A study on Secure Communication in Hyper-Chaos with SC-CNN using Embedding Method

Young-Chul Bae, Ju-Wan Kim, Hag-Hyun Song and **Yoon-Ho Kim**, *Member, KIMICS*

Abstract—In this paper, we introduce a hyper-chaos secure communication method using hyper-chaos circuit consist of State-Controlled Cellular Neural Network (SC-CNN). We make a hyper-chaos circuit using SC-CNN with the n-double scroll or Chua's oscillator. A hyper-chaos circuit 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. Hyper-chaos synchronization was achieved using GS (Generalized Synchronization) method between the transmitter and receiver about each state variable in the SC-CNN. In order to secure communication, we have synthesizing the desired information with a hyper-chaos circuit by adding the information signal to the hyper-chaos signal using the SC-CNN in the transmitter. And then, transmitting the synthesized signal to the ideal channel, we confirm secure communication by separating the information signal and the hyper-chaos signal in the receiver.

Index Terms—Chaos, Chaos Synchronization, Secure Communication, Hyper-chaos, Nonlinear Dynamics.

I. 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 an 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], and Chua's oscillator.

In order to make a hyper-chaos circuit, 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 hyper-chaos synchronization using GS (Generalized synchronization) method between the transmitter and receiver. 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].

II. HYPER-CHAOS CIRCUIT

To create a hyper-chaos circuit, we used to the n-double scroll or non-identical n-double scroll and Chua's oscillator using the weak coupling method [8].

A. 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

Manuscript received August 9, 2003 and accepted November 15, 2003. This work was supported by Korea Science and Engineering Foundation (KOSEF) through R05-2003-000-10618-0

Y.C. Bae is with the Division of Electron Communication and Electrical Engineering, Yosu National University, Yeosu-si, Jellnam-do, 550-749, Korea(Tel: +82-61-659-3315, Fax:+82-61-659-3310, E-mail:ycbae@yosu.ac.kr)

J.W. Kim is with the Department of Electrical Engineering, Graduate School of Yosu National University, Yeosu-si, Jellnamam-do, 550-749, Korea. (Tel: +82-61-659-3315, Fax:+82-61-659-3310, E-mail:lightntruth@hanmail.net)

H.H. Song is with the Institute of Information Technology Assessment(IITA), 52, Eoeun-dong, Yuseung-gu, Daejeon-si, 305-333,Korea. (Tel:+82-42-869-1440, Fax:+82-42-869-1079, E-mail: hhsong@iita.re.kr)

Y.H. Kim is with the Department of Computer Engineering., Mok Won University, Doan-dong 800, Seo-ku, Daejeon-si, 302-729, Korea. (Tel: +82-42-829-7633, Fax:+82-42-829-1079 E-mail:yhkim@mokwon.ac.kr)

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

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 2-double scroll attractor and 3-double scroll attractors are shown in Fig.1.

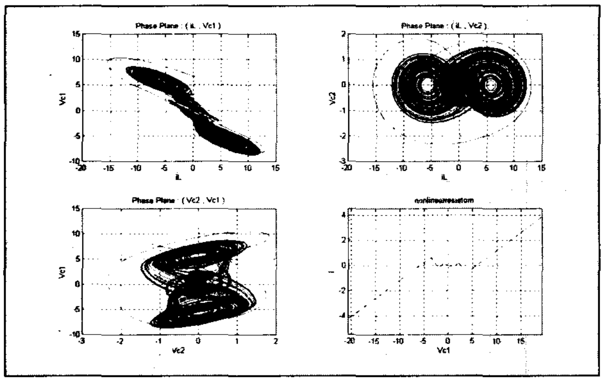


Fig. 1 2- double scroll attractor

B. 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

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

or

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

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.

Computer simulation result for hyper-chaos circuit with a CNN using n-double scroll and Chua's oscillator are shown in Fig. 2.

