Optics and Lasers in Engineering 86 (2016) 248–254

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

An enhanced sub-image encryption method

Xing-Yuan Wang [a,*], Ying-Qian Zhang [b,*], Lin-Tao Liu [a]

[a] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[b] City Institute, Dalian University of Technology, Dalian 116600, China

ARTICLE INFO

Article history:
Received 22 August 2015
Received in revised form
7 June 2016
Accepted 7 June 2016

Keywords:
High-dimensional chaos system
Enhanced method
Sub-image encryption
Parallel algorithm

ABSTRACT

Recently a parallel sub-image encryption method is proposed by Mirzaei et al., which is based on a total shuffling and parallel encryption algorithm. In this paper, we firstly show that the method can be attacked by chosen plaintext attack and then propose an enhanced sub-image algorithm, which can completely resist the chosen plaintext attack. Moreover, our improved algorithm can reduce the encryption time dramatically. The experimental results also prove that the improved encryption algorithm is secure enough. So the improved method can be used in image transmission system.

1. Introduction

With the rapid development of network communication, more and more private information need to be transmitted through Internet. However, it is threatening that the information transmitted on the Internet can be intercepted, tampered and destroyed illegally. Among all the information transmitted on Internet, the number of image files keeps increasing. So, the secure transmission of images has become more significant and image encryptions has attracted scholars in both research and application fields. Due to some intrinsic features of images such as bulk data capacity and high correlation among pixels, traditional encryption methods like DES, IDEA and RSA are not suitable for image encryptions. Since chaotic systems have the features of non-periodicity, non-convergence, ergodicity and sensitiveness on initial conditions, chaos-based encryption algorithms that rely on these features have been regarded as a promising research for image encryptions.

The classic encryption architecture is the permutation-diffusion pattern suggested by Shannon and the chaos-based encryption was first proposed by Matthews in 1989 [1]. In the past decade, various chaotic systems [2–4] and chaotic cryptology methods [5–28] are proposed including logistic map [29], Lorenz system [30], Chen system [31] and Arnold cat map or generalized cat map in the permutation section [32]. Therefore, many chaotic encryption schemes have been proposed and obtained excellent results [33–44]. But due to fatal drawbacks of short periodic and frangibility of resisting chosen plaintext attack, cat map is not secure for directly applications [7,8]. The solely XOR operation designed in some other proposed image encryption schemes [9–12] on the original. or scrambling images are not secure because the key stream only depends on the key not the plaintext. Therefore, it is easy to be cracked by chosen plaintext attack [13,14]. According to the encryption schemes [15–20] and there corresponding analyses [21–23], these schemes have the same fatal drawback: in the diffusion phase, the pixel values are changed in the static order from top to bottom and from left to right which reveals important information of the encryption method to the attackers. Most of the cryptanalyses of image encryption algorithms indicate that attackers always successfully cracked cryptosystems by using the order from top to bottom and from left to right. In addition, small key space of single chaotic map is another risk in security. For example, when employing logistic map in the cryptosystem, the parameter must be very close to 4 for generating an idea randomness. Thus, the key space is small not to resist the attack of brute-force.

Recently, a parallel sub-image encryption algorithm is proposed [24]. However, there are some fatal flaws: division of plain-image into sub-images and the sub-images shuffling before the total shuffling process has no use at all; the total shuffling process is not safe; in the diffusion process, the order changing the pixel values is in the fixed sequence. To overcome these defects, we propose an improved algorithm which can resist the chosen plaintext attack completely and reduce the encryption time dramatically. The contributions of the work are that we propose dynamical pixel order for diffusion and sub-images division method, which depends on secret key only; therefore, the proposed scheme is sensitive to the keys.

This paper is organized as follows. Section 2 gives the brief of

* Corresponding authors.
E-mail addresses: wangxy@dlut.edu.cn (X.-Y. Wang), zhangyq@dlut.edu.cn (Y.-Q. Zhang).

http://dx.doi.org/10.1016/j.optlaseng.2016.06.008
0143-8166/

the original algorithm. Section 3 shows the flaws of the original scheme. Section 4 shows the improved sub-image encryption scheme in detail. Section 5 presents the computer simulation results. Section 6 discusses the security analyses. Finally, Section 7 is the conclusions of this paper.

2. The original algorithm in brief

In the sub-image encryption algorithm proposed by Ref. [24], permutation–diffusion architecture is employed. For permutation process, the original algorithm employs Logistic chaotic map in division of plain-image to calculate "Random ***A***" and obtain sub-images before to calculate total shuffling matrix for image permutations.

Logistic chaotic map can be described as following, which is proved to be chaotic by Ref. [29]:

$$x_{n+1} = 4x_n(1 - x_n). \tag{1}$$

Although the logistic map has some drawbacks [42–44] such as periodic windows in the bifurcation diagrams in the range of $\mu \in [3.4, 3.9]$, the parameter $\mu = 4$ in the logistic map has good dynamical behaviors [36–38]. Therefore, the logistic map is feasible for encryptions when $\mu = 4$.

Lorenz system [30] is often described by:

$$\begin{cases} \dot{x}_1 = p(x_2 - x_1) \\ \dot{x}_2 = -x_1x_3 + rx_1 - x_2, \\ \dot{x}_3 = x_1x_2 - tx_3 \end{cases} \tag{2}$$

where p, r and t are parameters, and when p=10, r=28 and t=8/3.

