Analysis of Performance about Secure Communication Based on Fourth-Order Hyperchaotic System

Nie Chun-yan
Electronic Information Institute
Changchun University
Changchun, China, 130022
e-mail: ncy66@163.com

Sun Hai-xin
Electronic Information Institute
Changchun University
Changchun, China, 130022
haixin_s@hotmail.com

Wang xin
The Chinese People's Liberation
Army Troops 65635
Jinzhou, China, 121000

***Abstract*—In this paper, we propose a new secure communication synchronization system which exploits the combination of the fourth-order hyperchaotic system and the synchronization theory. We study the fast encryption and decryption methods of the images and the performance analysis of the secure communication based on the hyperchaotic system. The simulation results show that the proposed hyperchaotic secure communication generates the unpredicted pseudorandom sequences which have greater complexity and better randomness characteristics comparing to the traditional chaotic encryption schemes. Furthermore, it has larger key space and higher safety performance. Since the proposed system provides a new thought for the synchronization problems of the hyperchaotic system, it is regarded as a potential scheme for resisting the popular attack means.**

Keywords-Hyperchaotic;Coupled Synchronization; Chaotic Coding; Secure Communication

I. INTRODUCTION

The construction of the advanced secure communication system based on hyperchaotic system which combines the chaos theory and the encryption technique is more and more highly valued. The secure communication requires a kind of pseudorandom signals which have strong randomness and long-term unpredictability. At the transmitter, the system employs the pseudorandom signal to generate the concealed synthesized signal, namely ciphertext, which is the phase modulation of the encryption key and the plaintext information, then transmits in the public channels. It is known to all that the chaotic signals have strong concealing features. First, it is highly sensitive to the initial values. Second, it is a kind of the pseudorandom signals of long-term unpredictability and its motion characteristics are difficult to grasp. Third, it has a noise like wideband power spectral density, thus it has the strong anti-interception capability. Meanwhile, the structure of the chaotic system is simple and easy to construct. Hence, it is very suitable for being applied in the field of secure communication [1-2]. In recent years, the application of the chaos theory in secure communication has become a research hotspot in the field of information security. The scholars continuously explore in the aspects of the hyperchaotic theory, hyperchaotic control and the hyperchaotic secure communication. For example, the hyperchaotic secure communication system, which is constructed by the combination of the hyperchaotic theory and the secure communication, has more strong anti-attacked characteristics and larger key space, and the security performance can be improved comparing to the conventional chaotic system [3]. However, the chaotic systems applied in the secure communication are usually low-dimensional. The studies show that the low-dimensional chaotic systems have small key space and weak security performance [4]. Nevertheless, for the high-dimensional hyperchaotic system, it has more complex dynamic characteristics and can generate approximate random sequence, thus it improves the security performance of the system. In this paper, we propose a modified high-dimensional hyperchaotic system and analyze the system performances in the aspect of the secure communication in details. The simulation results show that the proposed system improves the security of the secure communication system effectively.

II. FOURTH-ORDER HYPERCHAOTIC SYSTEM

The hyperchaotic system has two or more positive Lyapunov exponents. Compared to the low-dimensional chaotic system with one positive Lyapunov exponent, the chaotic attractors of the hyperchaotic system become more drastic during the orbit separation, the generated oscillation are fiercer and the dynamic behaviors are more complex. The two chaotic systems begin with different initial values. After a period of time, if the motion orbits of the two systems tend to coincide with each other gradually and last in the same pace, we say that the two chaotic systems achieve synchronization. The meaning of the chaotic synchronization is that it can obtain the motion orbits of the driving system from the response system which has an arbitrary initial value. When the chaotic synchronization is applied in the secure communication, the concealed information in the chaotic signal can be recovered at the receiver [5-7]. Since the hyperchaotic attractors have the advantages of complex dynamic characteristics, strong randomness and long-term unpredictability , the hyperchaotic system has larger key space, stronger robustness and information processing abilities, more safe secure performance compared to the general chaotic secure communication systems.