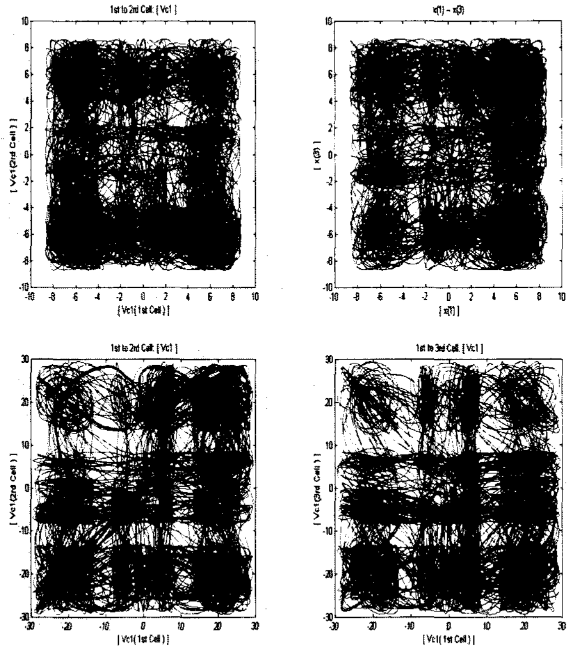


Fig. 2 Computer simulation result for hyper-chaos circuit

C. SC-CNN model [12,13]

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

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

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

$$y_j = 0.5(|x_j + 1| - |x_j - 1|) \quad (6)$$

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

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

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

$$\begin{aligned}
\dot{x}_1 &= -x_1 + a_1 y_1 + a_{12} y_2 + a_{13} y_3 + \sum_{k=1}^{3} s_{1k} x_k + i_1 \\
\dot{x}_2 &= -x_2 + a_{21} y_1 + a_2 y_2 + a_{23} y_3 + \sum_{k=1}^{3} s_{2k} x_k + i_2 \\
\dot{x}_3 &= -x_3 + a_{31} y_1 + a_{32} y_2 + a_3 y_3 + \sum_{k=1}^{3} s_{3k} x_k + i_3
\end{aligned} \tag{8}$$

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]

III. THE SYNCHRONIZATION OF HYPER-CHAOS

In order to apply to generalized synchronization theory in the hyper-chaos, we compromised to state equation of dimensionless type of SC-CNN is written as follows:

The state equation of transmitter

$$\begin{aligned}
&\dot{x} = Ax + g(x), \\
&g(x) = [g(x_1), 0, 0, g(x_4), 0, 0]^T \\
&\dot{x}' = Ax' + g'(x') + F(x, x')
\end{aligned} \tag{9}$$

The state equation of receiver

$$\begin{aligned}
&\dot{y} = Ay + g(y), \\
&g(y) = [g(y_1), 0, 0, g(y_7), 0, 0]^T \\
&\dot{y}' = A'x' + g'(y') + F(y, y')
\end{aligned} \tag{10}$$

The block diagram of the proposed hyper-chaos synchronization system is shown in Fig. 3 and the result of hyper-chaos synchronization is shown in Fig. 4 respectively

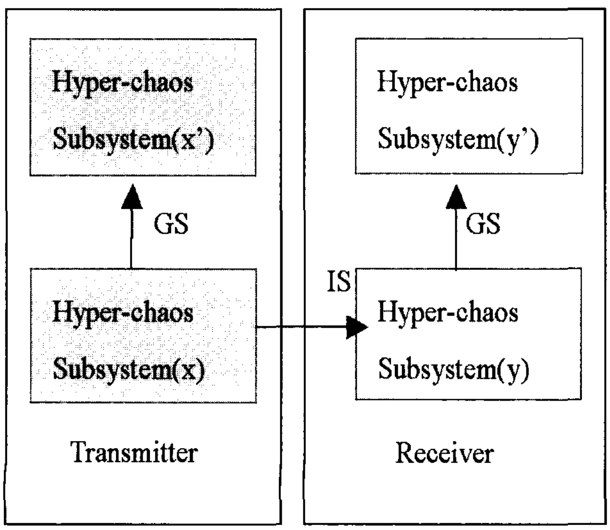
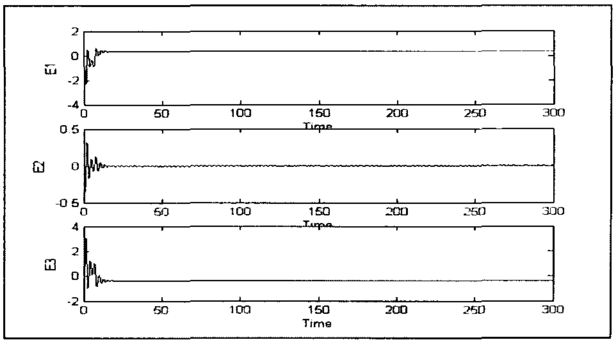
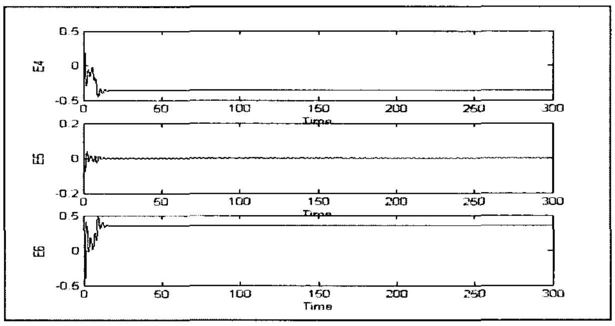