The third system is Chen's system [31]:

$$\begin{cases} \dot{x}_4 = a(x_5 - x_4) \\ \dot{x}_5 = (c - a)x_4 - x_4x_6 + cx_5, \\ \dot{x}_6 = x_4x_5 - bx_6 \end{cases} \tag{3}$$

where a, b and c are parameters, and when a=35, b=3 and c=28.

Lorenz system and Chen's system are employed to calculate $\{B_{x_i}, i = 1, 2, 3, 4\}$ detailed in Ref. [24], for the diffusion process [24]:

$$\begin{aligned} C_{i,j}^{4k+1} &= (B_{i,j}^{4k+1} \oplus B_{x_1}) \oplus C_{i+M/2,j+N/2}^{4k} \\ C_{i,j+N/2}^{4k+2} &= (B_{i,j+N/2}^{4k+2} \oplus B_{x_2}) \oplus C_{i,j}^{4k+1} \\ C_{i+M/2,j}^{4k+3} &= (B_{i+M/2,j}^{4k+3} \oplus B_{x_3}) \oplus C_{i,j+N/2}^{4k+2} \\ C_{i+M/2,j+N/2}^{4k+4} &= (B_{i+M/2,j+N/2}^{4k+4} \oplus B_{x_4}) \oplus C_{i+M/2,j}^{4k+3}, \end{aligned} \tag{4}$$

where $\oplus$ represents the exclusive OR operation bit-by-bit. $C_{i,j}^{4k+m}(m=1\text{–}4)$ represents the ciphered pixel value in (i, j)-pixel of m sub-image. k represents the ($k-1$)th iteration of the two chaotic systems detailed in Ref. [24]. $B_{i,j}^{4k+m}(m=1\text{–}4)$ represents the plaintext pixel value in (i, j)-pixel of m sub-image.

3. Flaws of the original algorithm

Although sub-image encryption algorithm proposed by [24] has many good encryption effects, there are three fatal flaws in the encryption process as follows:

(1) Division of plain-image into sub-images and the shuffle of sub-images before the total shuffling process solely depend on logistic map.

(2) The total shuffling process solely depends on logistic map.

(3) In the diffusion process, the order changing the pixel values is in sequence without concerning values of the plaintext image.

According to the Kerckhoffs's principle [32], when cryptanalyzing a cryptosystem, a general assumption is that cryptanalyst can acquire the information on the design and working of the studied cryptosystem, i.e., for any researcher, he/she can know everything about the cryptosystem except the secret keys for the encryption and decryption. This criterion is a basic standard for any encryption system in nowadays' secure communications networks.

Following the operations to sub-images transformed from Eq. (4), we obtains corresponding part of sequence $\{B_{x_i}\}$:

$$\begin{aligned} B_{x_1} &= (C_{i,j}^{4k+1} \oplus C_{i+M/2,j+N/2}^{4k}) \oplus B_{i,j}^{4k+1} \\ B_{x_2} &= (C_{i,j+N/2}^{4k+2} \oplus C_{i,j}^{4k+1}) \oplus B_{i,j+N/2}^{4k+2} \\ B_{x_3} &= (C_{i+M/2,j}^{4k+3} \oplus C_{i,j+N/2}^{4k+2}) \oplus B_{i+M/2,j}^{4k+3} \\ B_{x_4} &= (C_{i+M/2,j+N/2}^{4k+4} \oplus C_{i+M/2,j}^{4k+3}) \oplus B_{i+M/2,j+N/2}^{4k+4}, \end{aligned} \tag{5}$$

where $i = (M/2) + 1, \ldots, M$; $j = (N/2) + 1, \ldots, N$. When choosing the image with all pixel values of zero. The permutation process is transparent and invalid. Therefore, we can get the corresponding part of sequence $\{B_{x_i}\}$ which is one of the equivalent secret keys.

For "Random ***A***", there are 4!=24 kinds of assignment, which can be cracked by brute-force attacks. Without loss of generality, we assign that the "Random ***A***" array is {1, 4, 2, 3}; $\boldsymbol{P}_2$ is the chosen plaintext image for calculating the column transformation permutation matrix; $\boldsymbol{P}_3$is the chosen plaintext image for calculating the row transformation permutation matrix.

$$\boldsymbol{P}_2 = \begin{pmatrix} \boldsymbol{E} & \boldsymbol{E} \\ \boldsymbol{F} & \boldsymbol{F} \end{pmatrix}_{M\times N}, \quad \boldsymbol{P}_3 = \begin{pmatrix} \boldsymbol{G} & \boldsymbol{H} \\ \boldsymbol{G} & \boldsymbol{H} \end{pmatrix}_{M\times N},$$

where

$$\boldsymbol{E} = \begin{pmatrix} 1 & 2 & \cdots & N/2 \\ 1 & 2 & \cdots & N/2 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \cdots & N/2 \end{pmatrix}_{M/2\times N/2}, \quad \boldsymbol{F} = \begin{pmatrix} N/2+1 & N/2+2 & \cdots & N \\ N/2+1 & N/2+2 & \cdots & N \\ \vdots & \vdots & \ddots & \vdots \\ N/2+1 & N/2+2 & \cdots & N \end{pmatrix}_{M/2\times N/2},$$

