Research on Component Fusion Image Encryption Method based on Compound Chaotic Model

Huihong Chen[1], Shiming Liu[2*]

[1]School of Information Engineering, Guangzhou Panyu Polytechnic University, GuangZhou, 511483, China
[2]School of Management, Guangzhou Panyu Polytechnic University, GuangZhou, 511483, China

Abstract: In order to improve the security and encryption performance of component fusion image encryption, a method of component fusion image encryption is proposed based on composite chaotic model. A component fusion image is decomposed into three grayscale images, and a composite chaotic model is constructed by using Logistic chaotic map and Hyperhenon chaotic map, and the chaotic algorithm is combined with traditional cyclic encryption. The chaotic system with dynamic initial conditions is used to generate three pseudorandom sequences to encrypt the fused image. The encryption key generated by the logistic chaotic sequence is replaced by the encryption key in the Hyperhenon chaotic sequence to generate the image encryption sequence. The vector quantization coding of image encryption is carried out by piecewise linear chaotic mapping, and the optimal design of image encryption algorithm is realized. The simulation results show that the proposed method has good fusion performance and strong anti-attack ability to ensure the security and stability of image transmission.

Keywords: Compound chaotic model; Component fusion; Image encryption; Logistic chaotic mapping

1. Introduction

In recent years, the spread of digital images with the power of communication media has been greatly developed. Therefore, the security problem of visual information in storage and propagation becomes more and more important, at the same time, it needs a variety of effective solutions to deal with security problems. In the process of image transmission and storage, image encryption design is needed. Chaotic encryption technology is an important branch of nonlinear science[1], which has developed rapidly in recent years, because of its characteristics of aperiodic, continuous broadband, noise and long-term unpredictable. So it is especially suitable for confidential communication. The existing research on chaotic sequences is taken based on statistical analysis or given through experimental tests. It is difficult to ensure that each implementation sequence is sufficiently long and complex enough that people cannot use it to encrypt[2]. Chaotic systems are very sensitive to initial conditions and parameters and have noise-like characteristics, so they are widely used in the design of secure communication systems. Many scholars have proposed many image encryption algorithms based on chaos, some using hyperchaotic systems, some using multi-chaos and composite chaos, some using piecewise linear chaos and so on. No matter what design method is adopted, security and running speed are two important indexes to evaluate the performance of the algorithm. It has great significance to study the image encryption technology based on chaos in improving the security performance of image transmission[3-5].

Chaos research is one of the hotspots in the field of nonlinear science. Chaotic class noise and sensitivity to the height of initial value are closely related to the characteristics of the encryption system, so it is also used more and more in systems such as secure communication and image encryption[6]. Chaos is a seemingly random motion in the decisive dynamic system. The essence is the sensitivity of the long term behavior of the system to the initial conditions. At present, most of the encryption algorithms based on chaos are constructed based on the combination of single chaotic system or simple chaotic system. Although the single chaotic system has the advantages of convenient calculation and small time overhead, the complexity of the sequence is low because of its smaller key space and the low complexity of the sequence. The system security is not high. High dimensional chaos has more than two positive Lyapunov exponents, its nonlinear behavior is more complex and more difficult to predict[7]. In the encryption structure, many high dimensional chaotic systems are introduced with combined chaos, which can provide large key space and improve the complexity of the encryption structure. Image encryption algorithms for chaos and combinatorial chaotic systems have become the mainstream of research.

For image encryption algorithms that require a large number of data operations, parallel computing can double the speed of computing. A good image parallel encryption algorithm should satisfy the good diffusion effect, guarantee the balance of calculation load and realize the critical area management. Zhou et al. proposed a parallel image encryption algorithm based on discrete chaotic mapping. AES algorithm is used to encrypt each packet, then the pixels are rearranged between groups, and then each packet is repeatedly encrypted. The algorithm uses the K (Kolmogorov flow) transformation to rearrange the pixels between groups. It needs multiple multiplication operations. The time consuming is too high. Miraei propsoed a parallel subgraph encryption algorithm based on hyperchaos, which divides the image into the upper and lower parts. About four sub graph operations, because the pixels between subgraphs are independent of each other, they cannot get good diffusion effect[8].