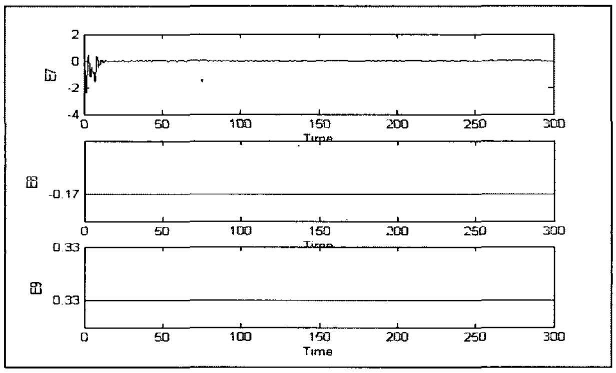
Fig. 3 The Block diagram of synchronization



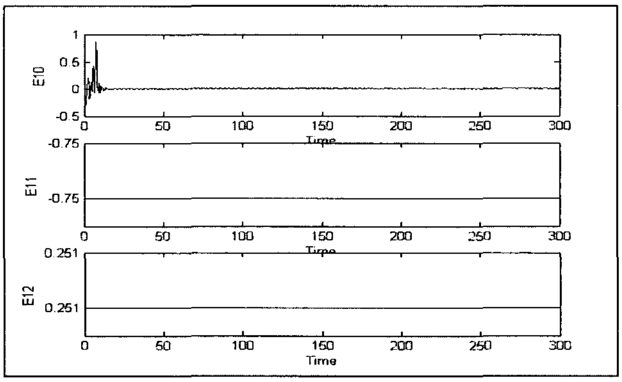
(a) $x_i - y_i (i = 1,2,3)$



(b) $x_i - y_i (i = 4,5,6)$



(c) $x'_i - y'_i \ (i = 1,2,3)$



(d) $x'_i - y'_i \ (i = 4,5,6)$

Fig. 4 The timeseries of the error of the transmitted and received signal

In the Fig. 4, we confirmed that effective synchronization result between the transmitter and receiver in the SC-CNN.

IV. THE SECURE COMMUNICATION OF HYPER-CHAOS CIRCUIT

The method we used to accomplish the secure communication was to synthesize the desired information with the hyper-chaos circuit by adding sinusoidal signal as an information signal to the hyper-chaos signal by using an adder in which state variable x_1, x_2, x_3 are added 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].

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 SC-CNN and written as follows:

The state equation of transmitter

$$\begin{aligned} &\dot{x} = Ax + g(w) \\ &g(w) = [g(x_1 + 0.1\sin(2\pi f))\ \ 0\ \ 0\ \ g(x_4)\ \ 0\ \ 0] \\ &\dot{x}' = Ax' + g(x') + F(x, x') \end{aligned} \tag{11}$$

The state equation of receiver

$$\begin{aligned} &\dot{y} = Ay + g(y) \\ &g(y) = [g(y_1)\ \ 0\ \ 0\ \ g(y_7)\ \ 0\ \ 0] \\ &\dot{y}' = Ay' + g(y') + F(y, y') \end{aligned} \tag{12}$$

Proposed secure communication diagram of hyper-chaos is shown in Fig. 5.

In Fig. 5, we use sinusoidal signal as an information signal and shown Fig. 6, and add it to state variables x_1 and x_3 in the SC-CNN.

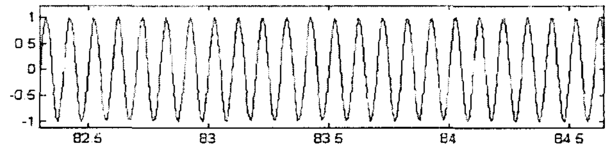


Fig. 6 Information signal

Fig. 7 and 8 are shown that the result of adding the information signal to state variable x_1 and x_3.