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ M/2 & M/2 & \cdots & M/2 \end{pmatrix}_{M/2\times N/2},$$

$$\boldsymbol{H} = \begin{pmatrix} M/2+1 & M/2+1 & \cdots & M/2+1 \\ M/2+2 & M/2+2 & \cdots & M/2+2 \\ \vdots & \vdots & \ddots & \vdots \\ M & M & \cdots & M \end{pmatrix}_{M/2\times N/2}.$$

When divided of plain-image into sub-images, the $\boldsymbol{P}_2$ and $\boldsymbol{P}_3$ can be changed into $\boldsymbol{P}'_2$ and $\boldsymbol{P}'_3$:

$$\boldsymbol{P}'_2 = \begin{pmatrix} 1 & 2 & \cdots & N \\ 1 & 2 & \cdots & N \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & \cdots & N \end{pmatrix}_{M\times N}, \quad \boldsymbol{P}'_3 = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ \vdots & \vdots & \ddots & \vdots \\ M & M & \cdots & M \end{pmatrix}_{M\times N}$$

After encrypted by the original algorithm for $\boldsymbol{P}_2$ and $\boldsymbol{P}_3$ respectively, the corresponding ciphered images are obtained. Since the sequence $\{B_{x_i}\}$ is obtained, the permuted images of $\boldsymbol{P}_2$ and $\boldsymbol{P}_3$ can be recovery, noted as $\boldsymbol{P}_2^h$ and $\boldsymbol{P}_3^h$ respectively. The total row shuffling permutation is invalid for $\boldsymbol{P}'_2$ because entire rows are identical. Therefore, the column permutation matrix can be recovery by $\boldsymbol{P}_2^h$. The same reason can also be used for recovery of the row permutation matrix by $\boldsymbol{P}_3^h$. Thus, row transformation and column transformation matrixes are obtained, which are equivalent keys.

Although the secret keys are unknown, we can find the equivalent keys by chosen plaintext attack. Therefore, the original algorithm can be cracked according to the Kerckhoffs's principle. The equivalent keys in the original algorithm are sequence $\{B_{x_i}\}$, row transformation and column transformation matrixes.

4. The improved encryption method

To overcome these three defects, we improves the sub-image encryption method to make it possible to resist the chosen plaintext attack. The detailed encryption process is described by following:

(1) Using logistic chaotic map and initial condition x_0, divide the plaintext image into four sub-images, follow the total shuffling according to Ref. [24] to the four sub-images respectively. Then conduct the total shuffling to the whole image.
(2) Shuffle the sub-images using the current x_0 and logistic chaotic map according to Ref. [24].
(3) The diffusion process is almost the same as in Ref. [24] except for the order changing the pixel value. Every four times of iterations the logistic map uses another initial value x_{00} to generate a pseudo-random array as Ref. [24]. The pseudo-random array determines the order of changing pixels. For example, if we obtain a pseudo-random array of $\{3, 1, 4, 2\}$, we change the corresponding pixel in the order of sub-image 3, sub-image 1, sub-image 4 and sub-image 2.

5. Experimental results

We execute the encryption and decryption programs by Microsoft Visual C++6.0 on computer with Intel Core i7 CPU, 4 GB memory and Microsoft Windows 7 operation system. In Fig. 1, we show the encryption and decryption results of Lena.bmp and Baboon.bmp of size (256×256). The keys we select are: $x_0 = 0.123456$, $x_{00} = 0.7654321$, $x_1 = 0.3$, $x_2 = -0.4$, $x_3 = 1.2$, $x_4 = 10.2$, $x_5 = -3.5$, $x_6 = 4.4$, $N_0 = 500$, $M_0 = 500$. From Fig. 1 (b) and (e), we can see that the improved sub-image encryption method has good secret effect.

6. Security analysis

A good encryption scheme should be able to resist known plaintext attack, chosen plaintext attack, cipher image only attack and chosen cipher image attack. Therefore, we develop the corresponding experiments such as large key space, uniform distribution of cipher pixels, information entropy close to 8 and sensitive to both the key and plaintext images.

6.1. Key space analysis

In our improved sub-image encryption method, two logistic maps, Lorenz chaotic system and Chen's system are used. The initial values of these systems are the keys. Since all the initial values are float types with the precision of 2^{-32}, the key space is 2^{256}. Moreover, N_0, M_0 are also the keys. Thus, the key space in the improved algorithm is larger than that in the original algorithm

