Optik 126 (2015) 2445–2452

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

An image encryption scheme based on a new hyperchaotic finance system

Xiao-Jun Tong[a,*,1], Miao Zhang[a,1], Zhu Wang[c,1], Yang Liu[a,1], Jing Ma[b,1]

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

ARTICLE INFO

Article history:
Received 12 February 2014
Received in revised form 30 April 2015
Accepted 3 June 2015

Keywords:
Finance system
Hyperchaos
Image encryption
Pseudo-random sequence

ABSTRACT

For the realization of chaos encryption in higher dimension and improving security, in this paper, a new four-dimensional hyperchaotic finance system based on a chaotic finance system is presented. The chaotic sequence is generated by using Runge–Kutta method, the key sequence is generated by chaotic sequence comparison. The key sequence is used for image encryption with relation to plaintext. The results of several analyses about histogram, randomness and information entropy of the encrypted image show that the new hyperchaotic system has high security and complexity.

1. Introduction

The network carries a lot of information, especially multimedia information, the protection of sensitive image data will inevitably bring about the problem of information security. How to ensure the security of our information and how to protect our privacy catch more attention at present; this promotes the research on information security technology. Data encryption is an effective and reliable method for information security which uses computer systems to ensure the security of information.

Chaos is a similar random, seemingly irregular movement that is generated from deterministic nonlinear dynamical system [1]. Chaos is not equal to confusion; it is an order phenomenon which seems complicated and disordered [2]. The greatest characteristic of a chaotic system is that it is very sensitive to the initial value, so from a long-term perspective, the future behavior of the system is unpredictable [3]. Even the same two trajectories with different initial conditions in phase plane of the same system will soon be inconsistent. In addition, chaos has the property of ergodic, the overall stability of local instability, pseudo-randomness, fractal structure and so on [4]. These characteristics of chaos are accord with the basic requirements of cryptography. Therefore, chaos is widely applied to encryption in recent years. It is a breakthrough to encrypt the image using chaotic map in the application field of cryptography. However, the chaos sequences based on low dimensional chaotic system only use simple iteration with few initial values and system parameters, these chaotic sequences have stable periodic window. Hyperchaos has two or more than two positive Lyapunov exponents and is at least contraction and divergence in one torus. So it has more complex dynamic behavior compared with the low dimensional chaotic systems. Because of these advantages, researches on hyperchaos more and more receive attention recently.

The first system shows strange attractor was proposed in 1963 by the American meteorologist Lorenz [5]. In 1979, Rossler gave a definition of hyperchaos, he pointed out two necessary conditions to get hyperchaos: dimension is at least four; the number of coupled equations to ganerate unsteady characteristics must be more than two and one of them must include a nonlinear function. But even so, generating a new hyperchaotic system is still a challenge. Rossler also acquires the hyperchaotic Rossler system [6] using computer simulation. In recent years, domestic and foreign scholars carried out deep research and analysis, they generated many three-dimensional chaotic systems, such as Chen system [7], Lü system [8,9], Liu system [10], Qi system [11].

Based on the classical system, many scholars have made new development. Based on the Lorenz system, Wang [12], Jia [13], Si [14], have found their four-dimensional hyperchaotic map with perfect effect by adding a new nonlinear term. Based on the Chen

* Corresponding author. Tel.: +86 13061181039.
E-mail addresses: tong_xiaojun@163.com (X.-J. Tong), zhangmiaozm209@163.com (M. Zhang).
[1] Research interests: Chaos cryptography, information security.

http://dx.doi.org/10.1016/j.ijleo.2015.06.018
0030-4026/

system, Jia et al. [15] construct a four-dimensional hyperchaos by adding one dimensional and changing xy to y. Based on the Rossler system, Deng et al. [16] construct a new our-dimensional hyperchaotic Rossler system by adding a feedback control. Based on the Lü system, Chen et al. [17] add new nonlinear term, Pang et al. [18] add two nonlinear terms, and they also construct the four-dimensional hyperchaos. Lorenz system family [19] is proposed in 2002 because the Lorenz, Chen and Lü system are similar. Huang constructed a four-dimensional nonlinear dynamics system [20] on the basis of the nonlinear part's characteristics of Qi attractor and Chen attractors. In addition, some three-dimensional chaotic systems such as chaotic financial system [21], Rabinovich system [22] are proposed and their features have been proven, these three-dimensional systems provide basis and reference for future research.

Hyperchaotic system [23,24] has two or more positive Lyapunov exponents, and to generate hyperchaotic system needs at least four dimensions for the integer order continuous autonomous system.

Chaotic sequences of such system are more dependent on the parameters and initial conditions. Its dynamic behavior is more difficult to predict. Its attractors are more complex than general attractor. Diffusion and confusion can be carried out simultaneously in several dimensional spaces. Therefore, hyperchaotic system has a distinct advantage over low dimensional chaos.

