SC-CNN을 이용한 하이퍼카오스 회로에서의 비밀 통신

배영철* · 김주완*

*여수대학교

The Secure Communication of Hyper-chaos circuit using SC-CNN

Youngchul Bae* · Juwan Kim**

*Yosu University

E-mail : ycbaebyc@hanmail.net

요 약

본 논문에서는 하이퍼카오스 회로에서의 비밀통신 방법을 제시한다. 하이퍼카오스 회로는 n-double scroll CNN 회로를 이용하였으며, 동일한 2개 또는 4개의 셀을 가진 n-double scroll 회로를 이용하여 송·수신부를 구성하고 이 송·수신부 사이에 구동 동기를 이용한 동기화를 이루었으며, 상태 변수 x_3에 의한 비밀통신이 상태 변수 x_2, x_1에 의한 방법보다 우수함을 보였다.

ABSTRACT

A hyper-chaos circuit is created by applying identical n-double scrolls with weak coupled method, to each cell. Hyper-chaos synchronization was achieved using drive response synchronization between the transmitter and receiver about each state variable in the SC-CNN. From result of the recovery signal through the demodulation method in the receiver, We shown that recovery quality of state variable x_3 is superior to that of x_2, x_1 in secure communication.

키워드

hyperchaos, SC_CNN, Secure Communication

Ⅰ. 서 론

최근에 카오스 현상에 대한 관심이 물리학, 화학, 생물학, 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다. Chua 회로는 매우 단순한 자율, 3차 시스템으로 가역성을 가지며 1개의 비선형 소자인 3구분 선형 저항(3 - segment piecewise - linear resistor)과 4개의 선형 소자인 (R, L, C1, C2)로 구성되는 발진회로다.

Chua 회로는 확률적 공진(stochastic resonance), 신호 증폭, 1/f 잡음 현상, 카오스 간헐성(intermittency), 주기 배증(periodic doubling), 주기 가산(periodic Adding), autowave, 나선형파(spiral wave), 자기유사성(self-similarity), 보편성(university) 등의 현상이 관찰되고 있어 카오스 및 그 응용 연구에 중요한 역할을 하고 있다.

Matsumoto에 의해 제안된 Chua 회로[1]을 그림 1에 나타냈으며 상태방정식은 식(1)과 같이 표시된다.

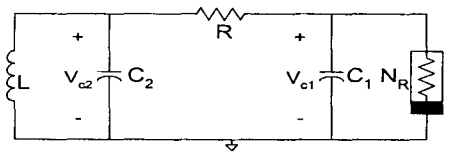

그림 1. Chua 회로

Fig. 1 Chua's circuit

$$C_1\frac{dv_{C_1}}{dt} = G\,(v_{C_2} - v_{C_1}) - g(v_{C_1})$$

$$C_2\frac{dv_{C_2}}{dt} = G\,(v_{C_1} - v_{C_2}) + i_L \qquad (1)$$

$$L\frac{di_L}{dt} = -v_{C_2}$$

여기서 $G = 1/R$, $g(\cdot)$은 식 (2)와 같이 표현되는 3구분 선형 함수 (3- segment piecewise-linear function) 이며 그림 2에 나타내었다.

$$g(v_R) = m_0 v_R + \frac{1}{2}(m_1 - m_0)[|v_R + B_P| - |v_R - B_P|] \quad (2)$$

여기서 m_0 는 외부 영역의 기울기, m_1 은 내부 영역의 기울기, $\pm B_P$ 는 break-point이다.

