

N-double scroll을 이용한 하이퍼카오스 회로에서의

카오스 동기화

배영철, 김주완

여수대학교

Secure Communication using N-double scroll in HyperChaos circuit.

Young-Chul Bae, Ju-Wan Kim

Nat'l Yosu University

E-mail : ycbae@yosu.ac.kr

요약

최근 카오스현상에 대한 연구가 지속적으로 이루어지고 있다. 카오스 현상을 이용하여 많은 분야에서 다양하게 연구되고 많은 응용기술이 개발되고 있다. 본 논문에서는 1차원 CNN을 구성하여 하이퍼카오스 신호를 생성하고 하이퍼카오스 동기화 구현하는데 초점을 맞추었다.

ABSTRACT

Nowadays there are being done many researches on chaos phenomenon among many kinds of people. Currently, already many applications has been developed, and they applied this phenomenon to engineering problem. now we have tried to make it possible to use secure communication through hyperchaotic synchronization system using 1-dimensional CNN(Cellular Neural Network). we focused on materializing secure communication.

키워드

카오스, 하이퍼카오스, CNN, 동기화, 암호 통신

I. 서론

Chua 회로는 잠음과 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 N-Double scroll 회로를 이용하여 하이퍼카오스 회로를 구성하고, 동일한 하이퍼카오스 회로를 송수신부로 정한 후 하이퍼카오스 회로의 송신부와 수신부 회로의 신호가 일치하도록 하는 하이

퍼카오스 동기화 기법을 제안하고 그 타당성을 검증하였다.

II. n-double scroll 회로

하이퍼카오스 회로를 얻기 위하여 Chua 회로의 변형인 n-double scroll 어트랙터를 고려하였다. n-double scroll을 얻기 위한 전기회로는 Arena에 의해 구현되었으며 상태방정식은 식(1)과 같이 주어지고 비선형 저항의 관계식은 식(2)에 나타내었다.

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

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

식(2)는 $2(2n-1)$ 개의 breakpoint를 가지며 $\alpha=9, \beta=14.286$ 라 할 때, 식(2)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

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

3) 3-double scroll

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

그림 1에 2-double scroll에 사용하는 비선형 저항을 그림2에 3-double scroll의 비선형 저항을, 그림 3에 2-double scroll 어트랙터를 각각 나타내었다.

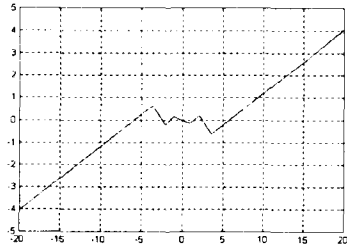


그림 1. 2-double scroll 비선형저항
Fig. 1 Nonlinear resistor of 2-double scroll

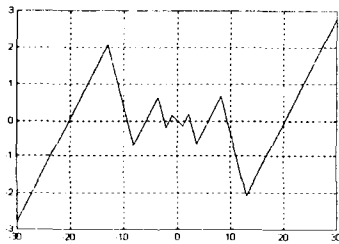


그림 2. 3-double scroll 비선형저항
Fig. 2 Nonlinear resistor of 3-double scroll

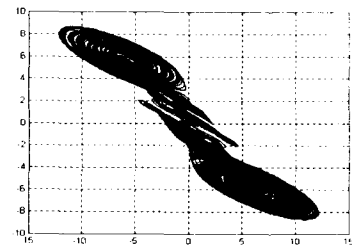
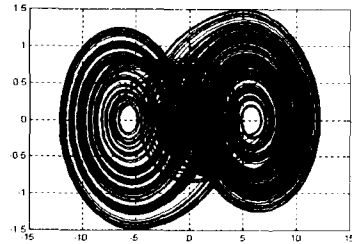
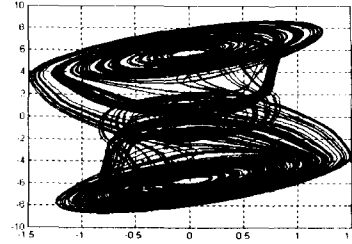


그림 3. 3-double scroll 회로의 어트랙터
Fig. 3 Attractor of 3-double scroll circuit

III. 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(3)에 x-확산 결합, 식(4) y-확산 결합식으로 나타내었다.

$$x^{(j)} = a[y^{(j)} - h(x^{(j)}) + D_x(x^{(j-1)} - 2x^{(j)} + x^{(j+1)})] \\ y^{(j)} = x^{(j)} - y^{(j)} + z^{(j)} \quad (3) \\ z^{(j)} = -\beta y^{(j)}, \quad j=1,2,\dots,L$$

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

여기서 L은 셀의 수를 나타낸다.

