Signal Processing 142 (2018) 292–300

Contents lists available at ScienceDirect

Signal Processing

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

Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation

Jiahui Wu, Xiaofeng Liao*, Bo Yang

Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 12 April 2017
Accepted 13 June 2017
Available online 29 June 2017

Keywords:
Chaos
Three-dimensional Chen system
Three-dimensional cat map
Permutation
Confusion
Cryptanalysis

ABSTRACT

Recently, an image encryption based on three-dimensional bit matrix permutation (TDBMP) has been proposed by Zhang *et al.* The encryption scheme has combined Chen chaotic system with a 3D Cat map in the permutation stage, and defined a new mapping rule (double random position permutation) and utilized key-streams generated by Logistic map to confuse the permuted image. However, we have found that this scheme is vulnerable to chosen plaintext attack and is not applicable to secure communications. In this paper, the shortcomings of TDBMP have been analysed and a chosen plaintext attack has been proposed to break the scheme. After that, we propose an enhanced algorithm to overcome the presented shortcomings in the above original scheme. Experimental results also illustrate that the enhanced scheme not only maintains the merits of the original one, but also has better cryptographic performances in key space, plaintext sensitivity, statistical characteristics, robustness against cropping attack and execution speed, and can therefore effectively ensure a secure image communication.

1. Introduction

With the development of Internet and modern information communication technology, increasing multimedia data are transmitted on the Internet. Consequently, secure transmission of media data has become an important issue and has attracted growing attention. Digital image as one of multimedia data has been widely studied on private protection, confidentiality, authentication and data integrity [1]. However, image encryption is different from conventional text encryption due to its intrinsic properties such as bulky data capacity, tight correlation among adjacent pixels and high redundancy [22]. Based on different theories and purposes, researchers have presented a number of effective cryptographic scheme to overcome the above-mentioned [2–14].

Chaotic system has received wide attention with its good characteristics of extreme sensitivity to initial values, ergodicity, and pseudo-randomness, which is very suitable for digital image encryption [16]. Image encryption based on chaos is first proposed by Fridrich [6], and has constantly developed in [7–11]. Many different methods have been used chaos-based image encryption, but some of them are proven to be insecure [17–22]. Thus, security analyses of chaos-based image encryption scheme is indispensable.

In this paper, by using the cryptanalysis methods, we find flaws of image encryption based on three-dimensional bit matrix permutation (TDBMP) [23], and furthermore, an enhanced encryption scheme is proposed to remedy the shortcomings of the TDBMP. Compared with the low-dimensional chaotic systems which have the flaws of short period and low precision and may be attack by brute force [14,15], hyper-chaotic systems have more complicated structures and pseudo-random properties, and can effectively overcome the flaws of low-dimensional systems. In recent years, a large number of researchers have used hyper-chaotic systems to achieve robust encryption schemes [12–14]. In TDBMP, the authors have used 3D chaotic systems to design chaos-based image encryption with permutation and diffusion model. In permutation phase, TDBMP proposed a new 3D permutation scheme based on a coupled Chen system and 3D chaotic cat map to realize image bit level permutation. Compared with some others bit level permutation algorithm, this permutation process has many merits, for instance, it modified the statistical information of each bit plane, changed the location and the weight of each bit, reduced the correlation between adjacent bit planes, removed all the limitations associated with bit level moving, met the ideal situation of bit level permutation and had a faster execution speed. However, some of the shortcomings on security have been exposed in TDBMP scheme. In TDBMP, parameters of cat maps which obtained from key-streams generated by 3D Chen system depend solely on the secret keys, and the location [0, 0, 0] is always mapped into itself in 3D cat

* Corresponding author.
E-mail addresses: xfliao@swu.edu.cn, xfliao@cqu.edu.cn (X. Liao).

http://dx.doi.org/10.1016/j.sigpro.2017.06.014
0165-1684/

map. In diffusion phase, all of the ciphertexts are only related to the corresponding current plaintext and the previous one ciphertext. Due to the above reasons, TDBLP is insecure with the chosen plaintext attack and we have successfully cracked it in this paper. In addition, we propose an enhanced algorithm to overcome the flaws of TDBMP. The enhanced scheme defines a statistic value of plain image, and encrypts plain image relating to the defined value to resist the known/chosen plaintext attack. The statistic value is also encrypted by the enhanced scheme and obtains a cipher value and a constant value 1. The cipher value and the cipher image are the cipher information to communicate. So, one can attack the enhanced scheme only when he has the secret keys, and the enhanced algorithm can resist the known/chosen plaintext attack. Experimental performance illustrates that the enhanced encryption algorithm has a large key space to resist the brute force attack, and has an equalized histogram. The measures of correlation between adjacent pixels, the *UACI*, *NPCR* scores and information entropy are all better than that of TDBMP. Furthermore, the enhanced scheme can resist cropping attack and runs less time than TDBMP.

The rest of the paper is organized as follows: Section 2 overviews the TDBMP algorithm. Section 3 analyses the TDBMP by using the chosen plaintext attack. Section 4 states the flaws of TDBMP and proposes an enhanced encryption and decryption algorithms. Experimental performance evaluation of the enhanced algorithm and comparisons between the enhanced and the original encryption scheme are shown in Section 5. Section 6 is a conclusion of this paper.