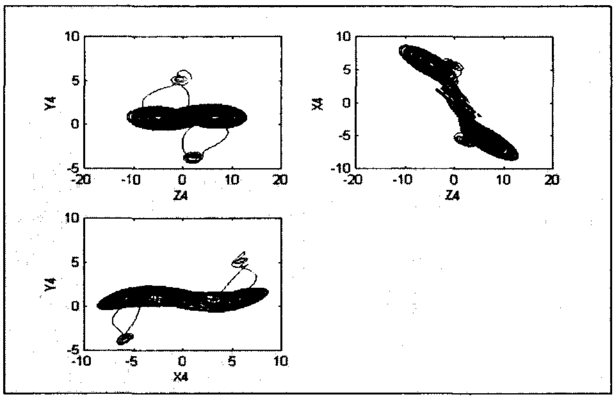


Fig. 7 The result of adding the information signal to state variable x_1

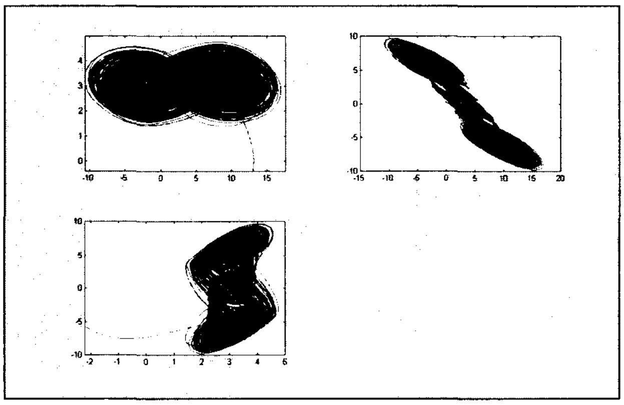


Fig. 8 The result of adding the information signal to state variable x_3

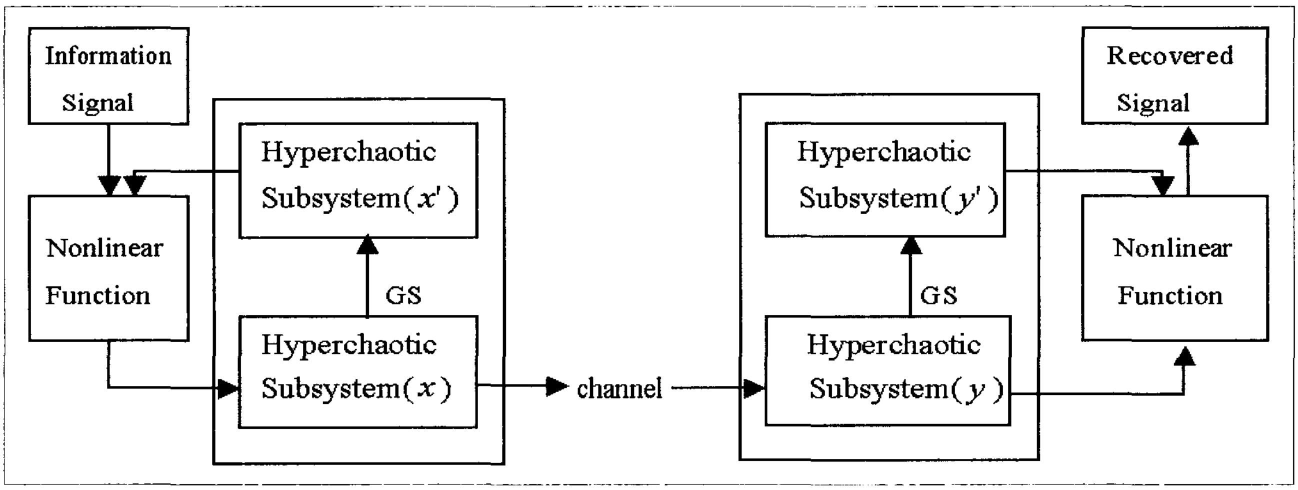


Fig. 5 Block diagram of hyper-chaos secure

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. 9 and 10, respectively.

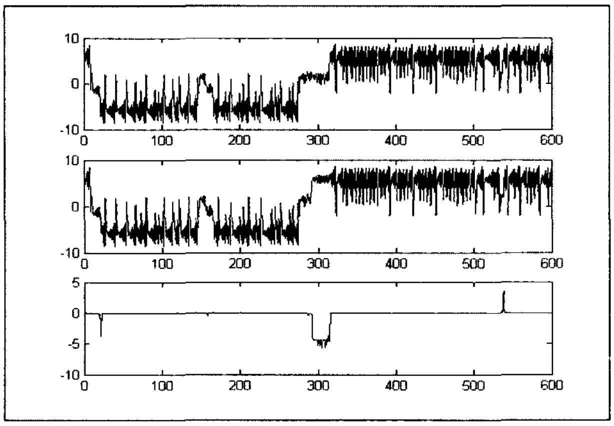


Fig. 9 The result of recovery information signal of state variable x_1

In Fig. 9, 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.

