복잡계 비밀 통신

배영철,김천석, 김주완, 구영덕*
여수대학교 전자통신전기공학부
Youngchul Bae ,Juwan Kim,Chunsuk Kim,Youngduk Koo
*Nat'l Yosu University, *KISTI
E-mail : ycbae@yosu.ac.kr

Abstract

In this paper, we introduce a secure communication method using complex system. We make a complex system with the n-double scroll or Chua's oscillator. The Complex system is created by applying identical n-double scroll or non-identical n-double scroll and Chua's oscillator with weak coupled method to each cell. In order to secure communication, we have synthesizing the desired information with a complex system circuit by adding the information signal to the hyper-chaos signal. And then, transmitting the synthesized signal to the ideal channel, we confirm secure communication by separating the information signal and the complex system signal in the receiver.

1. Introduction

Recently, there has been interest in studying the behavior of chaotic dynamics. Chaotic systems are characterized by sensitive dependence on initial conditions, making long term prediction impossible, self-similarity, and a continuous broad-band power spectrum, etc. Chaotic systems have a variety of applications, including chaos synchronization and chaos secure communication [1-6]. Chaos synchronization and secure communication has been a topic of intense research in the past decade. However, secure communication or cryptographic using chaos has several problems [7]. First, almost all chaos-based secure communication or cryptographic algorithms use dynamical systems defined on the set of real number, and therefore are difficult for practical realization and circuit implementation. Second, security and performance of almost all proposed chaos-based methods are not analyzed in terms of the techniques developed in cryptography. Moreover, most of the proposed methods generate cryptographically weak and slow algorithms.

To address these problems, we need a complex system to increase the complexity in secure communication or cryptographic communication. In this paper, we introduce an embedding secure communication method using complex system. We make a complex system with the n-double scroll [8], and Chua's oscillator.

In order to make a complex system, we used identical n-double scroll or non-identical n-double scroll and Chua's oscillator with weak coupled method to each cell.

Then we accomplished a complex system synchronization using GS (Generalized synchronization) method between the transmitter and receiver. We accomplish secure communication by synthesizing the desired information with a complex system by embedding the information signal to the hyper-chaos signal. After transmitting the synthesized signal to the ideal channel, we confirmed the actuality of secure

communication by separating the information signal and the complex system signal in the receiver].

2. Complex system

2.1. n-Double scroll circuit

In order to synthesize a hyper-chaos circuit, we first consider Chua's circuit modified to an n-double scroll attractor. The electrical circuit for obtaining n-double scroll, according to the implementation of Arena et al. [12] is given by

$$\begin{aligned}\dot{x} &= \alpha[y - h(x)] \\ \dot{y} &= x - y - z \\ \dot{z} &= -\beta y\end{aligned} \tag{1}$$

with a piecewise linear characteristic

$$h(x) = m_{2n-1}x + \frac{1}{2}\sum_{i=1}^{2n-1}(m_{i-1} - m_i)(|x + c_i| - |x - c_i|) \tag{2}$$

consisting of 2(2n-1) breakpoints, where n is a natural number. In order to generate n double scrolls one takes $\alpha = 9$ and $\beta = 14.286$. Some special cases are:

1-double scroll

$$m_0 = -\frac{1}{7}, m_1 = \frac{2}{7}, c_1 = 1$$

2-double scroll

$$m_0 = -\frac{1}{7}, m_1 = \frac{2}{7}, m_2 = -\frac{4}{7}, m_3 = m_1,$$
$$c_1 = 1, c_2 = 2.15, c_3 = 3.6$$

3-double scroll

$$m_0 = -\frac{1}{7}, m_1 = \frac{2}{7}, m_2 = -\frac{4}{7},$$
$$m_3 = m_1, m_4 = m_2, m_5 = m_3,$$
$$c_1 = 1, c_2 = 2.15, c_3 = 3.6, c_4 = 8.2, c_5 = 13$$

