J. Vis. Commun. Image R. 33 (2015) 219–234

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

A fast encryption algorithm of color image based on four-dimensional chaotic system ☆

Xiao-Jun Tong [a,*], Miao Zhang [a], Zhu Wang [b], Yang Liu [a], Hui Xu [a], Jing Ma [c]

[a] School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China
[b] School of Information and Electrical Engineering, Harbin Institute of Technology, Weihai 264209, China
[c] Science and Technology on Information Assurance Laboratory, Beijing 100072, China

ARTICLE INFO

Article history:
Received 24 October 2014
Accepted 25 September 2015
Available online 3 October 2015

Keywords:
Image encryption
Four-dimensional chaotic system
Hyper-chaos
Pseudo-random sequence generator
Diffusion and scrambling
Column-major
Row-major
Cat map with parameters

ABSTRACT

As the low complexity of low-dimensional chaotic system and the slow speed of image encryption, this paper proposes a fast encryption algorithm of color image based on four-dimensional chaotic system. Firstly, we propose a new method of designing four-dimensional chaotic system based on the classical equations of three-dimensional chaotic system, to increase the complexity and key space of the encryption algorithm. Secondly, according to the nature of color images' pixels channel, we design a new pseudo-random sequence generator and reuse the random sequence, to improve the speed of image encryption. Finally, the methods of row-major and column-major are used to diffuse the original image and the cat map with parameter is used to scramble the image pixels, respectively, to achieve the effect of encryption. The results of simulation and security analysis show that the proposed encryption algorithm is of good performance on security, robustness and high encryption speed.

© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Network information exchanging platform provides a great convenience for people's life. Multimedia communication has become an important means of communication. At the same time, the information security is becoming more and more important. Image as a carrier of information dissemination, its security is becoming very important. The main method to protect the image information is image encryption. Due to the large amount information of the image and the high correlation between pixels, traditional encryption methods are not suitable in image encryption. Because the dynamic properties of chaotic system are very similar with traditional cryptography, the chaotic cryptography has been widely studied in image encryption. The common encryption process is generating pseudo-random sequence by chaotic sequences, then using the pseudo-random sequence to scramble and diffuse the image pixels [1–4]. By increasing the scrambling and diffusing rounds to increase the complexity of the encryption algorithm or using complex chaotic equations to generate chaotic sequence [5,6] to increase the periodicity of the original chaotic system can well satisfy the performance requirements of image encryption, such as sensitivity to initial value, the ability of resisting differential attack and statistical analysis. By the principle of cryptanalysis, the security of an encryption algorithm is decided by its key space, the key space of encryption algorithm needs to be large enough to resist the brute force attack at the existing computing capacity. Common method of expanding the key space is designing a high-dimensional differential equations. Most of the methods of designing high-dimensional differential equation are adding a non-linear fourth-dimension based on the classic three-dimensional differential equations, then adding a linear feedback to the previous three dimensions [7–10]. Jia et al. [11] proposed a four-dimensional differential equation which exists chaotic state in a large range. In this way, they set the parameter of the chaos equation to be un-known as a key for the system to expand the key space. With the introduction of four-dimensional differential equation in image encryption, the method of generating pseudo-random sequence has a great influence on the speed and security of image encryption. Zhu et al. [12] proposed a method to generate a pseudo-random sequence which needs iterate the chaotic equation $\lceil(3 \times M \times N)/4\rceil$ times for diffusing a $M \times N$ color image one round. Wang and Jiang [13] proposed an improved HIE [14] algorithm which need iterate the chaotic equation at least $M \times N$ times for a $M \times N$ color image encryption. Using the chaotic equation to generate array for scrambling is the common method of scrambling image pixels, it will take extra time to generate the

☆ This paper has been recommended for acceptance by M.T. Sun.
* Corresponding author.
E-mail address: tong_xiaojun@163.com (X.-J. Tong).

http://dx.doi.org/10.1016/j.jvcir.2015.09.014
1047-3203/© 2015 Elsevier Inc. All rights reserved.

scrambling array. Guan et al. [15,16] used the cat map with parameters to scramble image pixels which can solve the extra time of generate scrambling array.

In order to improve the security and encryption speed of encryption system, this paper proposes a fast algorithm of color image encryption. The core is proposing a new method to design four-dimensional differential equation on the basis of the classic three-dimensional chaotic system. By validating dynamics characteristic under different parameters, we select the chaotic system in a better state. Then we use one round of row-major and column-major to diffuse the image, and make a reusing of key stream in the diffusion process which can greatly reduce the time of encryption. Finally, the cat map with parameters is used to scramble the image pixels, and the parameters are related to the original plaintext image, it can increase the complexity of the encryption algorithm.

In this paper, the chapters are organized as follows. Section 2 introduces the method of designing a new four-dimensional chaotic equation in detail and describes the dynamic characteristics of chaotic equation. Section 3 describes the algorithm of pseudo-random sequence generator. Section 4 introduces the specific encryption algorithm of color image based on hyper-chaotic system. Section 5 is the implementation of the encryption algorithm and security analysis of the encrypting algorithm. The last part makes a summary for this paper.