In this paper, the fourth-order hyperchaotic system is studied, which is generated by adding a new state variable u to the famous third-order Lorenz system. In the third-order

system, the nonlinear term yz is added in the first equation, the linear term $-y$ is changed to u in the second equation and the nonlinear term xy is rewritten as x^2 in the third equation, thus we obtain the equation of the fourth-order hyperchaotic system which is defined in (1):

$$\begin{cases} \dot{x} = a(y-x) + yz \\ \dot{y} = bx - xz + u \\ \dot{z} = -cz + x^2 \\ \dot{u} = -dy \end{cases} \quad (1)$$

III. The Construction of Nonlinear Feedback Controller

Due to the fact that the proposed system has quadratic terms, the synchronization conditions cannot be employed directly by the linear stability theorem. Hence the synchronization of the hyperchaotic system is achieved by the nonlinear feedback coupling method. In the following, we construct the feedback controller from the error system.

For the transmitting system which has the form of (1), we construct the nonlinear feedback controller and obtain the response system, as shown in Eq. (2):

$$\begin{cases} \dot{x} = a(y-x) + yz + m_1 \\ \dot{y} = bx - xz + u + m_2 \\ \dot{z} = -cz + x^2 + m_3 \\ \dot{u} = -dy + m_4 \end{cases} \quad (2)$$

Then we rewrite the Eq. (1) and (2) by substituting x_1, x_2, x_3, x_4 and y_1, y_2, y_3, y_4 for x, y, z, u respectively and obtain the modified forms of the driving system and the response system:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 \\ \dot{x}_2 = bx_1 - x_1 x_3 + x_4 \\ \dot{x}_3 = -cx_3 + x_1^2 \\ \dot{x}_4 = -dx_2 \end{cases} \quad (3)$$

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) + y_2 y_3 + m_1 \\ \dot{y}_2 = by_1 - y_1 y_3 + y_4 + m_2 \\ \dot{y}_3 = -cy_3 + y_1^2 + m_3 \\ \dot{y}_4 = -dy_2 \end{cases} \quad (4)$$

Let

$$e_1 = y_1 - x_1, e_2 = y_2 - x_2, e_3 = y_3 - x_3, e_4 = y_4 - x_4$$

and subtract (3) from (4), we get the error system, as given in Eq. (5):

$$\begin{cases} \dot{e}_1 = a(e_2 - e_1) + e_3 x_2 + e_2 x_3 + e_2 e_3 + m_1 \\ \dot{e}_2 = be_1 + e_4 - x_3 e_1 - x_1 e_3 - e_1 e_3 + m_2 \\ \dot{e}_3 = -ce_3 + e_1^2 + 2x_1 e_1 + m_3 \\ \dot{e}_4 = -de_2 \end{cases} \quad (5)$$

Next we design the controller. Let $m_1 = -e_3 x_2 - e_2 x_3 + k_1 e_1$, $m_2 = x_1 e_3 + x_3 e_1 + k_2 e_2$, $m_3 = -2x_1 e_1 - e_1^2 + k_3 e_3$, $m_4 = 0$, the response system and the error system are simplified to the forms of (6) and (7), respectively.

$$\begin{cases} \dot{y}_1 = a(y_2 - y_1) + y_2 y_3 - e_3 x_2 - e_2 x_3 + k_1 e_1 \\ \dot{y}_2 = by_1 - y_1 y_3 + y_4 + x_1 e_3 + x_3 e_1 + k_2 e_2 \\ \dot{y}_3 = -cy_3 + y_1^2 - 2x_1 e_1 - e_1^2 + k_3 e_3 \\ \dot{y}_4 = -dy_2 \end{cases} \quad (6)$$

$$\begin{cases} \dot{e}_1 = (k_1 - a) e_1 + ae_2 + e_2 e_3 \\ \dot{e}_2 = be_1 + k_2 e_2 + e_4 - e_1 e_3 \\ \dot{e}_3 = (k_3 - c) e_3 \\ \dot{e}_4 = -de_2 \end{cases} \quad (7)$$

From the above analysis, the synchronization problems for the driving system of Eq. (3) and the response system of Eq. (6) can be converted into the zero stability problems for the error system of Eq. (7).

