A general hybrid model for chaos robust synchronization and degradation reduction. Inf Sci 2015;305:146–64.
[5] Deng Y, Hu H, Xiong W, et al. Analysis and design of digital chaotic systems with desirable performance via feedback control. IEEE Trans Syst Man Cybern Syst 2015;99:1–14.
[6] Zhang W, Wong K W, Yu H, Zhu Z L. An image encryption scheme using reverse 2-dimensional chaotic map and depen 066-2080.
[7] Yang HQ, Wong KW, Liao XF, Zhang W, Wei PC. A fast image encryption and authentication scheme based on chaotic maps. Commun Nonlinear Sci Numer Simul 2010;15(11):3507–17.
[8] Hu H, Deng Y, Liu L. Counteracting the dynamical degradation of digital chaos via hybrid control. Commun Nonlinear Sci Numer Simul 2014;19(6):1970–84.
[9] Hu H, Xu Y, Zhu Z. A method of improving the properties of digital chaotic system. Chaos Solitons Fractals 2008;38(2):439–46.
[10] Matthes R. On the derivation of a Chaotic Encryption algorithm. Cryptologia 1989;13(1):29–42.
[11] Wang XY, Teng L. An image blocks encryption algorithm based on spatio-temporal chaos. Nonlinear Dynamics 2012;67(1):365–71.
[12] Bigdeli N, Farid Y, Afshar K. A novel image encryption/decryption scheme based on chaotic neural networks. Eng Appl Artif Intell 2012;25(4):753–65.
[13] Xu L, Li Z, Li J, Hua W. A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 2016;78:17–25.
[14] Ren XX, Liao XF, Xiong YH. New image encryption algorithm based on cellular neural network. J Comput Appl 2011;31(6):1528–30.
[15] Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2010;62(3):615–21.
[16] Wang L, Song H, Liu P. A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt Lasers Eng 2016;77:118–25.
[17] Sui L, Liu B, Wang Q, Li Y, Liang J. Color image encryption by using Yang-Gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional Sine logistic modulation map. Opt Lasers Eng 2015;75:17–26.
[18] Liu HJ, Wang XY. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59(10):3320–7.
[19] Abuturab MR. An asymmetric single-channel color image encryption based on Hartley transform and gyrator transform. Opt Lasers Eng 2015;69:49–57.
[20] Wheeler DD, Matthews R. Supercomputer investigations of a chaotic encryption algorithm. Cryptologia 1991;15:140–51.
[21] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos 2006;16:2129–51.
[22] Li CY, Chen YH, Chang TY, Deng LY, To K. Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. IEEE Trans VLSI Syst 2012;20:385–9.
[23] Nagaraj N, Shastry MC, Vaidya PG. Increasing average period lengths by switching of robust chaos maps in finite precision. Eur Phys J Spec Top 2008;165:73–83.

[24] Madhusudan J, Chandra Shakher, Kehar S. Color image encryption and decryption for twin images in fractional Fourier domain. Opt Commun 2008;8(23):5713–20.
[25] Guo Q, Liu ZG, Liu ST. Color image encryption by using Arnold and discrete fractional random transforms in IHS space. Optd Lasers Eng 2010;48(12):1174–1181.
[26] Tay CJ, Quan C, Chen W, Fu Y. Color image encryption based on interference and virtual optics. Opt Laser Technol 2010;42(2):409–15.
[27] Zhang XQ, Zhu GL, Ma SL. Remote-sensing image encryption in hybrid domains. Opt Commun 2012;285(7):1736–43.
[28] Gao F, Li XH. Bitmap encryption study based on chaotic sequences. Trans Beijing Inst Technol 2005;25(5):447–50.
[29] Wu X, Hu H, Zhang B. Parameter estimation only from the symbolic sequences generated by chaos system. Chaos Solitons Fractals 2004;22(2):359–66.
[30] Liu L, Hu H, Deng Y, et al. An entropy measure of non-stationary processes. Entropy 2014;16(3):1493–500.
[31] Hu H, Liu L, Ding N. Pseudorandom sequence generator based on the Chen chaotic system. Compu Phys Commun 2013;184(3):765–8.
[32] Liu L, Miao S, Hu H, et al. On the eigenvalue and Shannon's entropy of finite length random sequences. Complexity 2014. http://dx.doi.org/10.1002/cplx.21587.