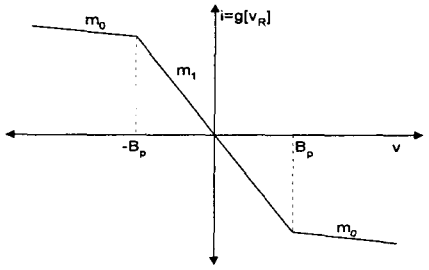

그림 2. 비선형 저항의 전압 전류 특성
Fig. 2 v-i characteristic of nonliner resistor

Chua 회로는 잡음과 같은 카오스 특성을 이용하여 카오스 신호에 정보 신호를 혼합하여 송신부에서 전송한 후 수신부에서 정보 신호와 카오스 신호를 분리하는 카오스 암호통신에 주로 이용하고 있으나[5,6] 카오스 신호 자체의 동특성으로 인하여 완벽하게 정보를 보호하지 못하고 도청되는 것으로 알려져 있다[8,9]. 따라서 카오스 신호보다 도청의 우려가 없는 더 복잡한 하이퍼카오스 신호를 이용하면 도청의 우려없이 정보신호를 원하는 장소까지 실어 보낼 수 있으나 하이퍼카오스 신호를 생성하기 위한 장치와 비밀 통신을 실행하기 위한 송수신부 동기화 기법의 어려움으로 연구가 활발하지 못한 실정이다.

이에 본 연구에서는 Chua 회로를 변형한 SC-CNN 회로를 이용하여 하이퍼카오스 회로를 구성하고, 이 하이퍼카오스 회로에서 비밀 통신 방법을 제안한다. 제안한 방법중 상태 변수 x_3에 정보 신호를 실어 보냈을 때가 상태변수 x_2, x_1에 비해 복조 효과가 우수함을 보였다.

II. 하이퍼카오스 회로

2-1. n-double scroll 회로

하이퍼카오스 회로를 얻기 위하여 Chua 회로의 변형인 n-double scroll 어트렉터를 고려하였다. n-double scroll을 얻기 위한 전기회로는 Arena[12]에 의해 구현되었으며 상태방정식은 식(3)과 같이 주어지고 비선형 저항의 관계식은 식(4)에 나타내었다.

$$\begin{aligned} \dot{x} &= \alpha[y - h(x)] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \quad (3)$$

$$h(x) = m_{2n-1}x + \frac{1}{2}\sum_{i=1}^{2n-1}(m_{i-1} - m_i)(|x + c_i| - |x - c_i|) \quad (4)$$

식(4)는 2(2n-1)개의 breakpoint를 가지며 $\alpha = 9, \beta = 14.286$ 할 때, 식(4)에서의 기울기와 파라미터의 값에 따라 여러 가지 n-double scroll이 발생하게 된다.

1) 1-double scroll

$m_0 = -1/7, \quad m_1 = 2/7, \quad c_1 = 1$

2) 2-double scroll

$m_0 = -1/7, \quad m_1 = 2/7, \quad m_2 = -4/7, \quad m_3 = m_1, \quad c_1 = 1, \quad c_2 = 2.15, \quad c_3 = 3.6$

3) 3-double scroll

$m_0 = -1/7, \quad m_1 = 2/7, \quad m_2 = -4/7, \quad m_3 = m_1, \quad m_4 = m_2, \quad m_5 = m_3, \quad c_1 = 1, \quad c_2 = 2.15, \quad c_3 = 3.6, \quad c_4 = 8.2, \quad c_3 = 13$

그림 3에 2-double scroll 어트렉터와 비선형 저항을 그림 4에 3-double scroll 어트렉터와 비선형 저항을 각각 나타내었다.

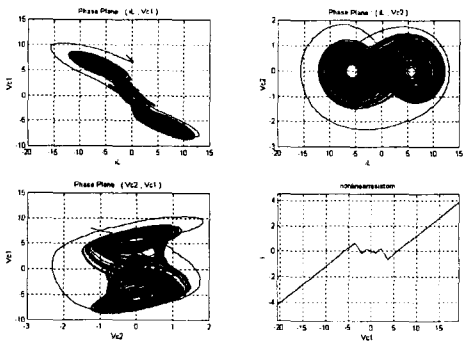

그림 3. 2-double scroll 위상공간과 비선형 저항
Fig. 3 phase plane of 2-double scroll and nonlinear resistor