IV. Simulation and Analysis for the Coupled Synchronization

Let the initial values of the driving system and the response system are $x_0 = [0;4;1;7]$ and $y_0 = [22;22;16;16]$, respectively. We observe the synchronous orbits of the driving system and the response system from the perspective of single state variable. The waveforms of the state variable x_1 and x_2 after iteration are indicated in Fig.1. We find that under certain initial conditions, the variation of the state variable of the response system follows that of the driving system after 200 iteration times and the synchronization is achieved.

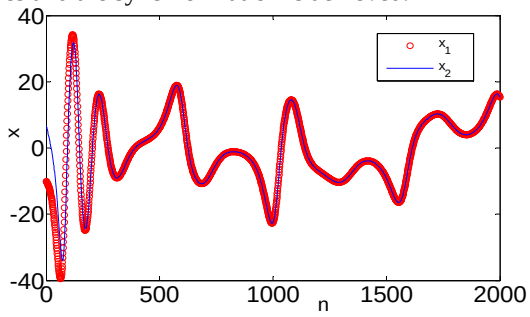


Figure.1 The waveforms of the state variables x_1 and x_2

In the following, we simulate and analyze from the perspective of synchronous error. Let $a=10, b=10, c=2.5, d=1, k_1=-20, k_2=-60, k_3=-20$ and select the system initial values of $x_0 = [2,4,1,7]$ and $y_0 = [25,25,22,20]$ for the iteration. The synchronous errors for x_1 and y_1, x_2 and y_2, x_3 and y_3, x_4 and

y_4 are analyzed in Fig.2, respectively.

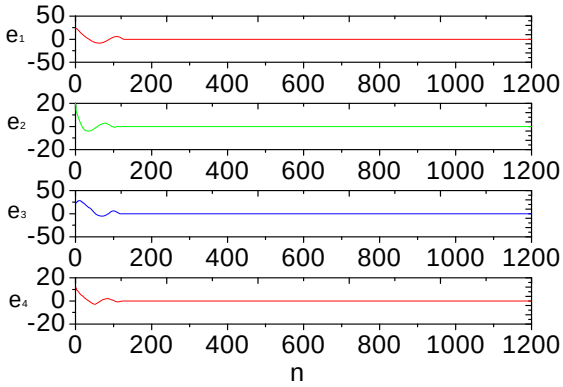
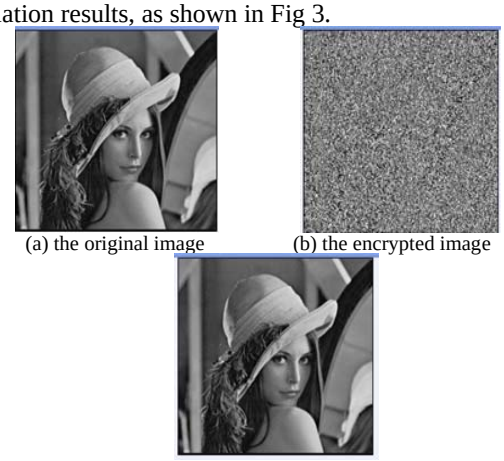


Figure..2 The synchronous errors of the driving system and the response system

From Fig.2, we observe that although the initial values are different, the synchronous error value is stable at the zero point after approximate 150 iteration times, which indicates that the coupled synchronization is achieved between the driving system and the response system.

V. Image Encryption Simulation of the Fourth-Order Hyperchaotic System

Keeping the system parameters and the key unchanged, we encrypt and decrypt the Lena image and obtain the simulation results, as shown in Fig 3.



(a) the original image (b) the encrypted image

(c) the restored image

Figure.3 The image encryption and decryption based on fourth-order hyperchaotic system

As indicated in Fig.3 (b), after the image encryption, we hardly identify any information of the original image. However, the encrypted image is restored well at the receiver.