In order to solve the above problems, this paper presents an image encryption method of component fusion based on composite chaotic model. A component fusion image is decomposed into three grayscale images. The chaotic system with dynamic initial conditions is used to generate three pseudorandom sequences to encrypt the fused image. The encryption key generated by the logistic chaotic sequence is replaced by the encryption key in the Hyperhenon chaotic sequence to generate the image encryption sequence. The vector quantization coding of image encryption is carried out by piecewise linear chaotic mapping, and the optimal design of image encryption algorithm is realized. Finally, the simulation results show the superiority of this method in improving the performance of image encryption.

2. Composite Chaotic Model based on Logistic Chaotic Mapping and Hyperhenon Chaotic Mapping Model

2.1. Image encryption analysis based on chaos

Logistic chaotic mapping is used to encrypt the image, the key stream generated by Logistic chaotic mapping is used to scramble the pixels of the plaintext image on the one hand, on the other hand, it is used to encrypt the plaintext image by using XOR operation after scrambling, and in the process of replacing the pixel position[9], the key stream is used to encrypt the image. In this paper, Logistic chaotic map is used to produce chaotic orbit.

$$y(x) = m\,x(1-x) \qquad (1)$$

Where, the state quantity $x \in [0,1]$, the bifurcation parameter $m \in [0,4]$ .When $3.5699456\,\mathbf{L} \le m \le 4$, the system enters a chaotic state, as shown in figure 1. Each point in orbit is expressed in binary form, as shown in formula 2:

$$x = 0.c_1(x)c_2(x)\,\mathbf{L}\,c_i(x)\,\mathbf{L}\,, x \in [0,1], c_i(x) \in \{0,1\} \qquad (2)$$

Where $c_i(x) = \sum_{r=1}^{2^i-1} (-1)^{r-1}\Theta_{r/2^i}(x)$, $\Theta_i(x)$ is threshold function, defined as:

$$\Theta_i(x) = \begin{cases} 0, & x < t, \\ 1, & x \ge t. \end{cases} \qquad (3)$$

From the above calculation, we can get the independent uniform distribution of pseudorandom sequence $\mathbf{C}_i^n = \{c_i(y^n(x))\}_{n=0}^{\infty}$, where n is binary sequence length, and $\mathbf{C}_i^n = \{c_i(y^n(x))\}_{n=0}^{\infty}$ is the N-th iteration value of Logistic chaotic map.

The row transformation of image encryption generates the key stream formula is expressed as follows:

$$r = (y(x) * 10^{10}) \bmod (M) \qquad (4)$$

Where, mod is a modular operation, M is the number of rows of a plaintext image, and M different R values are generated iteratively, $r_i, \{i = 0,1,\mathbf{L}\,, M-1\}$. The column transformation formula generates the key stream formula $c = (y(x) * 10^{10}) \bmod (N)$, where N is the number of columns of the plaintext image, and iterates to produce N different R values, denoted as $c_i, \{i = 0,1,\mathbf{L}\,, N-1\}$.

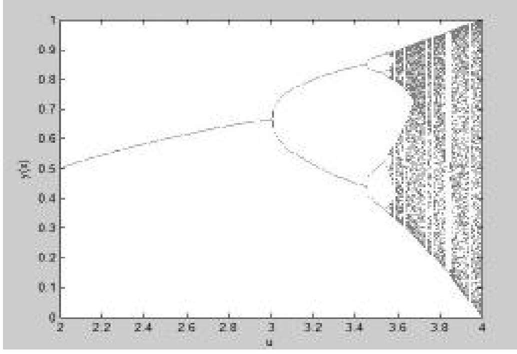


Figure 1. Chaotic Model of Image Encryption

2.2. Decomposition of component fusion images into RGB decomposition

The original plaintext image is divided into three gray images R , G , B , the size of each image is the same, $W*N$, and then the three gray images are encrypted with different encryption methods[10].

Firstly, the R grayscale image is encrypted, and the feature reconstruction of the encrypted sequence is carried out, and the edge pixel set of the component fusion image is represented as:

$$I_{if}(x,y) = I * G(x,y,s_i) \qquad (5)$$

$$I_{iv}(x,y) = I * stdfilt(x,y,w_i) \qquad (6)$$

Where, $G(x,y,s_i)$ represents the gray histogram of the component fusion image in the 4 × 4 grid region. The method of error compensation coding is used to enhance the noise of the component fusion image[11]. The vector error of the compressed component fusion image is obtained as follows:

$$\tilde{t}(x)=1-\min_c(\min_{y\in\Omega(x)}(\frac{I^c(y)}{A^c})) \qquad (7)$$

Where, $I^c(y)$ is the initial pixel set, and A^c represents the high frequency component of the component fusion image. The compression coding of the output component fusion image is：

$$J(x)=\frac{I(x)-A}{\max(t(x),t_0)}+A \qquad (8)$$

The image compression output is:

$$w(i,j)=\frac{1}{Z(i)}\exp(-\frac{d(i,j)}{h^2}) \qquad (9)$$

Where, $Z(i)=\sum_{j\in\Omega}\exp(-\frac{d(i,j)}{h^2})$ represents the vector quantization coding weight of the component fusion image[12].