2. New hyperchaotic system

2.1. Design of new hyperchaotic system

In 1985, the economics of chaos was found, the chaos in the economic system means that there is inherent instability in the macro-economic movement. Ref. [25] established a chaotic financial system consists of the production sub-block, currency, securities sub-block and labor sub-block:

$$\begin{cases} \dot{x} = z + (y - a)x \\ \dot{y} = 1 - by - x^2 \\ \dot{z} = -x - cz \end{cases} \tag{1}$$

where the parameter x is interest rate, y is investment demand, z is price index, a is the amount of savings, b is investment cost, c is demand elasticity of commodity. When parameters $a = 0.9$, $b = 0.2$, $c = 1.2$, the system shows chaotic behavior.

In this paper, according to the conditions of hyperchaotic system, a new hyperchaotic system is constructed by adding a new parameter w to the first equation of formula (1):

$$\begin{cases} \dot{x} = z + (y - a)x + w \\ \dot{y} = 1 - by - x^2 \\ \dot{z} = -x - cz \\ \dot{w} = -0.05xz + rw \end{cases} \tag{2}$$

where parameter r is the new parameter.

2.2. Proof of new hyperchaotic system

As we all know, a hyperchaotic system must meet the following conditions:

(1) The dimension of the phase space of an autonomous system is at least four.
(2) There are at least two equations giving rise to system instability. The two equations have at least one nonlinear term.
(3) The system has two or more than two positive Lyapunov exponents. Moreover, the sum of the four Lyapunov exponents is less than zero.

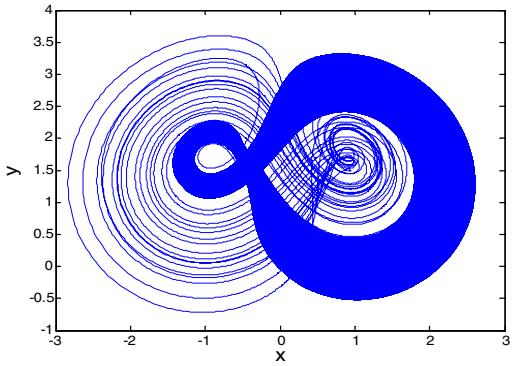

Fig. 1. Projection onto the x–y plane

(4) The Lyapunov dimension of the system is a fraction.

We will examine the conditions mentioned above to prove that the proposed system is a hyperchaotic system. For the proposed system, the first two conditions are met obviously. Now we consider the last two conditions.

2.2.1. Lyapunov exponent

Lyapunov exponent is a quantity to characterize the separation rate of infinitesimally close trajectories. For the proposed system, there are four Lyapunov exponents. When parameters $a = 0.9$, $b = 0.1$, $c = 1$ and $r = -0.6$, the four Lyapunov exponents calculated by Wolf algorithm are: $\lambda_{L1} = 0.100039$, $\lambda_{L2} = 0.003239$, $\lambda_{L3} = 0.488120$ and $\lambda_{L4} = -0.621555$. Obviously, the largest Lyapunov exponent is greater than zero and there are two positive Lyapunov exponents. Moreover, the sum of the four Lyapunov exponents is less than zero.

2.2.2. Lyapunov dimension

The Lyapunov dimension can be calculated by Kaplan–Yorke conjecture:

$$D_l = k + \frac{1}{\left|\lambda_{L,k+1}\right|}\sum_{i=1}^{k}\lambda_{L,i} = 2 + \frac{\lambda_{L1} + \lambda_{L2}}{\left|\lambda_{L3}\right|} = 2 + \frac{0.100039 + 0.003239}{\left|-0.488120\right|} = 2.211583. \tag{3}$$

Here k is an integer that satisfies the following expressions:

$$\sum_{j=1}^{k}\lambda_i \geq 0, \quad \sum_{j=1}^{k+1}\lambda_j < 0 \tag{4}$$

where λ_j denotes Lyapunov exponent. Obviously, for the proposed system, the Lyapunov dimension calculated by Eq. (3) is not an integer, so the system is chaotic.

Based on the analysis above, we have proved the proposed system is a hyperchaotic system.

2.3. Dynamic behavior analysis of new hyperchaotic system

2.3.1. Dissipation and existence of hyperchaotic attractor

The dissipation of the new four-dimensional system in formula (2) is

$$\nabla V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} + \frac{\partial \dot{w}}{\partial w} = -a - b - c + r < 0 \tag{5}$$

That is, the system is a dissipative nonlinear system. All the trajectories of the new system ultimately evolve to an attractor set as $t \to \infty$. This can prove the existence of attractor. The projections for attractor onto the planes are as shown in Figs. 1–6.