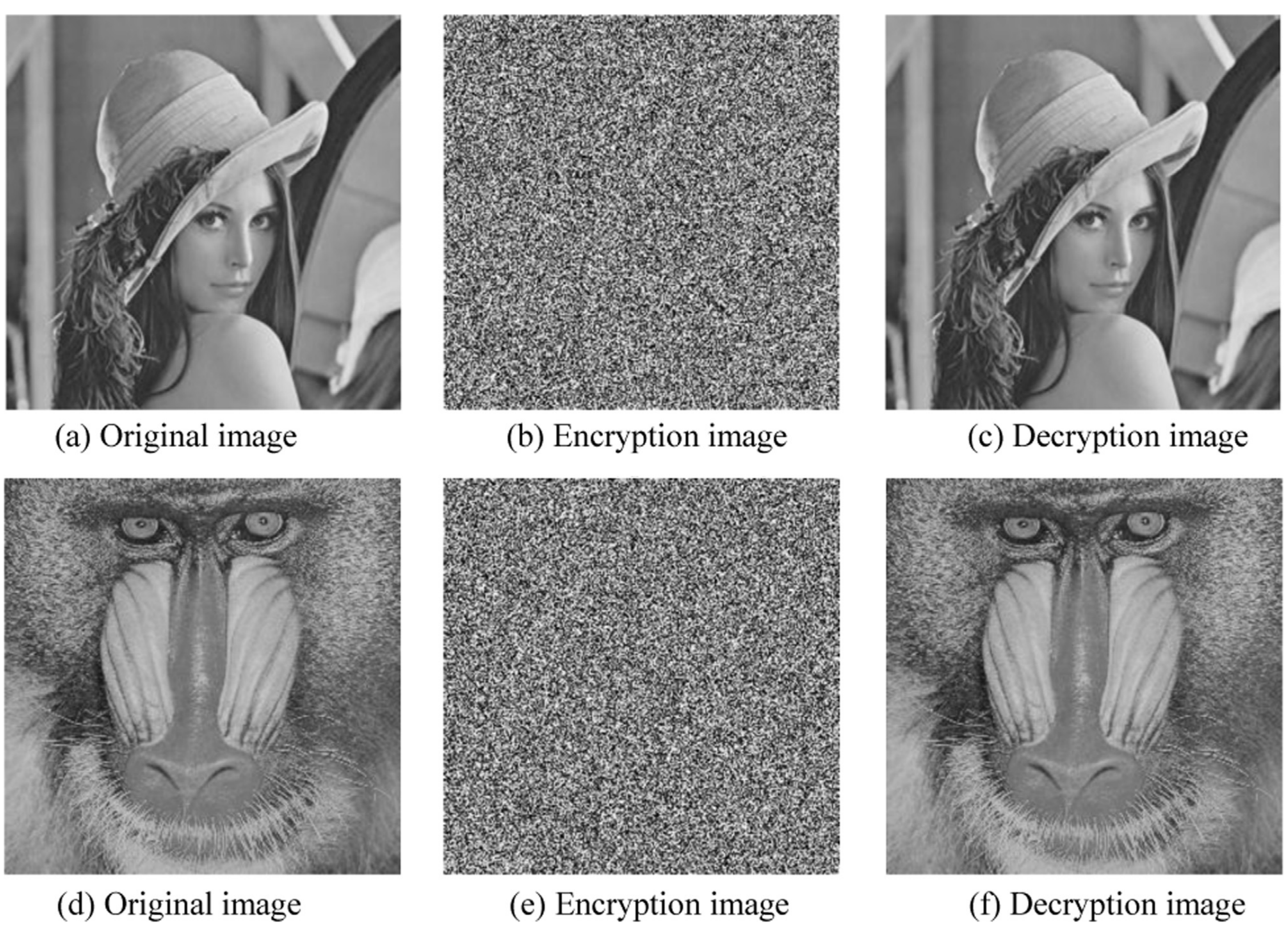


Fig. 1. Encryption and decryption results.