3. Improved Implementation of Image Encryption Algorithm

3.1. Image encryption sequence and key generation

Logistic chaotic map and Hyperhenon chaotic map are used to construct the composite chaotic model. The chaotic algorithm is combined with the traditional cyclic encryption[13-15], and the Hyperhenon chaotic map is defined as follows:

$$\begin{cases}X_{k+1}=c-Y_{k+1}^2-d\cdot Z_{k+1}\\ Y_{k+1}=X_k & k=0,1,2,\mathbf{L}\\ Z_{k+1}=Y_k\end{cases} \qquad (10)$$

Where, $c=1.76$, $d=0.1$, the system stays in a hyperchaotic state, and the Hyperhenon map is a hyperchaotic sequence. Here $X_0\in(0,1)$.

Lorenz chaotic map is defined as follows:

$$\begin{cases}\dot{x}=s\,(y-x)\\ \dot{y}=r\,x-y-xz\\ \dot{z}=xy-b\,z\end{cases} \qquad (11)$$

Where $[x,y,z]^T$ is a state variable, s, r and b are control parameters, and when $b=8/3$, the Lorenz system is a typical chaotic system under these parameters.

Composite chaotic maps are defined as follows:

$$x_{i+1}=F_{p_i}(x_i)=\begin{cases}x_i/p_i & 0\le x_i<p_i\\ (x_i-p_i)/(0.5-p_i) & p_i\le x_i<0.5\\ F_p(1-x_i) & x_i\ge 0.5\end{cases} \qquad (12)$$

Composite chaotic mapping has unique invariant distribution, good ergodicity, randomness and certainty, so it can provide good random sequences and is suitable for cryptographic systems[16].

Three pseudorandom sequences are generated by chaotic system with dynamic initial condition to encrypt the fusion image of components. The encryption key of the image generated by logistic chaotic sequence is used to encrypt the image, and the image center vector of component fusion is obtained, as R, k, assume $N=2^{kR/2}$, the edge contour feature extraction method is used to extract the high-frequency part $\{x_j\}$, $j=0,1,\cdots,m-1$ of the component fusion image. The N level details of the component fusion image are stratified to $\hat{A}_n$, and the quantization error of the output component fusion image is as follows.

$$P(\hat{A}_n)=\{s_i\}\,,i=1,2,\cdots,N \qquad (13)$$

Where, $s_i=\{x_j:d(x_j,y_i)\le d(x_j,y_l)\}$ is the output edge pixel value of the component fusion image.

3.2. Vector quantization coding and encryption steps of image encryption

In this paper, a component fusion image encryption method is proposed based on composite chaotic model. The chaotic system with dynamic initial conditions is used to generate three pseudorandom sequences to encrypt the fused image, and the encryption key is substituted into the Hyperhenon chaotic sequence to generate the image encryption sequence. The image is mapped by piecewise linear chaotic mapping. Like the vector quantization encoding of encryption, the realization steps of image encryption are expressed as follows:

Step1: The Hash value of the plaintext image is worth the initial value of the two sets of Lorenz equations (r_1,r_2,r_3) and (r_4,r_5,r_6).

Step2: (r_4,r_5,r_6) is substituted into the iterative $W*N$ generation sequence Z' of the Lorenz system, as:

$$Z=\{z_1,z_2,\mathbf{L},z_{W*N}\} \qquad (14)$$

$$Z'=\{z_1',z_2',\mathbf{L},z_{W*N}'\} \qquad (15)$$

Step3: Image encryption sequence of grayscale image Z_1' is:

$$Z_1=\{z_{11},z_{12},\mathbf{L},z_{1,W*N}\} \qquad (16)$$

$$Z_1'=\{z_{11}',z_{12}',\mathbf{L},z_{1,W*N}'\} \qquad (17)$$

$$\begin{cases} z_{1i} = (z_i \times 10^{14}) \bmod 3 + 2 \text{ , if } i \bmod 3 = 0 \\ z_{1i} = (z_i \times 10^{14}) \bmod 3 + 10 \text{ , if } i \bmod 3 = 1 \\ z_{1i} = (z_i \times 10^{14}) \bmod 3 + 18 \text{ , if } i \bmod 3 = 2 \end{cases} \quad (18)$$

