International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 7, Issue 2, April, 2018

Component Fusion Image Encryption Method Based on Compound Chaotic Model

Hui Hu, Song Hu, Sibo Huang, Yingxue Cai, Jia Chen, Zhaoquan Cai*
Huizhou University, Huizhou, China

Abstract: In order to improve the ability of image encryption and transmission, a component fusion image encryption method based on composite chaotic model is proposed. The Logistics chaotic map is used to scramble the pixels of the clear text image, and the clear text is used to control the output of the key stream. The relation between the key stream and the plaintext is used to recognize the pixel gray level of the component fusion image, and the binary vector quantization characteristic quantity of the component fusion image coding is obtained by using the single bit detection method. The piecewise linear coding method is used to realize the arithmetic coding and cyclic encryption of the component fusion image, and the composite chaotic model is used to realize the key construction and vector quantization encryption of the image. The simulation results show that the proposed method has strong anti-attack ability and good image encryption performance, which ensures the security of image transmission and storage.

Keywords: image; encryption; chaos; fusion

1. Introduction

With the rapid development of cloud computing and cloud storage technology, using cloud storage tools to realize real-time online storage of mass component fusion images has become an important way of image preservation in the future. In cloud storage, the structured storage design of component fusion image is carried out through distributed grid area storage structure to improve the real-time scheduling and access ability of image. With the increasing of image scale, the cloud storage space expands constantly[1]. People pay attention to the problem of image security. The key link of image security management is image encryption with component fusion. The image security is ensured by designing the structured component fusion image encryption based on cloud storage platform[2].

Because of the simple structure of component fusion image combination and the spatial self-organization and network openness of cloud storage platform, the image is vulnerable to network attack, and the security of component fusion image can be improved by using component fusion image encryption. Among the traditional methods, the main methods of image encryption are elliptical encryption method, segmented NTRUd public key encryption method and so on. In reference [3], an image encryption technique based on Elliptic Curve Cryptography (ECC) is proposed. The elliptic curve equation of image encryption is constructed in finite domain. The encryption and decryption key is designed to encrypt the component fusion image to improve the anti-attack ability of the encrypted image. This method has the problems of too much computation overhead and poor real-time encryption performance in the component fusion image encryption. In reference [4], a quantization coding algorithm of component fusion image based on singular value finite field filling encryption is proposed. The public key is embedded into the finite domain of the distribution of the master key, and the sensitive domain parameters of the key center are filled in to realize the component fusion image encryption. In this method, a large number of prior component fusion images are required as test sets, which results in poor anti-attack ability of component fusion image encryption[5].

Aiming at the above problems, this paper proposes a component fusion image encryption method based on composite chaotic model, which uses Logistics chaotic map to scramble the pixels of clear text image. Single bit detection method is used to obtain binary vector quantization (VQ) characteristic quantity of component fusion image coding, and the key construction and vector quantization encryption of image are realized by composite chaotic model. Finally, experimental analysis is carried out to demonstrate the superior performance of this method in improving the ability of image encryption in component fusion.

2. Mathematical Model and Feature Analysis of Component Fusion Image Encryption

2.1. Unstructured Reconstruction of Component Fusion Images

In order to realize the image encryption design of component fusion in cloud storage platform, the chaotic sensitivity feature representation method is first used to design the unstructured reconstruction of the component fusion image[6]. The elliptic function of image encryption in the finite domain is constructed as follows:

$$Decrypt(sk, c^*)\boldsymbol{A}^{-1} = \boldsymbol{T} = (t_{i,j})_{i,j=1}^{m} \quad (1)$$

The Logistics chaotic map is used to scramble the image, and the chaotic map entangled state is defined as:

$$|f\rangle_1 \in H_1, |f\rangle_2 \in H_2, ..., |f\rangle_n \in H_n \quad (2)$$

The additional state is:

$$|f\rangle = |f\rangle_1 \bullet |f\rangle_2 \bullet ..... \bullet |f\rangle_n \quad (3)$$