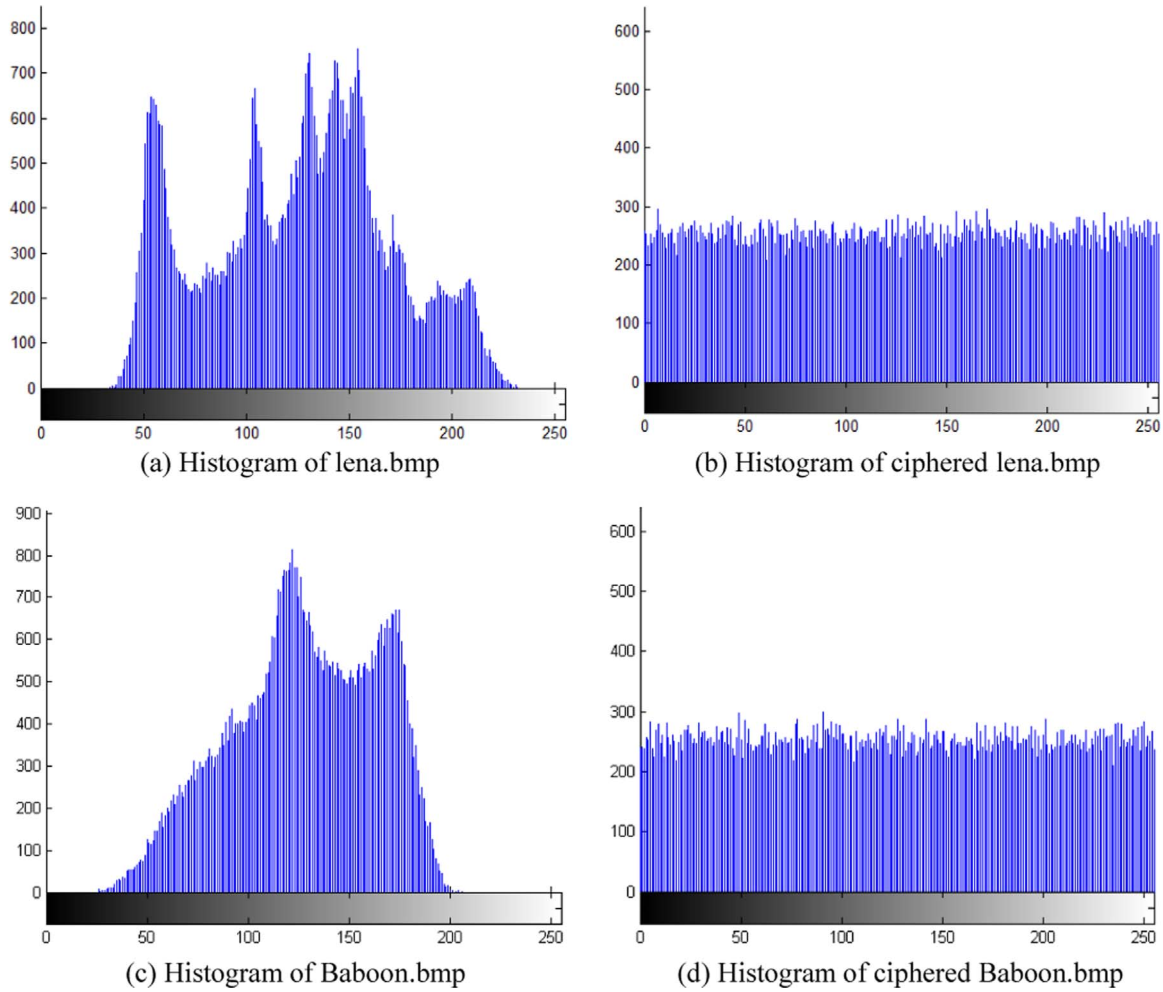


Fig. 2. Histograms analysis.

after employing keys of x_0 and x_{00}.

6.2. Statistical analysis

For statistical analysis, the histogram of the ciphered image, correlations of adjacent pixels in the ciphered image and information entropy of the ciphered image are calculated in our improved algorithm.

(1) Histograms of Corresponding images

An image-histogram illustrates how pixels are distributed by the number of pixels at each color intensity level. Histograms of the original 256 Gy-scale image Lena.bmp (256×256) and Baboon.bmp (256×256) with their corresponding ciphered images are shown in Fig. 2. Fig. 2(b) and (d) indicate that the histogram of the ciphered images are fairly uniformly distributed, which is important for resisting statistical analysis attack.

(2) Correlations of two adjacent pixels
Ciphered image should eliminate the high correlation between pixels. For calculating the correlations between two adjacent pixels, we randomly select 1000 pairs of two-adjacent pixels from plaintext and ciphered image in vertical, horizontal and diagonal direction respectively. Then calculate the correlation coefficient of each pair by Eq. (5).

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

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

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

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i, \tag{5}$$

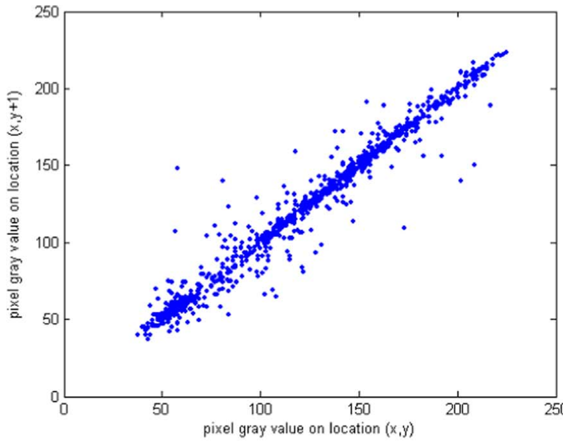
where x and y are gray values of two adjacent pixels in an image. The correlation of horizontally, vertically and diagonally adjacent pixels of Lena.bmp with size (256×256) are also show in Fig. 3. The correlation coefficients are presented in Table 1. Both Fig. 3 and Table 1 indicate that the correlation the ciphered images are lower.

(3) Information entropy analysis

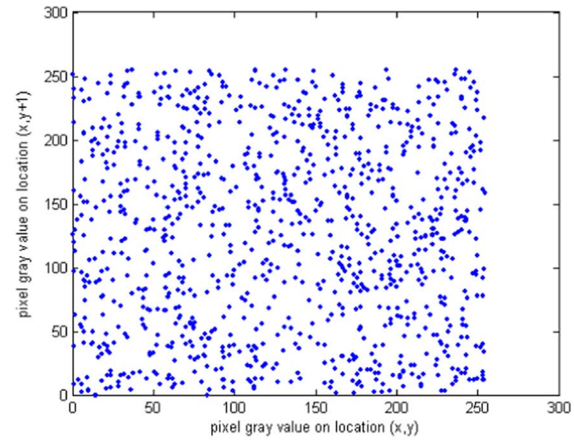
The information entropy is a measure of the uncertainty of randomness which can be calculated by Eq. (6):

$$H(s) = \sum_{i=0}^{2^{N-1}} p(s_i)\log_2\frac{1}{p(s_i)}, \tag{6}$$

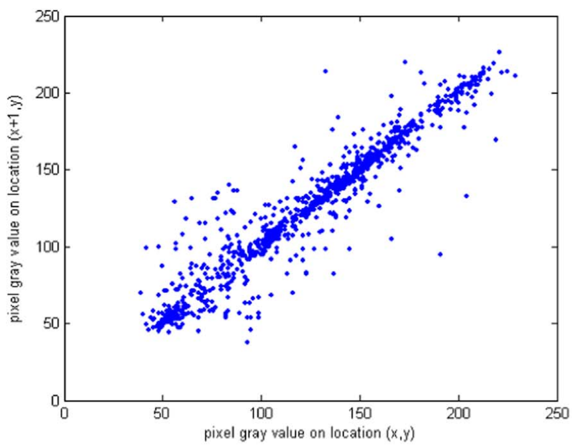
where $p(s_i)$ denotes the probability of symbol s_i. When a random source producing 2^L symbols, the entropy should be L. Take 256-gray-scale image for an instance, the entropy of the image must be