2. A study of new four-dimensional chaotic equation

2.1. The design of new four-dimensional chaotic equation

Because of the special nature of chaotic systems, researchers are constantly researching the new equations with chaotic dynamics on the basis of the existing chaotic equation. In this paper, based on the classic three-dimensional chaotic system, we design a method to generate a new four-dimensional chaotic equation. Eq. (1) is the model of three-dimensional chaotic system used in this paper.

$$\begin{cases} \frac{dy_1}{dt} = a_1(y_2 - y_1) \\ \frac{dy_2}{dt} = b_1 y_1 + c_1 y_2 - y_1 y_3 \\ \frac{dy_3}{dt} = d_1 y_3 + y_1 y_2 \end{cases} \tag{1}$$

When $a_1 = 16$, $b_1 = 45$, $c_1 = -1$, $d_1 = -2$, Eq. (1) is the differential equation of Lorenz system, the three Lyapunov exponents of Lorenz are 1.01, 0, −19.96. When $a_1 = 35$, $b_1 = -7$, $c_1 = -28$, $d_1 = 3$, Eq. (1) is the differential equation of Chen system, the three Lyapunov exponents of Lorenz are 2.04, 0, −12.04.

Replace y_1 in Eq. (1) with y_4, just like Eq. (2).

$$\begin{cases} \frac{dy_4}{dt} = a_2(y_2 - y_4) \\ \frac{dy_2}{dt} = b_2 y_4 + c_2 y_2 - y_4 y_3 \\ \frac{dy_3}{dt} = d_2 y_3 + y_4 y_2 \end{cases} \tag{2}$$

Combine Eqs. (1) and (2) to get Eq. (3), the combining rules are as follows. The first dimension comes from the first equation of Eq. (1), the second dimension is the sum of Eq. (1)'s second equation and Eq. (2)'s second equation, the third dimension is the sum of Eq. (1)'s third equation and Eq. (2)'s third equation, the fourth dimension comes from the first equation of Eq. (2).

$$\begin{cases} \frac{dy_1}{dt} = a_1(y_2 - y_1) \\ \frac{dy_2}{dt} = b_1 y_1 + (c_1 + c_2) y_2 + b_2 y_4 - y_1 y_3 - y_3 y_4 \\ \frac{dy_3}{dt} = (d_1 + d_2) y_3 + y_2 y_4 + y_1 y_2 \\ \frac{dy_4}{dt} = a_2(y_2 - y_4) \end{cases} \tag{3}$$

When $a_1 = ka_2,\ k \in R$, there is a linear correlation between the first and the fourth dimension. In order to eliminate the linear relation of the first and the fourth dimension at the special parameters, we add a nonlinear term on the fourth dimension, and rewrite the parameters. Then we get the new equation Eq. (4), where a, b, c, d, e, f, g are the parameters of new four-dimensional equation.

$$\begin{cases} \frac{dy_1}{dt} = a(y_2 - y_1) \\ \frac{dy_2}{dt} = b y_4 + c y_2 + d y_1 - y_1 y_3 - y_3 y_4 \\ \frac{dy_3}{dt} = f y_3 + y_2 y_4 + y_1 y_2 \\ \frac{dy_4}{dt} = g y_2 - e y_4 - 0.05 y_1 y_3 \end{cases} \tag{4}$$

There are many methods to determine whether a system's state is a chaotic state, such as Lyapunov exponent, Lyapunov dimension and Kolmogorov entropy. In this paper, we use Lyapunov exponent to analysis the system's state.

Lyapunov exponent is an important indicator of system dynamics, it characterizes the average rate of convergence or divergence between adjacent tracks of the system in phase space. A positive Lyapunov exponent, means that in system phase space, no matter how small the initial spacing of the two rail lines is, the difference will increase to reach unpredictable by exponential rate with time evolved, which is Chaos. A negative exponent means that the adjacent points eventually merged into a point, it corresponds to the stable fixed point and periodic motion. If exponent is greater than zero, it means that the adjacent points will be finally parted, which corresponds to local instability of the orbit. For a four dimensional dynamic system, when the Lyapunov exponents distribution is two positive value, a zero value and a negative value, the system is in a state of hyper-chaos. If the Lyapunov exponents distribution is one positive value, a zero value and two negative, the system is in a state of chaos. The complexity of hyper-chaos is higher than chaos [14,17,18]. For two chaotic systems, the larger the largest Lyapunov exponent is, the higher the complexity is.

2.2. The performance analysis of new four-dimensional chaotic equation

(1) The complexity analysis of combining two Lorenz systems.
When $a = 16$, $b = 45$, $c = -2$, $d = 45$, $f = -4$, $g = 16$, $e = 16$, the four-dimensional equation is combined by two Lorenz system. The four Lyapunov exponents calculated by Wolf method [19] are 2.10, 0, −15.21, −24.74. The chaotic attractors of three-dimension and two-dimension are shown in Figs. 1 and 2.

(2) The complexity analysis of combining Lorenz system and Chen system.
When $a = 35$, $b = 45$, $c = 27$, $d = -7$, $f = -5$, $g = 16$, $e = 16$, the four-dimensional equation is combined by Lorenz system and Chen system. In this condition, the four exponents are 3.80, 0, −15.36, −17.31. The chaotic attractors of three-dimension and two-dimension are shown in Figs. 3 and 4.

(3) The complexity analysis of hyper-chaos.
Change the value of the parameters in Eq. (1), when $g = -1$, $e = 1$, the Lyapunov exponents of the system are 0.67, 0.15, 0, −22.61. The two positive exponents indicate that the system is in a hyper-chaotic state. Through analysis, when $a = 16$, $b = 45$, $c = -2$, $f = -4$, $g = -1$, $e = 1$, and $d \in [42, 48]$, the systems are the hyper-chaotic system. Fig. 5 shows the variation of Lyapunov exponents with the changing of d. The red[1] line indicates the variation of the first Lyapunov

[1] For interpretation of color in Fig. 5, the reader is referred to the web version of this article.

Download English Version:

https://daneshyari.com/en/article/528557

Download Persian Version:

https://daneshyari.com/article/528557

Daneshyari.com