The structured feature decomposition of component fusion image encryption is carried out by using cyclic key pairing method[7], and the characteristic decomposition formula of component fusion image encryption key is obtained as follows:

$$Decrypt(sk, c^*)\boldsymbol{A}^{-1}\boldsymbol{A} = \begin{pmatrix} t_{1,1} & \mathbf{L} & t_{1,m} \\ \mathbf{M} & \mathbf{O} & \mathbf{M} \\ t_{m,1} & \mathbf{L} & t_{m,m} \end{pmatrix} \begin{pmatrix} a_{1,1} & \mathbf{L} & a_{1,m} \\ \mathbf{M} & \mathbf{O} & \mathbf{M} \\ a_{m,1} & \mathbf{L} & a_{m,m} \end{pmatrix} \quad (4)$$

The possible spin states of a two-particle system consisting of symbols are obtained as follows:

$$|f\rangle_{121} = |0\rangle_1 |0\rangle_2 \quad (5)$$

$$|f\rangle_{122} = |1\rangle_1 |1\rangle_2 \quad (6)$$

The definition of image arithmetic coding based on chaotic mapping is obtained as follows:

$$\begin{aligned} |y^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 |1\rangle_2 + |1\rangle_1 |0\rangle_2) \\ |y^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2) \\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 - |1\rangle_1 |1\rangle_2) \end{aligned} \quad (7)$$

The information entropy and variance are used as the encrypted homomorphic coding variables to reconstruct the unstructured fused image[8].

2.2. Design of Arithmetic Coding Algorithm Based on Chaotic Mapping

In this paper, based on the study of chaotic nonlinear dynamics control, the sensitivity of chaotic system to system parameters is used. The statistical characteristics of white noise and the ergodic property of chaotic sequences are analyzed. The arithmetic coding and Huffman coding scheme about source coding are designed. Firstly, the algorithm coding technique based on chaotic mapping is presented. The chaotic sequence is defined as:

$$f(x) = \begin{cases} x/p, & x \in [0, p) \\ (1-x)/p, & x \in [p, 1] \end{cases} \quad (8)$$

The mapping is obtained by the parameter. When $p = 0.5$, the map is a standard chaotic sequence map. In the composite chaotic model, the inverse function of arithmetic coding of chaotic map is expressed as arithmetic coding, that is:

$$f^{-1}(I) = \begin{cases} p * I, & s = \text{“0?} \\ 1-(1-p) * I, & s = \text{“1?} \end{cases} \quad (9)$$

Where, $I = [0,1]$ denotes the interval in which the symbol falls, the initial interval S. If multiple character sequences are encoded, the chaotic map can be extended to complete the encoding of the sequence, which is expressed as:

$$f(x) = \begin{cases} x/P_1, & x \in I_1 \\ (x-P_1)/P_2, & x \in I_2 \\ ..... & ..... \\ (x-\sum_{i=1}^{n-1} P_i)/P_n, & x \in I_n \end{cases} \quad (10)$$

In the process of pixel position scrambling, two sets of random numbers are generated by using Logistic chaotic mapping:

$$\boldsymbol{X} = \begin{bmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \\ \mathbf{M} \\ \boldsymbol{x}_3 \end{bmatrix} = \begin{bmatrix} \boldsymbol{a}_1^T \boldsymbol{c}_1 & \boldsymbol{a}_1^T \boldsymbol{c}_2 & \mathbf{L} & \boldsymbol{a}_1^T \boldsymbol{c}_m \\ \boldsymbol{a}_2^T \boldsymbol{c}_1 & \boldsymbol{a}_2^T \boldsymbol{c}_2 & \mathbf{L} & \boldsymbol{a}_2^T \boldsymbol{c}_m \\ \mathbf{M} & \mathbf{M} & \mathbf{O} & \mathbf{M} \\ \boldsymbol{a}_N^T \boldsymbol{c}_1 & \boldsymbol{a}_N^T \boldsymbol{c}_2 & \cdots & \boldsymbol{a}_N^T \boldsymbol{c}_m \end{bmatrix} \quad (11)$$