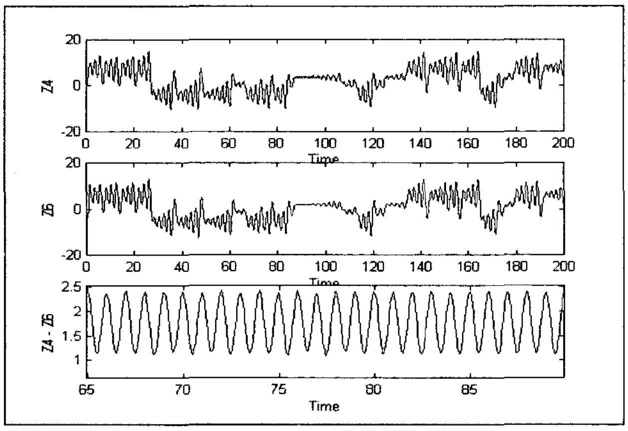


Fig. 10 The result of recovery information signal of state variable x_3

In Fig. 10, 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 SC-CNN. It is clear that state variable x_3 is superior to state x_1 or x_2 as a carrier signal in the SC-CNN. 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.

IV. CONCLUSIONS

In this paper, we introduced a hyper-chaos secure communication method which is called GS (Generalized synchronization) and embedding secure communication using SC-CNN. The method in which after we accomplished synchronization between the transmitter and receiver in the hyper-chaos circuit using GS method, 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_3 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.

ACKNOWLEDGMENT

This work has been carried out under University Research Program supported by Ministry of Information & Communication in Republic of Korea

REFERENCES

[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.

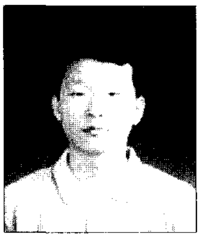
[15] M. Brucoli, D. Cafagna, L. Carnimeo & G. Grassi, "An efficient technique for signal masking using synchronized hyperchaos circuits", *Proc. 5th Int. workshop on Nonlinear Dynamics of Electronic Systems(NDES '97)*, Moscow, Russia, June 26-27, pp. 229-232, 1997.

[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.

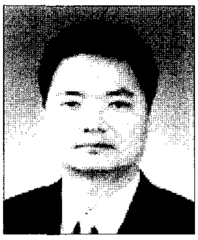
Young-Chul Bae

received his B.S degree, M.S and Ph. D. degrees in Electrical Engineering from Kwangwoon University in 1984, 1986 and 1997, respectively. From 1986 to 1991, he joined at KEPCO, where he worked as Technical Staff. From 1991 to 1997, he joined Korea Institute of Science and Technology Information (KISTI), where he worked as Senior Research. In 1997, he joined the Division of Electron Communication and Electrical Engineering, Yosu National University, Korea, where he is presently a professor. His research interest is in the area of Chaos Nonlinear Dynamics that includes Chaos Synchronization, Chaos Secure Communication, Chaos Crypto Communication, Chaos Control and Chaos Robot etc.



Ju-Wan Kim

He was born in Yosu, South Korea, on October 21, 1972. He received the B.E degree in Electronic Engineering from Sunchon Naiotnal University in 1998 and works currently under M.E course in Yosu National University, since 2001. He interests in chaos synchronization, secure communication, chaos robot.



Hag-Hyun Song

Received B.S degree in Public Administration from Korea National Open University, in Seoul in 1991, and M.S degree in electronic engineering from Seoul National University of Technology in 1996 and 1998, respectively. Since 1991, he has been a Assistant Director for Ministry of Information and Communication(MIC). He is currently a team leader and senior researcher for Institute of Information Technology Assessment(IITA). His current research interests include image processing, computer vision, neuro-fuzzy system, chaos and IT policy.

Yoon-Ho Kim

Received the B.S degree in Electronic Engineering from Chong Ju Univ. and M. S. degree in electronic engineering from Kyung Hee Univ. in 1986, and the Ph. D. degree in electronic engineering in 1992 from the Chong Ju Univ., respectively. In 1992, He joined the faculty of the Mok Won Uni., where he is currently an Associate Professor in the Department of Computer Engineering. His research interests focus on image processing, including pattern recognition, computer vision, fuzzy inference technologies, and neural network applications. he is a member of IEEE, IEEK, KICS and KIMICS.