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
Available online 20 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 $\boldsymbol{A}$" 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 $\boldsymbol{A}$", there are $4!=24$ kinds of assignment, which can be cracked by brute-force attacks. Without loss of generality, we assign that the "Random $\boldsymbol{A}$" 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.