The inverse function of entropy is obtained by calculating the inverse transformation of entropy:

$$f^{-1}(x) = \begin{cases} P_1 x \\ P_2 x + P_1 \\ ..... \\ P_n x + \sum_{i=1}^{n-1} P_i \end{cases} \quad (12)$$

By using ciphertext feedback, the key stream is correlated with plaintext to enhance the anti-attack of ciphertext, and the average amount of information in the corresponding sequence of encrypted image is obtained as follows:

$$H = -\sum_{i=1}^{n} P_i \log_2(P_i) \quad (13)$$

The plaintext is used to control the output of the key stream, the correlation between the key stream and the plaintext can be used to track and identify the pixel gray level of the fused image, and the ability of image encryption can be improved.

3. Optimization of Image Encryption Algorithm

3.1. Key Design

In this paper, a component fusion image encryption method based on composite chaotic model is proposed. The binary vector quantization characteristic quantity of component fusion image coding is obtained by single bit detection method, and the component is realized by piecewise linear coding method. Fusion image arithmetic coding and cyclic encryption, using chaotic mapping to obtain the key efficiency is:

$$X_n = \{X_n, X_{n-t}, X_{n-2t}, \cdots, X_{n-(d-1)t}\} \quad (14)$$

For each channel model in binary symbol coordinate space, the space vector is expressed as:

$$R_1 = \{X_1, X_2, X_3, \cdots, X_d\}^T \quad (15)$$

For each channel model in binary symbol coordinate space, the space vector is expressed as:

$$R_1^T R_1 = \{X_1, X_2, \cdots, X_m\}\{X_1, X_2, \cdots, X_m\}^T \quad (16)$$

By decomposing the eigenvalue of the upper expression, the following results can be obtained:

$$R_1^T R_1 = V_1 \sum\nolimits_1 V_1^T \quad (17)$$

The chaotic initial sensitivity parameter k is input and the symmetric Hash function is used to design the piecewise map of chaotic encryption. The algorithm is described as follows:

$$\mathrm{C} \to \mathrm{S}: \mathrm{Certificate}\{\mathrm{Cert}_c\}$$

$$\mathrm{C} \to \mathrm{S}: \mathrm{ClientKeyExchange}\{K_c\}$$

$$\mathrm{C} \to \mathrm{S}: \mathrm{CertificateVerify}\left\{\{\mathrm{hash}(\mathrm{messages})\}_{P_c^{-1}}\right\}$$

3.2. Image Encryption Output

The chaotic mapping cryptosystem is used to construct piecewise linear chaotic mapping equation, the component fusion image encryption is obtained as follows:

$$f(x) = \begin{cases} x / P_1, & x \in I_1 \\ (x - P_1) / P_2, & x \in I_2 \\ \quad \cdots\cdots & \quad \cdots\cdots \\ (x - \sum_{i=1}^{n-1} P_i) / P_n, & x \in I_n \end{cases} \quad (18)$$

Where, $P_i (i = 1, \ldots\ldots, n)$ represents the interval distribution probability of chaotic sequences, Because the arithmetic coding of chaotic map is an inverse function, the interval of chaotic map is also inverse corresponding, and it can be obtained as:

$$\begin{aligned} size(I^1) &= \Pi_{i=1}^{M} P(s_i \in S) \\ &= \Pi_{n=1}^{N} (P_n)^{card\{s_i | s_i = S_n\}} \\ &= \Pi_{n=1}^{N} (P_n)^{P_n M} \end{aligned} \quad (19)$$

Then

$$-\log_2(size(I^1)) = -\sum_{n=1}^{N} P_n M \log_2(P_n) = M \otimes H \quad (20)$$

In the circular window of the plaintext sequence, the following cyclic shift update mode of image encryption is obtained:

$$\begin{cases} KC_1 = KC_1 \oplus \{t_j, t_{j+1}, t_{j+2}, \ldots\ldots, t_{j+m-2}\} \\ KS_1 = KS_1 \oplus \{t_{j+m-2}\} \end{cases} \quad (21)$$

Based on the above steps, the remaining blocks are encoded and encrypted in turn, and the segmentation encryption algorithm based on cyclic shift key coding proposed in this paper is finally completed, and the segmented encryption of the image of component fusion is completed.