2.2 Hyper-chaos circuit

To synthesize a hyper-chaos circuit, we second consider one-dimension cellular neural network (CNN) with n-double scroll cell [8]. The following equations describe a one-dimensional CNN consisting of identical n-double cell with diffusive coupling as

$$\begin{aligned}\dot{x}^{(j)} &= \alpha\left[y^{(j)} - h(x^{(j)})\right] + D_x(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ \dot{y}^{(j)} &= x^{(j)} - y^{(j)} - z^{(j)} \\ \dot{z}^{(j)} &= -\beta\, y^{(j)} \quad j = 1,2,\ldots,L\end{aligned} \tag{3}$$

or

$$\begin{aligned}\dot{x}^{(j)} &= \alpha\left[y^{(j)} - h(x^{(j)})\right] \\ \dot{y}^{(j)} &= x^{(j)} - y^{(j)} - z^{(j)} + D_y(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ \dot{z}^{(j)} &= -\beta\, y^{(j)} \quad j = 1,2,\ldots,L\end{aligned} \tag{4}$$

where L denotes the number of cells. We impose the condition that $x^{(0)} = x^{(L)}, x^{(L+1)} = x^{(1)}$ for equation (3) and (4).

For the coupling constants, $K_0 = 0, K_j = K(j = 1,\ldots,L-1)$ and positive diffusion coefficients D_x, D_y are chosen base on stability theory.

3. The Secure Communication of Complex System using embedding Method

The method we used to accomplish the secure communication was to synthesize the desired information with the complex system by adding sinusoidal signal as an information signal to the complex system .

After transmitting the synthesized signal to the ideal channel, we confirmed secure communication by separating the information signal and the hyper-chaos signal in the receiver [10,11].

In order to achieve the secure communication, we propose that method using only one state variable embedding instead of use to all state

variable driven-synchronization method in the transmitter [11]. To information signal embedding,

We chosen x_1 and x_3 term as a state variable in the transmitter state equation with complex system written as follows:

The state equation of transmitter

$$\dot{x} = Ax + g(w)$$
$$g(w) = [g(x_1 + 0.1\sin(2\pi f)) \ 0 \ 0 \ g(x_4) \ 0 \ 0]$$
$$\dot{x}' = Ax' + g(x') + F(x, x') \tag{5}$$

The state equation of receiver

$$\dot{y} = Ay + g(y)$$
$$g(y) = [g(y_1) \ 0 \ 0 \ g(y_7) \ 0 \ 0]$$
$$\dot{y}' = Ay' + g(y') + F(y, y') \tag{6}$$

Proposed secure communication diagram of hyper-chaos is shown in Fig. 1. In Fig. 2, we use sinusoidal signal as an information signal and shown Fig. 3, and add it to state variables x_1 and x_3 in the complex system.

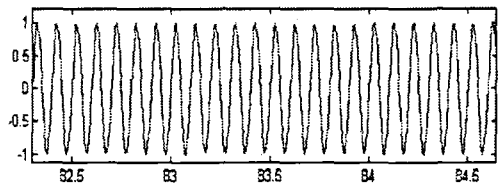

Fig. 2 Information signal

Fig. 3 and 4 are shown that the result of adding the information signal to state variable x_1 and x_3.