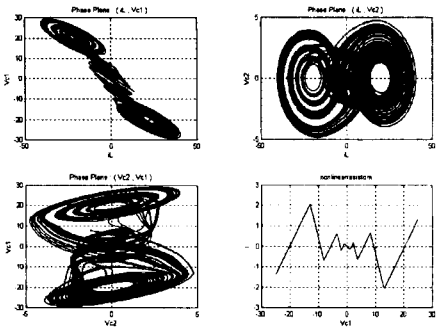

그림 4. 3-double scroll 위상공간과 비선형 저항
Fig. 4 phase plane of 3-double scroll and nonlinear resistor

2-2. 하이퍼카오스 회로

하이퍼카오스를 구성하기 위해서는 동일한 n-Double scroll 셀로 구성된 1차원의 셀룰러 신경망(CNN)의 회로로 구성하고 셀 사이를 서로 결합하여야만 한다. 셀 사이를 결합하는 결합 방법에는 단방향 결합(unidirectional coupling)과 확산 결합이 있으나[7], 본 연구에서는 확산 결합을 이용하여 하이퍼카오스 회로를 구성하였다. n-double scroll 셀들을 가진 1차원 CNN을 구성하기 위한 관계식을 식(5)에 x-확산 결합, 식(6) y-확산 결합식으로 나타내었다.

$$\begin{aligned} x^{(j)} &= \alpha[y^{(j)} - h(x^{(j)}] \\ &\quad + D_x(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ y^{(j)} &= x^{(j)} - y^{(j)} + z^{(j)} \\ z^{(j)} &= -\beta y^{(j)}, \qquad j = 1,2,.....L \end{aligned} \tag{5}$$

$$\begin{aligned} x^{(j)} &= \alpha[y^{(j)} - h(x^{(j)}] \\ y^{(j)} &= x^{(j)} - y^{(j)} + z^{(j)} \\ &\quad + D_y(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ z^{(j)} &= -\beta y^{(j)}, \qquad j = 1,2,.....L \end{aligned} \tag{6}$$

여기서 L은 셀의 수를 나타낸다.

2-3. SC-CNN 모델[12,13]

문헌[12,13]에서 다음과 같은 일반화된 셀 모델을 만들 수 있다.

(7)

여기서 j는 셀 수, x_j는 상태 변수, y_j는 셀 출력수를 나타내며 다음 식과 같이 주어진다.

$$y_j = 0.5(|x_j + 1| - |x_j - 1|) \tag{8}$$

여기서 a_j는 상수 파라미터, i_j는 임계값(threshold value)이다.

식(7)에서 G_o는 출력의 선형 조합이며, G_s는 연결 셀의 상태 변수이다. 식 (8)의 출력 비선형성 생성은 식(8)과 같은 새로운 출력 PWL 방정식을 고려한다.

$$y_j = \frac{1}{2}\sum_{k=1}^{2n-1} n_k(|x + b_k| - |x - b_k|) \tag{9}$$

여기서 b_k는 차단점(break point)이며 n_k는 선형 구간의 기울기와 관련된 계수이다.

SC-CNN 셀은 상태 방정식(7)과 출력 방정식(9)의 조합으로 식 (10)과 같은 n-Double scroll을 만들 수 있다.

$$\begin{aligned} \dot{x}_1 &= -x_1 + a_1 y_1 + a_{12} y_2 + a_{13} y_3 + \sum_{k=1}^{3} s_{1k} x_k + i_1 \\ \dot{x}_2 &= -x_2 + a_{21} y_1 + a_2 y_2 + a_{23} y_3 + \sum_{k=1}^{3} s_{2k} x_k + i_2 \\ \dot{x}_3 &= -x_3 + a_{31} y_1 + a_{32} y_2 + a_3 y_3 + \sum_{k=1}^{3} s_{3k} x_k + i_3 \end{aligned} \tag{10}$$

여기서 x_1, x_2, x_3는 상태 변수이며, y_1, y_2, y_3는 이에 대응한 출력 변수이다.

