2003 International Symposium on Advanced Intelligent Systems
September 25-28, 2003, Jeju, Korea

The secure communication in hyper-Chaos

Youngchul Bae, Juwan Kim, Yigon Kim
Division electronic communication and electrical engineering of Yosu National University
San 96-1, Dundeok-dong, Yosu-si, Jeollanam-do, Korea, 550-749
ycbae@yosu.ac.kr

Abstract- In this paper, we introduce a hyper-chaos secure communication method using Hyper-chaos consist of State – Controlled Cellular Neural Network (SC-CNN). A hyper-chaos circuit is created by applying identical n-double scroll with weak coupled method to each cell. Hyper-chaos synchronization was achieved using embedding synchronization between the transmitter and receiver about in SC CNN. And then, we accomplish secure communication by synthesizing the desired information with a hyper-chaos circuit by embedding the information signal to the only one state variable instead of all state variables in the driven-synchronization method. After transmitting the synthesized signal to the identical channel, we confirm secure communication by separating the information signal and the hyper-chaos 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 hyper-chaos circuit to increase the complexity in secure communication or cryptographic communication. In this paper, we introduce a embedding hyper-chaos secure communication method using State-Controlled Cellular Neural Network (SC-CNN) as a hyper-chaos circuit. We make a hyper-chaos circuit using SC-CNN with the n-double scroll [8].

In order to make a hyper-chaos circuit, we use identical n-double scroll with weak coupled method to each cell. Then we accomplish a hyper-chaos synchronization using embedding synchronization between the transmitter and receiver as only one state variable embedding method instead of use to all state variables in the driven-synchronization method [9]. We accomplish secure communication by synthesizing the desired information with a hyper-chaos circuit by embedding the information signal to the hyper-chaos signal, using only one state variable of the SC-CNN in the transmitter. After transmitting the synthesized signal to the ideal channel, we confirmed the actuality of secure communication by separating the information signal and the hyper-chaos signal in the receiver [10, 11].

2. Hyper-chaos circuit

To create a hyper-chaos circuit, we used to the n-double scroll using the weak coupling method [8].

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

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

The 3-double scroll attractor is shown in Fig. 1

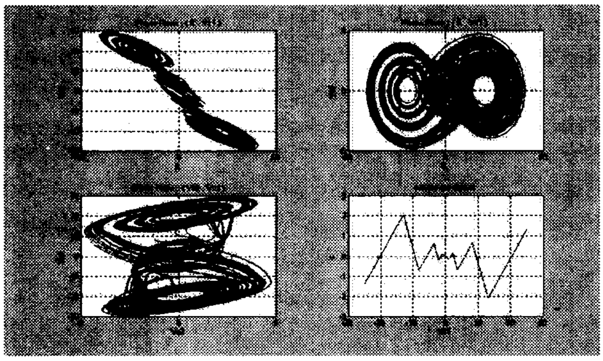

Fig. 1 3- double scroll attractor

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

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

or

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

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.

2.3 SC- CNN model [12, 13]

In [12, 13], the follow generalized cell was introduced:

$$\dot{x}_j = x_j + a_j y_j + G_o + G_s + i_j \tag{5}$$

where j is the cell index, x_j the state variable, y_j the cell output given as

$$y_j = 0.5(|x_j + 1| - |x_j - 1|) \tag{6}$$

where, a_j a constant parameter and i_j a threshold value.

In equation (5), G_o is linear combination of the outputs and G_s is state variable of the connected cells.

Generalizing the output nonlinearity (6), the following new output PWL equation is considered

$$y_j = \frac{1}{2}\sum_{k=1}^{2n-1} n_k(|x + b_k| - |x - b_k|) \tag{7}$$

where b_k are the break point and the coefficients n_k are related to the slopes of segments.

SC-CNN cells required to generate the n-double scroll in accordance with the state equation (5) and output equation (7) are given by

$$\dot{x}_1 = -x_1 + a_1 y_1 + a_{12} y_2 + a_{13} y_3 + \sum_{k=1}^{3} s_{1k} x_k + i_1$$

$$\dot{x}_2 = -x_2 + a_{21} y_1 + a_2 y_2 + a_{23} y_3 + \sum_{k=1}^{3} s_{2k} x_k + i_2 \qquad (8)$$

$$\dot{x}_3 = -x_3 + a_{31} y_1 + a_{32} y_2 + a_3 y_3 + \sum_{k=1}^{3} s_{3k} x_k + i_3$$

where x_1 , x_2 , x_3 are state variables and y_1 , y_2 , y_3 are corresponding outputs. More details about the SC-CNN are given in reference [12, 13]

3. The synchronization of hyper-chaos circuit

To accomplish synchronization in hyper-chaos circuit, we applied embedding synchronization theory between the identical transmitters and receivers with the SC-CNN. Tthe result of synchronization is shown in Fig. 2.