$$\begin{cases} z'_{1i} = (z'_i \times 10^{14}) \bmod 3 + 2 \text{ , if } i \bmod 3 = 0 \\ z'_{1i} = (z'_i \times 10^{14}) \bmod 3 + 10 \text{ , if } i \bmod 3 = 1 \\ z'_{1i} = (z'_i \times 10^{14}) \bmod 3 + 18 \text{ , if } i \bmod 3 = 2 \end{cases} \quad (19)$$

Step4: By combining chaotic algorithm with traditional cyclic encryption, three pseudorandom sequences are generated by chaotic system with dynamic initial conditions to encrypt the fused image, as $G_1^S = \left\{ g_{11}^S, g_{12}^S, \mathbf{L}\ g_{1,WN}^S \right\}$:

$$g_{1i}^S = circshift(g_i, z_{1i}) \quad (20)$$

Step5 Set the initial value g_{10} to 0:

$$g_{1i}^C = (g_{1i}^S + g_{1,i-1}^C) \bmod 256 \oplus z'_{1i} \quad (21)$$

Step6: The image matrix is obtained, which converts the encrypted sequence $G_1^C = \left\{ g_{11}^C, g_{12}^C, \mathbf{L}, g_{1,WN}^C \right\}$ to $W * N$, get the encrypted sequence:

$$\begin{cases} C_i = B'_i \oplus B'_{i+1} \oplus B'_{i+2} \oplus Y'_i & \text{if } i \bmod 2 = 0 \\ C_i = B'_i \oplus B'_{i+1} \oplus B'_{i+2} \oplus \neg Y'_i & \text{if } i \bmod 2 = 1 \end{cases} \quad (22)$$

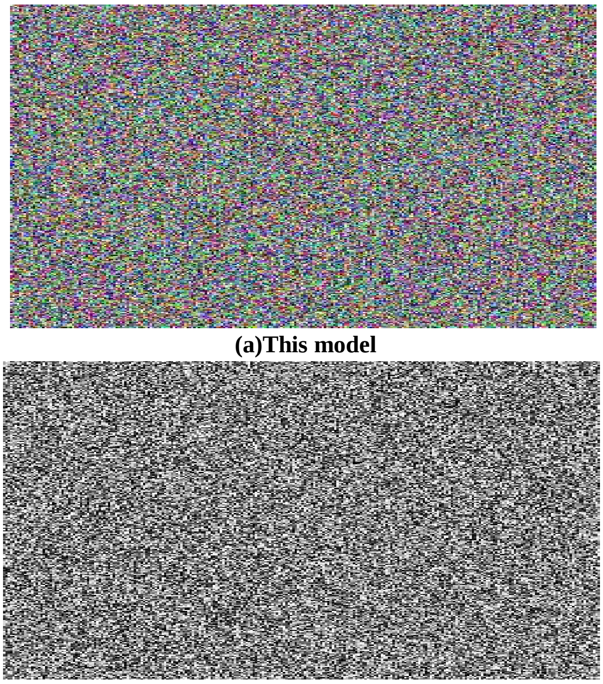
In summary, the component fusion image encryption based on composite chaotic model is realized.

4. Simulation Experiment and Performance Analysis

In order to test the application performance of this method in image encryption, simulation experiments are carried out. The Matlab design is adopted in the experiment. The main processor is Intel(R) Pentium(R) Dual. The main frequency is 1.8GHz, 0.98G, and the capacity of hard disk is 100GB. Parameters are set as: $u = 3.9754$, $c_0 = 0.8161$ $p = 0.1208$, $xfirst = 0.4063$, $(r_1 = 12, r_2 = 2, r_3 = 9)$ and $(r_4 = 13, r_5 = 5, r_6 = 8)$. Initial key $u \in (3.6, 4)$, $c_0 \in (0,1)$, $p \in (1, 0.5)$, $xfirst \in (0,1)$, (r_1, r_2, r_3) and (r_4, r_5, r_6). Double precision is used for the key, each key is a double precision floating-point number, a double-precision floating-point number is usually represented by 64 bits, and generally can represent a valid number of about 16 bits, then the actual key space is $(10^{16})^{10} = 10^{160}$. According to the above parameters setting, the original image to be encrypted is shown in figure 2.