III. 하이퍼카오스 회로 비밀 통신

SC-CNN 하이퍼카오스 회로의 동기화를 위하여 동일한 SC-CNN 회로를 송·수신부로 놓고 정보 신호를 각 상태에 실어서 송신부에서 전송 한 후 수신부에서 이를 복원하는 방법을 제안하였다.

정보 신호로는 정현파를 이용하였으며, 이 정보신호를 하이퍼카오스 신호인 SC-CNN의 각 상태 변수 x_1, x_2, x_3에 더하여 송신하고 수신기에서 복조하였으며 각 상태 변수에 따른 복원 결과를 확인하였다.

그림 5에 SC-CNN을 이용한 하이퍼카오스 비밀통신 회로 블록 다이어그램을 나타내었다.

그림 6에 정보 신호를 상태변수 x_1의 하이퍼카오스 신호를 합성하고 송신부와 수신부의 동기화에 따른 어트렉터를 나타내었다.

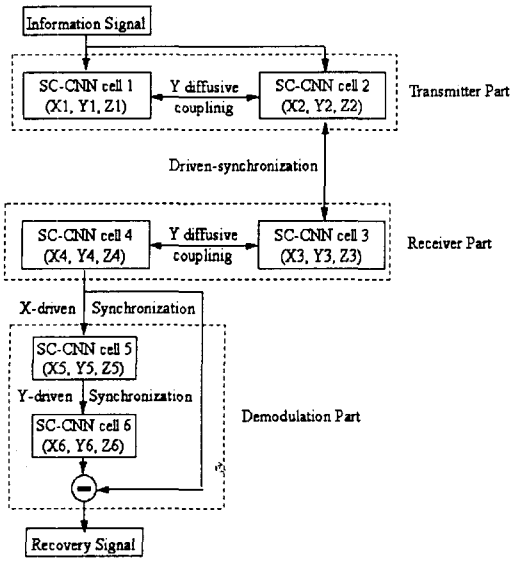

그림 5. 하이퍼카오스 회로의 동기화 개략도

Fig. 5 The block diagram of hyper-chaos secure communication

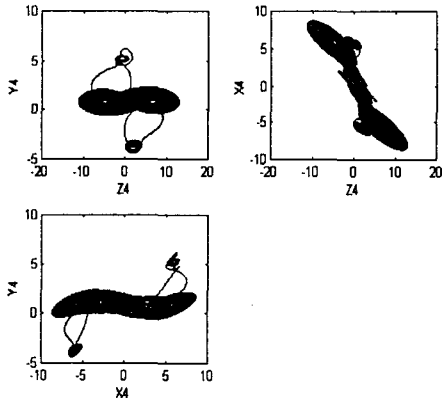

그림 6. 정보 신호를 상태변수 x_1에 합성하였을 때의 어트렉터

Fig. 6. the result of adding the information signal to state variable x_1

그림 7에 정보 신호를 상태변수 x_3의 하이퍼카오스 신호를 합성하고 송신부와 수신부의 동기화에 따른 어트렉터를 나타내었다.

그림 7과 8을 비교해 보면, 상태 변수 x_3를 사용한 경우 x_1에 비하여 어트렉터 구성이 단순함을 알 수 있으며, 이는 복조시 보다 완벽한 복조 성능과도 관계됨을 확인할 수 있다.

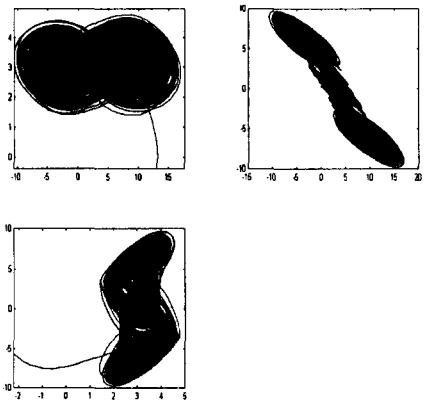

그림 7. 정보 신호를 상태변수 x_3에 합성하였을 때의 어트렉터

Fig. 7. the result of adding the information signal to state variable x_3

그림 8에 그림 5에 의한 하이퍼카오스 회로의 중 상태변수 x_1에 의한 비밀 통신 결과를 나타내었다.