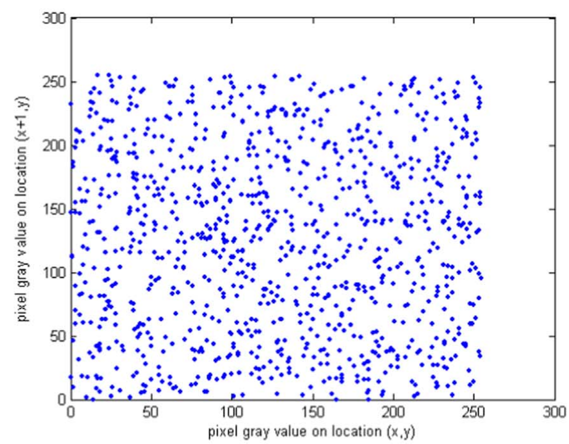
(a) Vertical correlation of original image



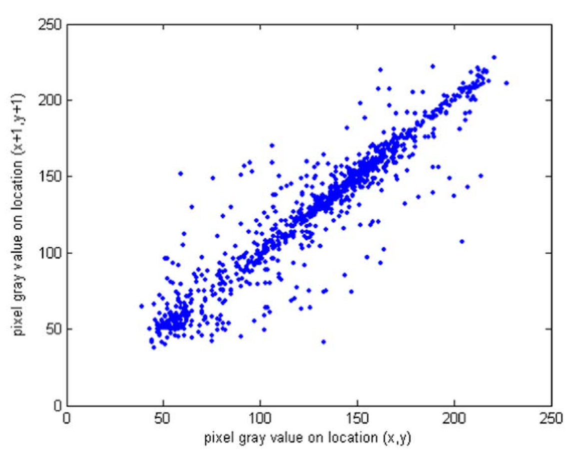
(b) Vertical correlation of ciphered image



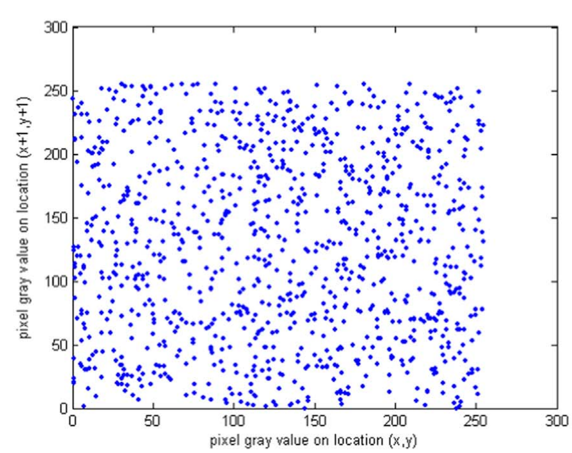
(c) Horizontal correlation of original image



(d) Horizontal correlation of ciphered image



(e) Diagonal correlation of original image



(f) Diagonal correlation of ciphered image

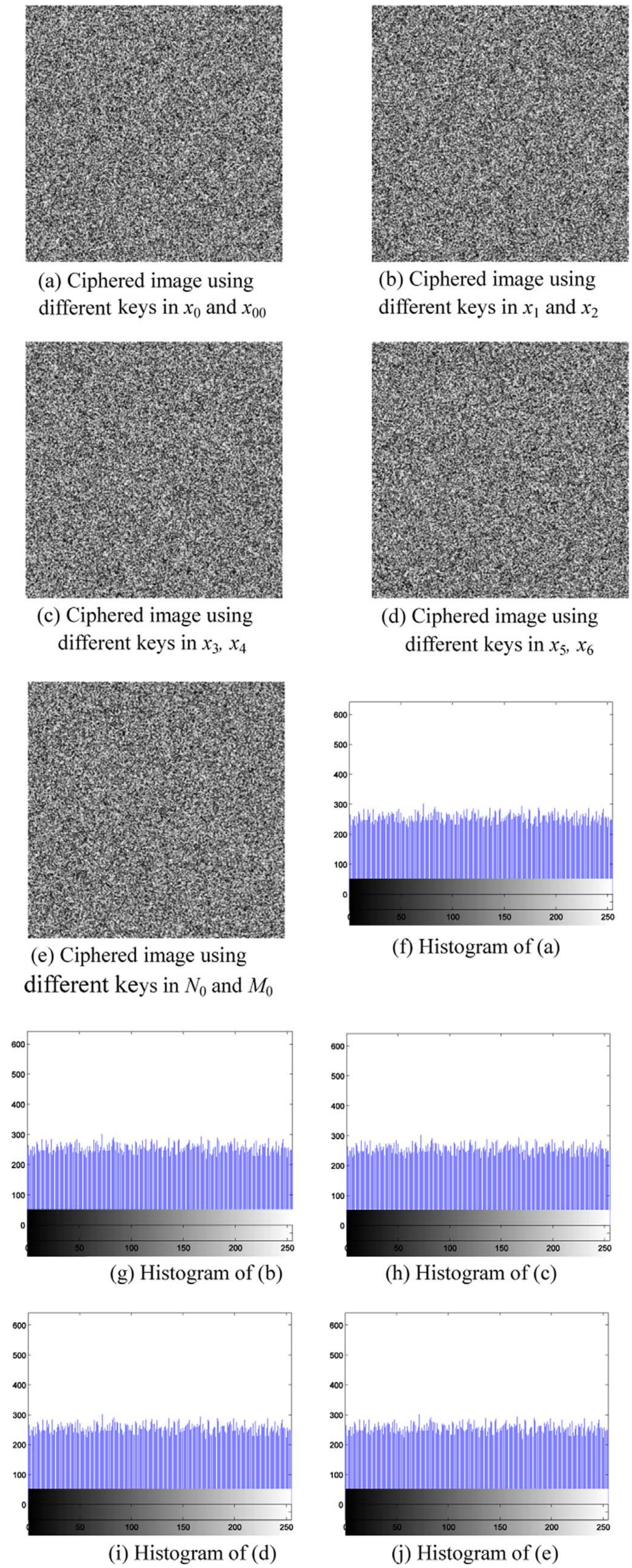
Fig. 3. Correlation of two adjacent pixels.