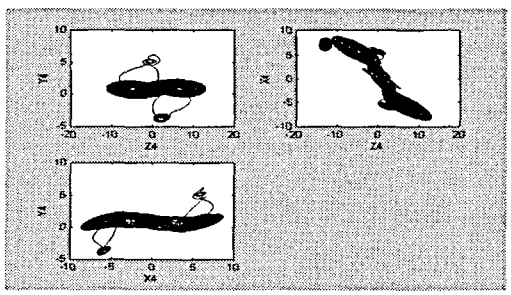

Fig. 3 The result of adding the information signal to state variable x_1

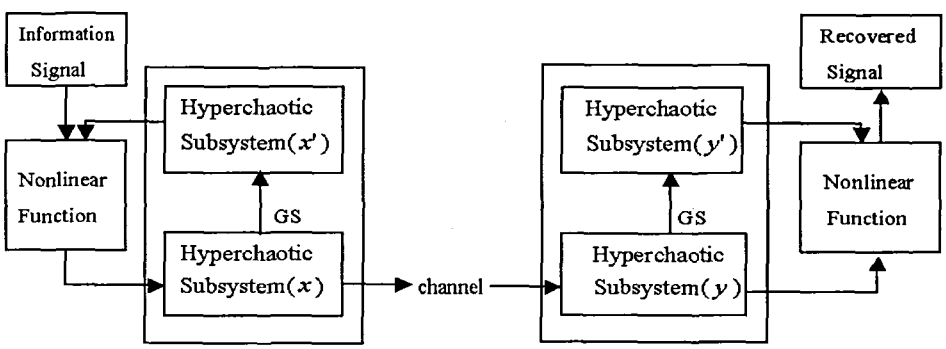

Fig. 1 Block diagram of complex secure communication

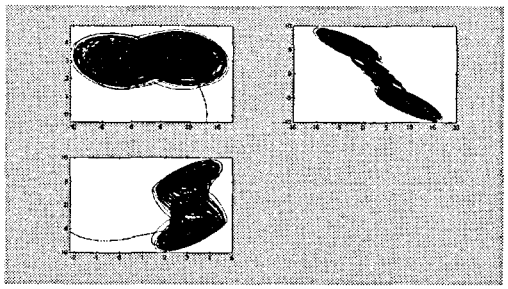

Fig. 4 The result of adding the information signal to state variable x_3

After synchronizing the transmitter and receiver in a hyper-chaos circuit through the ideal channel, we separate the information signal and the hyper-chaos signal in the demodulation part. Recover signals in the demodulation part are shown in Fig. 5 and 6, respectively.

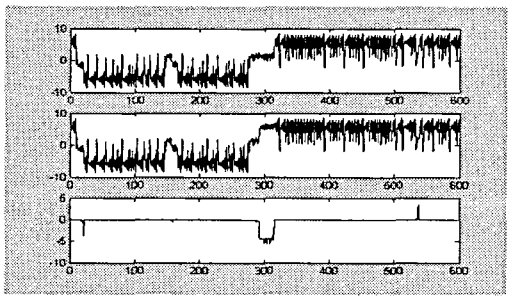

Fig. 5 The result of recovery information signal of state variable x_1

In Fig. 5, the first part shows state x_1 with information signal embedding, the second part shows the result in the receiver, and the third part shows the recover signal.

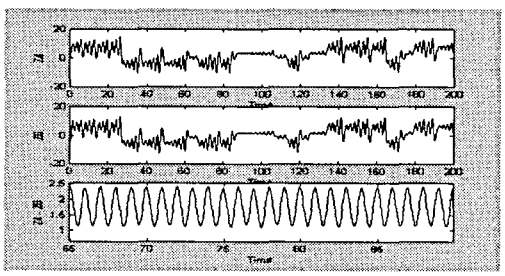

Fig. 6 The result of recovery information signal of state variable x_3

In Fig. 6, the first part shows state x_3 with information signal embedding, the second part shows the result in the receiver, and the third part shows the recover signal

We show that the superiority of the recovery signal for state x_3 to state x_1. This is significant because we can not use the current component i_L in Chua's circuit or Chua's oscillator, which is replaced by x_3 in the hyper-chaos circuit using the complex system. It is clear that state variable x_3 is superior to state x_1 or x_2 as a carrier signal in the complex system In order to increase secure communication complexity, we can choose better transmitter signal which is x_3 when it is compare with x_1 and x_2.