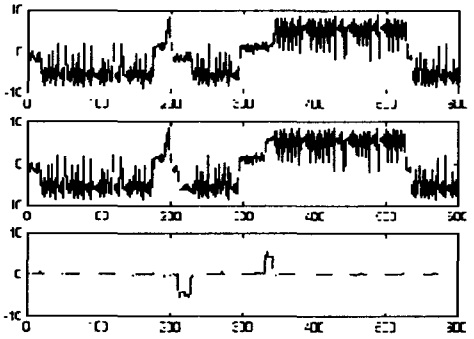

그림 8. 상태 변수 x_1에 의한 비밀 통신 복원 결과

Fig 8. Recovery signal about state variable x_1 in the SC-CNN.

그림 9에 그림 5에 의한 하이퍼카오스 회로의 중 상태변수 x_3에 의한 비밀 통신 결과를 나타내었다.

그림 8과 그림 9를 비교해 보면 상태변수 x_3를 이용한 경우가 복조 성능이 우수함을 확인할 수 있었다.

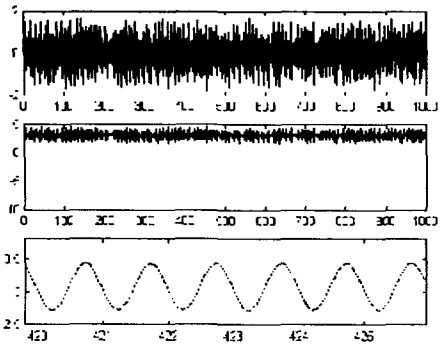

그림 9. 상태 변수 x_3에 의한 비밀 통신 복원 결과

Fig. 9. The recovery signal about state variable x_3 in the SC-CNN

IV. 결 론

본 연구에서는 SC-CNN을 이용한 하이퍼카오스를 비밀통신에 대하여 살펴보았다. 정보신호를 하이퍼카오스 신호와 합성할 때 상태 변수 $x_1.x_2.x_3$를 이용하였으며, 이들 각각의 복조 결과를 비교하였다. 상태 변수 x_3에 의한 방법은 Chua 회로에서는 하드웨어 구현의 불가능으로 이용하지 못한 방법이었으나 하이퍼카오스 회로에서는 이용할 수 있는 방법임을 제시하였다. 앞으로 강건한 동기화와 음성 및 디지털 통신에 적용할 수 있는 범용적인 하이퍼카오스 회로와 동기화 기법, 비밀 통신 복조 기법 등이 연구 과제로 남는다.

참고문헌

[1] T. Matsumoto, "A Chaotic Attractor from Chua's circuit", IEEE Trans. on Circuit and System, vol. CAS-31, pp. 1055 - 1058, 1984.

[2] 배영철, 고재호, 임화영, "Chua 회로에서의 Bifurcation과 Attractor", 대한전기학회 하계 학술대회 논문집, pp..664 - 666, 1995.

[3] 배영철, 고재호, 임화영, "구분 선형 함수의 최적 구현에 관한 연구", 한국자동제어학술 회의 논문집, pp. 370 - 373, 1995.

[4] 배영철, 고재호, 임화영, "Chua 회로에서의 파라미터 변화에 의한 Period-doubling과 Bifurcation에 관한 연구", 한국 자동제어 학술 회의 논문집, pp. 482 - 485, 1995.

[5] 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.

[6] 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.

[7] 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.

[8] L. O. Chua "Chua's circuit 10 Years Later", Int. J. Circuit Theory and Application, vol. 22, no. pp 79-305, 1994

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

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

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

[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, Chuas circuit can be generated by CNN cell, IEEE Trans. Circuit and Systems I, CAS-42, pp. 123-125. 1995.

[14] 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.

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

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