Table 1
Correlation coefficients of two adjacent pixels in three directions.

Directions	Original image	Ciphered image [24]	Ciphered image of the improved scheme
Horizontal	0.98051573371574	−0.08835249513014	−0.00316265983864
Vertical	0.95252519724865	0.00386549834541	−0.00168207118348
Diagonal	0.93666819191441	0.00322485401485	−0.00189195881424

Table 2
Information entropies.

Test image	Original image	Ciphered image
Lena.bmp (256 × 256)	7.34824581126937	7.99688237260227
Baboon.bmp (256 × 256)	7.12732107924970	7.99715973488881
Cameraman (256 × 256)	7.00971628334551	7.99754623959667
Goldhill.bmp (256 × 256)	7.47606452804718	7.99739506581265



(a) Ciphered image using different keys in x_0 and x_{00}
(b) Ciphered image using different keys in x_1 and x_2
(c) Ciphered image using different keys in x_3, x_4
(d) Ciphered image using different keys in x_5, x_6
(e) Ciphered image using different keys in N_0 and M_0
(f) Histogram of (a)
(g) Histogram of (b)
(h) Histogram of (c)
(i) Histogram of (d)
(j) Histogram of (e)

Fig. 4. Key sensitivity test.

8. Therefore, the image is random as long as its information entropy is close to 8. The entropies of some plaintext images and their corresponding ciphered images are shown in Table 2, which are higher than the average value of 7.995 in Ref. [19].

6.3. Sensitivity analysis

A good cryptosystem should be sensitive to key. Thus, we test the key sensitivity by using keys which are a little different between them. Fig. 4 illustrates the sensitivity of our improved scheme to the secret key x_0, x_{00}, x_1, x_2, x_3, x_4, x_5, x_6, N_0 and M_0. Fig. 1(b) is the encrypted Lena image with the parameters of $x_0=0.123456$, $x_{00}=0.7654321$, $x_1(0)=0.3$, $x_2(0)=-0.4$, $x_3(0)=1.2$, $x_4(0)=10.2$, $x_5(0)=-3.5$, $x_6(0)=4.4$, $N_0=500$ and $M_0=500$.

Fig. 4(a) is the encryption result with all the parameters equal except $x_0 = 0.123456 + 10^{-14}$, $x_{00} = 0.7654321 + 10^{-14}$. Fig. 4(b) is the encryption result with all the parameters equal except $x_1(0)=0.3000001$, $x_2(0)=-0.4000001$. Fig. 4(c) is the encryption result with all the parameters equal except $x_3(0)=1.2000001$ and $x_4(0)=10.2000001$. Fig. 4(d) is the encryption result with all the parameters equal except $x_5(0)=-3.5000001$ and $x_6(0)=4.4000001$. Fig. 4(e) is the encryption result with all the parameters equal except $N_0=501$ and $M_0=501$. So, it can be concluded that the improved chaotic encryption algorithm is sensitive to the key. A small change of the key will generate a completely different decryption results.

6.4. Encryption speed

The improved algorithm is implemented in Microsoft Visual C++ 6.0 and deployed on the computer with the Intel Core i7 CPU, 4 GB memory, 500 G hard-disk capacity and Microsoft Windows 7 operation system. For parallel optimization of the improved algorithm, the Intel C++ compiler is also applied for this multi-core processor. The time used in proposed algorithm is 86.35 ms for a 512×512 image encryption. However, the original sub-image encryption method needs 55.855276 s to encrypt a 512×512 image. In Ref. [5], the execution time is 1 s when encrypting a 512×512 image. Therefore, the improved algorithm is efficient.

7. Conclusions

In this paper, we found that the sub-image encryption method is insecure and proposed an improved algorithm. In the improved algorithm, the security level and the encryption speed of the improved scheme have been enhanced greatly. Experimental results show that the improved sub-image encryption scheme can resist chosen plaintext attack, brute-force attack, statistical attack and differential attack. In the future work, the algorithm can be transplanted in the cloud. The multi-images encryption parallel algorithm of the sub-images scheme will be redesigned properly.