2. Overview of the TDBMP encryption algorithm

The encryption process consists of bit level permutation and confusion. First, the plain image $I_{m\times n}$ with 256 gray levels is converted to a bit image $I_{m\times n\times 8}$, then the bit image is reshaped to obtain a 3D bit matrix $I_{h\times h\times h}$ (Note that $8mn = h^3$). In the process of permutation, the algorithm shuffles the 3D bit matrix using three-dimensional Arnold cat map and then reverts the scrambled 3D bit matrix into 2D pixel image. In the process of diffusion, the algorithm changes the gray levels of the pixels.

2.1. Permutation based on 3D bit matrix

Using Chen system to generate random sequences which establish the order of visiting 3D bit matrix. The following Eq. (1) is Chen system:

$$\begin{cases} x' = a(y-x), \\ y' = (c-a)x - xz + cy, \\ z' = xy - bz, \end{cases} \tag{1}$$

where a, b and c are parameters of Chen system. The system is chaotic when $a = 35$, $b = 3$ and $c \in [20, 28.4]$. Run Chen system to obtain three chaotic sequences as Eq. (2).

$$\begin{cases} qx_i = (x_i \times 10^9) \bmod 65536, \\ qy_i = (y_i \times 10^9) \bmod 65536, \\ qz_i = (z_i \times 10^9) \bmod 65536, \end{cases} \tag{2}$$

where x_i, y_i and z_i $(i = 0, 1, \cdots, h-1)$ are the random numbers generated by Chen system. The three sequences are sorted to get the sorted sequences sqx, sqy, sqz respectively. The sequences X, Y, Z record the location of sqx_i, sqy_i, sqz_i in sequence qx, qy, qz respectively. Then the first mapping rule is defined as Eq. (3).

$$(X, Y, Z) \longrightarrow (x, y, z). \tag{3}$$

The second mapping rule is the 3D cat map defined as Eq. (4).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z (a_y b_y + 1) \\ b_z + a_x b_y (a_z b_z + 1) & a_z b_z + 1 & a_y b_z + a_x (a_y b_y + 1)(a_z b_z + 1) \\ b_y (a_x b_x + 1) & b_x & (a_x b_x + 1)(a_y b_y + 1) \end{pmatrix} \times \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \bmod N \triangleq M \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \bmod N, \tag{4}$$

where a_x, a_y, a_z, b_x, b_y and b_z are calculated by Eq. (5).

$$\begin{cases} a_x = (x_{200} \times 10^9) \bmod 64, \\ a_y = (y_{200} \times 10^9) \bmod 64, \\ a_z = (z_{200} \times 10^9) \bmod 64, \\ b_x = (x_{201} \times 10^9) \bmod 64, \\ b_y = (y_{201} \times 10^9) \bmod 64, \\ b_z = (z_{201} \times 10^9) \bmod 64. \end{cases} \tag{5}$$

Connecting the first mapping rule and the second mapping rule, the complete bit permutation algorithm of TDBMP is obtained.

2.2. Diffusion scheme

This scheme is performed at the pixel level. First, transform the scrambled 3D bit matrix to the 2D pixel image and further to a 1D pixel array, and then diffuse the 1D pixel array by Eq. (6).

$$\begin{cases} tmp = (f_3(0) \times 1000) \bmod 256, \\ cph(0) = pm(0) \oplus rdm_2(rdm_1(tmp)), \\ cph(i) = pm(i) \oplus rdm_2(rdm_1(cph(i-1))), i = 1, 2, \cdots, mn-1, \end{cases} \tag{6}$$

where $pm(i)$ denotes the ith pixel in the permuted image and $cph(i)$ is the ith pixel of the encrypted image. tmp is the initial condition. rdm_1 and rdm_2 are random sequences calculated by Eq. (7).

$$\begin{cases} rdm_1 = (f_1(2000 + i) \times 10^9) \bmod 256, \\ rdm_2 = (f_2(2000 + i) \times 10^9) \bmod 256, \end{cases} \tag{7}$$

where f_1, f_2 and f_3 are two random sequences obtained by iterating Logistic map in Eq. (8) with different initial values.

$$f(x_n) = \alpha x_{n-1}(1 - x_{n-1}). \tag{8}$$

When calculating rdm_1 and rdm_2, one discards the repeated numbers and gets the final sequences which both have 256 different numbers.

2.3. Encryption scheme

In this section, the encryption scheme is described in details. The secret keys are Chen system parameters a_1, b_1, c_1 and initial values x_{10}, y_{10}, z_{10} in first permutation mapping rule, and a_2, b_2, c_2 and initial values x_{20}, y_{20}, z_{20} in second permutation mapping rule, and Logistic map parameters α and its initial values key_{d1}, key_{d2}, key_{d3} which generate the chaotic sequences f_1, f_2 and f_3. The encryption steps are as follows:

(1) Transform the plain image from 2D pixel matrix to 3D bit matrix.
(2) Permutate the bit matrix with the first mapping rule and the second mapping rule introduced in Section 2.1.
   a. Generate three random sequences qx_i, qy_i and qz_i by Chen system.
   b. Sort the three sequences and compare the sorted sequences with original sequences to obtain the index sequences X, Y and Z. The random visiting order is $[X(i), Y(i), Z(i)]$ $(i = 0, 1, 2, \cdots)$.
   c. Calculate new location of bit matrix by 3D cat map with the visiting order defined in step (b).
(3) Transform the permuted 3D bit matrix to the 2D pixel matrix and further to 1D pixel array.