Figure 2. Original Image to be Encrypted

In order to verify the sensitivity of the encryption method to the key, the sensitivity of the plaintext image and the sensitivity of the key are verified. Firstly, the sensitivity of the plaintext image is verified, the House image and the image with a pixel change are selected, and the key sensitivity of the image encryption is compared as shown in figure 3. Figure 3 shows that the key sensitivity of image encryption using this method is good, which shows that encryption has strong anti-attack ability.



(a)This model

(b)Traditional model

Figure 3. Image Encryption Output

5 . Conclusions

In this paper, a component fusion image encryption method based on composite chaotic model is proposed. A component fusion image is decomposed into three grayscale images: r, G, B, and a composite chaotic model is constructed by using Logistic chaotic map and Hyperhenon chaotic map. The chaotic algorithm is combined with traditional cyclic encryption, and the dynamic initial is used. The conditional chaotic system produces three pseudorandom sequences to encrypt the fused image, and the logistic chaotic sequence generates the component fusion image encryption key. The encryption key is substituted into the Hyperhenon chaotic sequence to generate the image encryption sequence. Vector quantization coding of image encryption based on piecewise linear chaotic mapping to realize the optimization design of image encryption algorithm. The simulation results show that the proposed method has good fusion performance and strong anti-attack ability, the security and stability of image transmission is ensured.

References

[1] DU Lin, ZHANG Ying, HU Gao-ge, LEI Youming. Chaos Control for the Duopoly Cournot-Puu Model. Applied Mathematics and Mechanics, 2017, 38(2): 224-232.

[2] Xiao D, Liao X, Deng S. A novel key agreement protocol based on chaotic maps [J]. Information WANG Lifang, DONG Xia, QIN Pinle, GAO Yuan. Multi-modal brain image fusion method based on adaptive joint dictionary learning. Journal of Computer Applications, 2018, 38(4): 1134-1140.

[3] ZONG J.J, QIU T.S, GUO D.M. Simultaneous medical image fusion and de-noising with joint sparse representation[J]. Chinese Journal of Biomedical Engineering, 2016, 35(2):133-140.

[4] LIAN Q.S, SHI B.S, CHEN S.Z. Research advances on dictionary learning models, algorithms and applications[J]. Acta Automatica Sinica, 2015, 41(2):240-260.

[5] SHI W.Z, ZHU C.Q, TIAN Y, et al. Wavelet-based image fusion and quality assessment[J]. International Journal of Applied Earth Observation & Geoinformation, 2005, 6(3/4):241-251.

[6] WANG Z, BOVIK A.C, SHEIKH H.R, et al. Image quality assessment:from error visibility to structural similarity[J]. IEEE Transactions on Image Processing, 2004, 13(4):600-612

[7] WANG Y, WONG K.W, LIAO X, et al.A new chaos-based fast image encryption algorithm [J]. Applied Soft Computing, 2011, 11(1): 514-522.

[8] LIU Z, XU L, LIU T, et al. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains [J]. Optics Communications, 2011, 284(1): 123-128.

[9] ABUTURAB M R. Securing color information using Arnold transform in gyrator transform domain [J]. Optics and Lasers in Engineering, 2012, 50(5): 772-779.

[10] YE G, WONG K.W. An efficient chaotic image encryption algorithm based on a generalized Arnold map[J]. Nonlinear dynamics, 2012, 69(4): 2079-2087.

[11] HUANG X. Image encryption algorithm using chaotic Chebyshev generator [J]. Nonlinear Dynamics, 2012, 67(4): 2411-2417.

[12] LIU H, WANG X. Color image encryption based on one-time keys and robust chaotic maps [J]. Computers & Mathematics with Applications, 2010, 59(10): 3320-3327.

[13] LIU H, WANG X. Triple-image encryption scheme based on one-time key stream generated by chaos and plain images [J]. Journal of Systems and Software, 2013.86(3) 826-834

[14] PAREEK N.K, PATIDAR V, SUD K K. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9): 926-934.

[15] ZHANG L. Cryptanalysis of the public key encryption based on multiple chaotic systems [J]. Chaos, Solitons & Fractals, 2008, 37(3): 669-674.

[16] SALLEH M, IBRAHIM S, ISNIN I F. Image encryption algorithm based on chaotic mapping [J]. Jurnal Teknologi, 2012, 39(1): 1-12.