Acknowledgment

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] Matthews R. On the derivation of a “chaotic” encryption algorithm. Cryptologia 1989;13:29–42.
[2] Ma TD, Jiang WB, Fu J, et al. Adaptive synchronization of a class of fractional-

order chaotic systems. Acta Phys Sin 2012;61:160506.
[3] Ma TD, Jiang WB, Fu J, et al. Synchronization of hyperchaotic systems via improved impulsive control method. Acta Phys Sin 2012;61:100507.
[4] Ma TD, Fu J. Global exponential synchronization between Lü system and Chen system with unknown parameters and channel time-delay. Chin Phys B 2011;20:050511.
[5] Chen GR, Mao YB, Chui CK. A symmetric image encryption based on 3D chaotic cat maps. Chaos Solitons Fractals 2004;21:749–61.
[6] Guan ZH, Huang FJ, Guan WJ. Chaos-based encryption algorithm. Phys Lett A 2005;346:153–7.
[7] Cahit C, Ercan S. Cryptanalysis of a chaos-based image encryption algorithm. Phys Lett A 2009;373:1357–60.
[8] Wang K, Pei WJ, Liu HZ, He ZY. On the security of 3D cat map based symmetric image encryption scheme. Phys Lett A 2005;343:432–9.
[9] Gao TG, Chen ZQ. Image encryption based on a new total shuffling algorithm. Chaos Solitons Fractals 2008;38:213–20.
[10] Gao TG, Chen ZQ. A new image encryption algorithm based on hyper-chaos. Phys Lett A 2008;372:394–400.
[11] Yen JC, Guo JI. A new chaotic key-based design for image encryption and decryption. IEEE Int Symp Circuits Syst 2000;4:49–52.
[12] Srividya G, Nandakumar P.:A triple-key chaotic image encryption method. In: International conference on communications and signal processing (ICCSP); 2011. p. 266–70.
[13] Arroyo D, Li CQ, Li SJ, Alvarez G, Halang WA. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos Solitons Fractals 2009;41:2613–6.
[14] Rhouma R, Safya B. Cryptanalysis of a new encryption algorithm based on hyper-chaos. Phys Lett A 2008;372:5973–8.
[15] Jin J. An image encryption based on elementary cellular automata. Opt Lasers Eng 2012;50:1836–43.
[16] Gao HJ, Zhang YS, Liang SY, Li DQ. A new chaotic algorithm for image encryption. Chaos Solitons Fractals 2006;29:393–9.
[17] Kwok HS, Tang WSK. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fractals 2007;32:1518–29.
[18] Pareek NK, Patidar V, Sud KK. Image encryption using chaotic logistic map. Image Vis comput 2006;24:926–34.
[19] Xiang T, Liao XF, Tang GP, Chen Y, Wong KW. A novel blocks cryptosystem based on iterating chaotic map. Phys Lett A 2006;349:109–15.
[20] Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2010;62:615–21.
[21] Zhang Y, Li CQ, Li Q, Zhang D, Shu S. Breaking a chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2012;69:1091–6.
[22] Wang Y, Liao XF, Xiang T, Wong KW, Y D. G. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map. Phys Lett A 2007;363:277–81.
[23] Wang XY, Yu CH. Cryptanalysis and improvement on a cryptosystem based on chaotic map. Comput Math Appl 2009;57:476–82.
[24] Mirzaei O, Yaghoobi M, Irani H. A new image encryption method: parallel sub-image encryption with hyper chaos. Nonlinear Dyn 2012;67:557–66.
[25] Belazi A, Hermassi H, Rhouma R. Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dyn 2014;76:1989–2004.
[26] Farash MS, Attari MA. Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing. Nonlinear Dyn 2014;76:1203–13.
[27] Zhang YQ, Wang XY. Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. Nonlinear Dyn 2014;77:687–98.
[28] Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice. Inf Sci 2014;273:329–51.
[29] May RM. Simple mathematical models with very complicated dynamics. Nature 1976;261:459–67.
[30] Lorenz EN. Deterministic nonperiodic flow. J Atmos Sci 1963;20:130–41.
[31] Chen GR, Ueta T. Yet another chaotic attractor. Int J Bifurc Chaos 1999;9:1465–6.
[32] Stinson DR. Cryptography: theory and practice. Boca Raton: CRC Press; 1995.
[33] Deng Y, Hu H, Xiong N, Xiong W, Liu L. A general hybrid model for chaos robust synchronization and degradation reduction. Inf Sci 2015;305:146–64.
[34] Deng Y, Hu H, Xiong N, Xiong W, Liu L. Analysis and design of digital chaotic systems with desirable performance via feedback control. IEEE Trans Syst Man Cybern: Syst 2015;45(8):1187–200.
[35] 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.
[36] Liu L, Miao S, Hu H. On the eigenvalue and Shannon's entropy of finite length random sequences. Complexity 2014;21(2):154–61.
[37] Liu L, Hu H, Deng Y. An entropy measure of non-stationary processes. Entropy 2014;16(3):1493–500.
[38] Hu HP, Liu LF, Ding ND. Pseudorandom sequence generator based on the Chen chaotic system. Comput Phys Commun 2013;184(3):765–8.
[39] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 2015;73:53–61.
[40] Wang XY, Gu SX, Zhang YQ. Novel image encryption algorithm based on cycle shift and chaotic system. Opt Lasers Eng 2015;68:126–34.
[41] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;66:10–8.
[42] Zhang YQ, Wang XY, Liu J, Chi ZL. An image encryption scheme based on the MLNCML system using DNA sequences. Opt Lasers Eng 2016;82:95–103.
[43] Zhang YQ, Wang XY, New Image A. Encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 2015;26:10–20.
[44] Zhang Y, Wang X. Spatiotemporal Chaos in mixed linear- nonlinear coupled logistic map lattice. Phys A: Stat Mech Appl 2014;402:104–18.