4. Simulation Experiment and Result Analysis

In order to test the performance of this method in the realization of component fusion image encryption, the simulation experiment is carried out. The experiment is designed by Matlab 7, the length of bitstream of component fusion image is 1024, the image of S, gray level is 256, the image of Lena and Airplane, Barbara, Boat, Baboon) is used in the experiment. The test results show that the bifurcation parameter is $m = 3.96521$, and the initial value of the key is $x_0 = 0.395642571026984$. according to the above simulation parameters, the plaintext image to be encrypted is obtained as shown in Figure 1.

Figure 1. Image To Be Encrypted.

The proposed method to encrypt the image, the scrambled image is obtained as shown in Figure 2.

Figure 2 shows that the proposed method has better scrambling performance, and decrypts the image is shown in Figure 3.

The analysis shows that the decryption image has a great change, it shows that the information of the plaintext image cannot be displayed from the decryption error image, which indicates that the algorithm has sufficient key space to resist exhaustive attack.

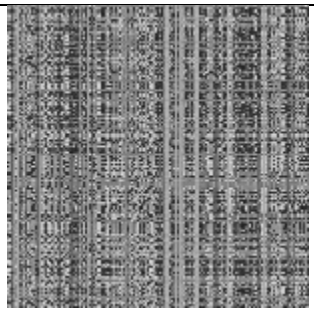

Figure 2. Image Encrypted Scrambled Image.

Figure 3. Decrypted Image.

5. Conclusions

In this paper, a component fusion image encryption method based on composite chaotic model is proposed. The Logistics chaotic map is used to scramble the pixels of the clear text image, and the clear text is used to control the output of the key stream. The piecewise linear coding method is used to realize the arithmetic coding and cyclic encryption of the component fusion image, and the composite chaotic model is used to realize the key construction and vector quantization encryption of the image. The simulation results show that the proposed method has strong anti-attack ability and good image encryption performance, which ensures the security of image transmission and storage, it has good application value in practice.

6. Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 61772225);the Foundation for Distinguished Young Talents in Higher Education of Guangdong (No. 2015KQNCX153);Science and Technology Program of Huizhou (No. 2015B010002002, No. 2016X0431046,No. 2016X0434049, No. 2016X0432047, No.2017c0406022,No.2017c0407023,No.2017c0414030).

References

[1] Zhao Juan, Zhao Qiang, Wu Fenxia. Self-organizing Map Neural Network Based Image Retrieval Algorithm[J]. Bulletin of Science and Technology. 2013; 29(2): 55-57.

[2] CAO Jian, LI Hai- sheng, CAI Qiang. Research on Feature Extraction of Image Target[J]. Computer Simulation. 2013; 30(1): 409-413.

[3] PAN Y, DENG Y. A Ciphertext-Only Attack Against the Cai-Cusick Lattice-Based Public-Key Cryptosystem[J]. Information Theory, IEEE Transactions on, 2011, 57(3): 1780-1785.

[4] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.

[5] A. D. Ker , R. Böhme. Revisiting weighted stego-image steganalysis[J]. In Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, volume 6819, pages 5 1–5 17, San Jose, CA, January 2008:27–31.

[6] AKHSHANI A, AKHAVAN A, LIM S-C, et al. An image encryption scheme based on quantum logistic map[J]. Communications in Nonlinear Science and Numerical Simulation. 2012,17(12):4653-4661.

[7] LUI O-Y, WONG Kwok-Wo, CHEN Jianyong, et al. Chaos-based joint compression and encryption algorithm for generating variable length ciphertext[J]. Applied Soft Computing, 2013,12(1):125-132.

[8] DAI Yin , ZHANG Han-qiu , YU Li-wei. Medical Image Encrypting Method Based on Even Scrambling and Chaotic Mapping[J]. Journal of Northeastern University(Natural Science), 2013, 34(8): 1096-1099.