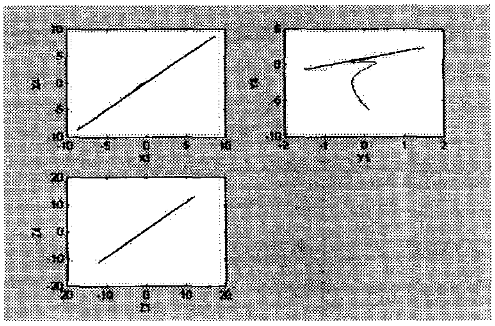

Fig. 2 The synchronization result

Fig. 2 Confirms effective synchronization result between the transmitter and receiver in the SC-CNN.

4. The secure communication of hyper-chaos circuit

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_2 term as a state variable in the transmitter state equation with SC-CNN and written as follows:

The state equation of transmitter

$$\begin{aligned} \dot{x}_1 &= -x_1 + x_1 + \alpha(x_2(I) - g_1) \\ \dot{x}_2 &= -x_2 + x_1 + x_3 \\ x_3 &= -x_3 - \beta x_2 + x_3 \\ g_1 &= m_3 x_i + 1/2\sum_{k=0}^{2}(m_k + m_{k+1})(|x_1 + c_k| - |x_1 - c_k|) \end{aligned} \qquad (9)$$

The state equation of receiver

$$\begin{aligned} \dot{x}_4 &= -x_1 + x_1 + \alpha(x_2 - g_2) \\ \dot{x}_5 &= -x_5 + x_4 + x_6 \\ x_6 &= -x_6 - \beta x_5 + x_6 \\ g_2 &= m_3 x_i + 1/2\sum_{k=0}^{2}(m_k + m_{k+1})(|x_1 + c_k| - |x_1 - c_k|) \end{aligned} \qquad (10)$$

The method we used to accomplish the secure communication was to synthesize the desired information with the hyper-chaos circuit by embedding sinusoidal signal as an information signal to the hyper-chaos signal by using an embedding in which state variable x_2 is embedding in the SC-CNN. 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].

Secure communication diagram of hyper-chaos is shown in Fig. 3. In Fig. 3, we use sinusoidal signal as an information signal and embedding it to state variables x_2 in the SC-CNN. After synchronizing the transmitter and receiver in a hyper-chaos circuit by embedding-synchronization 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. 4

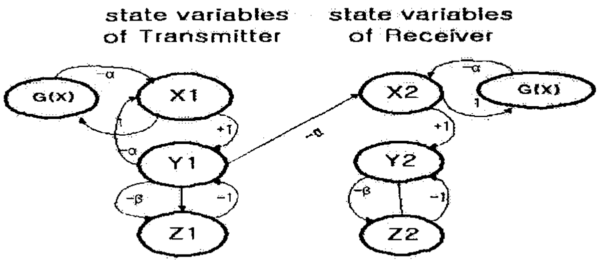

Fig. 3 Block diagram of hyper-chaos secure communication

In Fig. 4, the first part shows state x_2 with information signal embedding, the second part shows the result in the receiver, and the third part shows the recover signal.

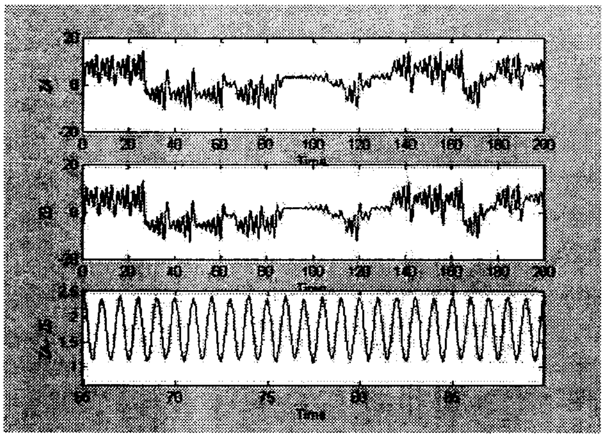

Fig. 4 Recovery signals in the SC-CNN

5. Concluding Remarks

In this paper, we introduced a hyper-chaos secure communication method which is called embedding synchronization and embedding secure communication using SC-CNN. The method in which we used to accomplish the secure communication was to synthesizing the desired information with a hyper-chaos circuit by embedding the information signal to the hyper-chaos signal by only one state variable x_2 embedding from the SC-CNN to the transmitter. As a computer simulation result, we confirm embedding secure communication method by separating the information signal and the hyper-chaos signal in the receiver with SC-CNN.

Acknowledgement

This work has been carried out under University Research Program supported by Ministry of Infor mation & Communication in republic of Korea.

Reference

[1] L. O. Chua "Chua's circuit 10 Years Later", Int. J. Circuit Theory and Application, vol. 22, no. 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.