VI. Sensitivity Analysis of the Key

Generally, different chaos systems generate different random sequences. Even if the systems have the same form, the chaotic characteristics are different in the case of different parameters. Hence, the chaotic characteristics are determined by two parts. One part is the nonlinear equations and the parameters of the system. Since chaotic motion is highly sensitive to the initial values, the system will generate different random sequences in case of different initial values even if the system equations and parameters are exactly the same. The other part is that the generated random sequences are also determined by the encoding mode and the data processing mode and the encrypted data are determined by the iteration times. A good encryption scheme should be sensitive to the key. Next, we take the text encryption for example and investigate the sensitivity degree of the ciphertext for the key. We simulate in the case of system parameter changing slightly and iteration times changing slightly, respectively. The variations of the ciphertext are shown in We simulate in the case of system parameter changing slightly and iteration times changing slightly, respectively. The variations of the ciphertext are shown in Fig.4

It is argued that the decryption cannot be accomplished when the iteration times are set in the oscillating intervals. If the oscillating parts are given up, the key space is decreased and there are many troubles for determining the oscillating boundary conditions of different parameters at the same time.

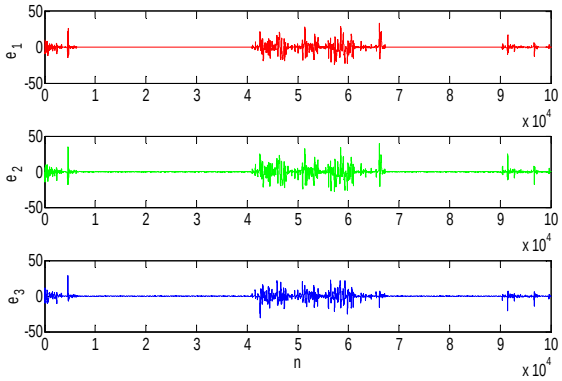


Figure.4 The variation of the synchronous deviation based on hyperch aotic system

VII. Conclusion

A new hyperchaotic secure communication system is proposed in this paper. In the system, the encryption key is arbitrary. Different keys can be exploited by the encryption algorithm and the keys can be changed for each part of the system. Hence the system can resist the known plaintext attack. Furthermore, the system generates the decryption keys at the receiver by exploiting synchronization, which avoids the transportation and the storage of the huge mass of keys and reduces the possibilities of recognizing keys by the attackers. Due to the advantages of high sensitivities to the key, the proposed system can also resist the differential analysis decipher method effectively.

References

[1] Nie Chunyan. Chaotic System and Weak Signal Detection. Beijing: Tsinghua University Press, 2009.3：12～13.

[2] Liu Yang, Peng Liangyu. A Novel Secure Communication of the Unified Chaos. Information Security and Communications Privacy,

2007. 7：103～104.

[3] Li Yuxia，Chen Guanrong，Tang W K S. Controlling a Unified Chaotic System to Hyperchaotic. IEEE Trans. On Circ. Sys. (Ⅱ)：EXPRESSBRIEFS，2005，52(4) ：204～207.

[4] Alvarez G，Montoya F，Romera M，et al. Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value.Chaos，Solitons and Fractals, 2005, 23: 1749～1756

[5] Wang Xue-bing, Zhang Lin-hua, Li Chuan-dong. Synchronization of Chaotic Systems and Its Applications in Secure Communication. Application Research of Computers, 2007, 24(5): 127～130.

[6] Gong Meijing, Qu Shaocheng, Wang Xiaoyan. A Novel Method of Realizing Chaotic Secure Communication by Synchronization of Different Structure. Journal of Electronics & Information Technology, 2009.31(6)：1442～1443.

[7] Zhu Jianliang, Gong Yunrui. Designing the Experimental Circuit of Chaotic Secure Communication. Electric Machinesand Control, 2007.10(3)：265