4. Conclusion

In this paper, we introduced a complex system communication method which is called GS (Generalized synchronization) and embedding secure communication. The method in which after we accomplished synchronization between the transmitter and receiver in the complex system using GS method, we used to accomplish the secure communication was to synthesizing the desired information with a complex system circuit by embedding the information signal to the complex system signal by only one state variable x_3 embedding from the complex system to the transmitter. As a computer simulation result, we confirm embedding secure communication method by separating the information signal and the complex system signal in the receiver.

REFERENCE

[1] L. O. Chua "Chua's circuit 10 Years Later", Int. J. Circuit Theory and Application, vol. 22, pp 79-305, 1994

[2] M. Itoh, H. Murakami and L. O. Chua, "Communication System Via Chaotic Modulations" IEICE. Trans. Fundamenrtals. vol. E77-A, no. 6, pp. 1000-1005, 1994.

[3] L. O. Chua, M. Itoh, L. Kocarev, and K. Eckert, "Chaos Synchronization in Chua's Circuit" J. Circuit. Systems and computers, vol. 3, no. 1, pp. 93-108, 1993.

[4] M. Itoh, K. Komeyama, A.Ikeda and L. O. Chua, "Chaos Synchronization in Coupled Chua Circuits", IEICE. NLP. 92-51. pp. 33-40. 1992.

[5] K. M. Short, "Unmasking a modulated chaotic communications scheme", Int. J. Bifurcation and Chaos, vol. 6, no. 2, pp. 367-375, 1996.

[6] K. M. Cuomo, "Synthesizing Self - Synchronizing Chaotic Arrays", Int. J.Bifurcation and Chaos, vol. 4, no. 3, pp. 727-736, 1993.

[7] L. Kocarev, "Chaos-based cryptography: A brief overview", IEEE, Vol. pp. 7-21. 2001.

[8] J.A.K.Suykens, "n-Double Scroll Hypercubes in 1-D CNNs" Int. J. Bifurcation and Chaos, vol. 7, no. 8, pp. 1873-1885, 1997.

[9] L. M. Pecora and T. L. Carroll "Synchronization in Chaotic System" Phy. Rev. Lett., vol. 64, no. 8, pp. 821-824, 1990.

[10] L. Kocarev, K. S. Halle, K. Eckert and L. O. Chua, "Expermental Demonstration of Secure Communication via Chaotic Synchronization" Int. J. Bifurcation and Chaos, vol. 2, no. 3, pp. 709-713, 1992.

[11] K. S. Halle, C. W. Wu, M. Itoh and L. O. Chua, "Spread Spectrum communication through modulation of chaos" Int. J. Bifurcation and Chaos, vol. 3, no. 2, pp. 469-477, 1993.

[12] P.Arena, P.Baglio, F.Fortuna & G.Manganaro, "Generation of n-double scrolls via cellular neural networks", Int. J. Circuit Theory Appl, 24, 241-252, 1996.

[13] P. Arena, S. Baglio, L. Fortuna and G. Maganaro, "Chua's circuit can be generated by CNN cell", IEEE Trans. Circuit and Systems I, CAS-42, pp. 123-125. 1995.

[14] L. Kocarav, L & U. Parlitz, "Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical systems", Phys. Rev. Lett, vol. 76, no.11, pp. 1816-1819, 1996.

[15] M. Brucoli, D. Cafagna, L. Carnimeo & G. Grassi, "An efficient technique for signal masking using synchronized hyperchaos circuits", Proc. 5$^{thInt.}$ workshop on Nonlinear Dynamics of Electronic Systems(NDES '97), Moscow, Russia, June 26-27, pp. 229-232, 1997.

[16] J.A.k. Suyken, P.F. Curran & L.O. Chua, "Master-slave synchronization using dynamic output feedback", Int. J. Bifurcation and Chaos, vol. 7, no. 3, 671-679, 1997.

[17] J.J. Slotine & W.Li, "Applied Nonlinear Control", Prentice-Hall, NJ, 1991.