식(4)을 이용하여 구성한 하이퍼카오스 어트랙터를 그림 4 ~ 그림 5에 나타내었다. 그림 4는 2-double scroll 시스템의 2개의 CNN을 이용한 하이퍼카오스 어트랙터를, 그림 5는 3-double scroll 시스템의 4개의 CNN을 이용한 하이퍼카오스 어트랙터를 각각 나타내었다. 2-double scroll 시스템의 4개의 CNN과 3-double scroll 시스템의 2개의 CNN을 이용한 것들에서도 비슷한 형태의 결과를 가져왔다.

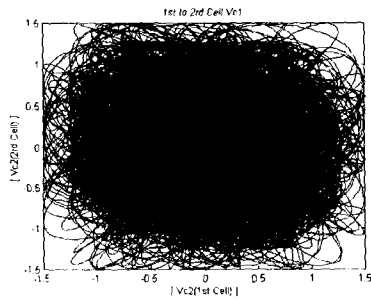
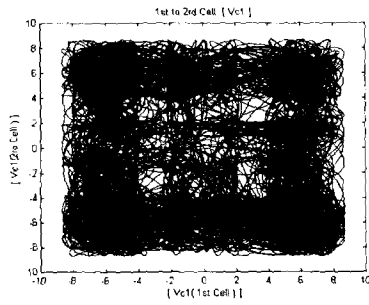


그림 4. 2-double scroll 시스템의 2개의 CNN을 이용한 하이퍼카오스 어트랙터
Fig. 4 Hyper-chaotic attractor using 2 CNNs of 2 double scroll system

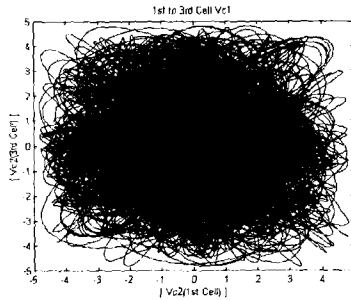
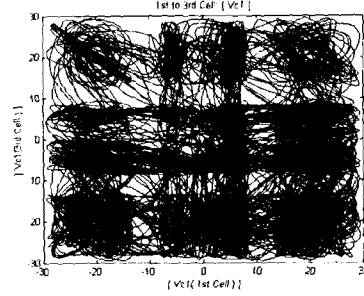


그림 5. 3-double scroll 시스템의 4개의 CNN을 이용한 하이퍼카오스 어트랙터
Fig. 5 Hyper-chaotic attractor using 4 CNNs of 3-double scroll system

IV. 하이퍼카오스 회로 동기화

n-double scroll 하이퍼카오스 회로의 동기화를 위하여 동일한 n-double scroll 회로를 송수신부로 놓고 결합동기에 의한 동기화를 이루었다. 송신부의 상태방정식은 식(5)와 같으며 수신부의 상태방정식은 식(6)과 같다.

송신부의 상태방정식

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

수신부의 상태방정식

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

$$z^{(j)} = -\beta y^{(j)}, \quad j=1,2,\dots,L$$

본 연구에서는 동일한 2개의 2-double scroll 시스템의 2 CNN을 이용하여 송신부와 수신부를 구성한 후 송신부와 수신부의 시스템이 안정하도록 차 시스템(difference system)을 이용하여 결합 계수를 결정하면 $K < -1.3$ 의 범위에서 동기화가 이루어진다.

그림 6와 7에 동일한 2개의 2-double scroll 시스템의 2 CNN에 대한 하이퍼카오스 회로의 동기화 결과를 나타내었다. 그림 6은 동기화 척도로 동일한 시계열 데이터를 겹쳐 놓은 것으로 일치선으로 나타낼 때 동기화가 완전하기 이루어진 것으로 판단한다. 그림 6의 결과에서는 일정시간 동안 동기화를 이루기 못하다가 동기화가 이루어짐을 알 수 있다.

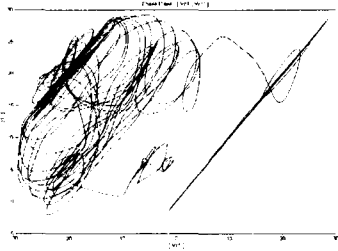


그림 6. 동기화 결과

Fig. 6 The result of synchronization

그림 7은 송수신부의 시계열 데이터의 차를 나타낸 것으로 그림 7에서 확인하듯이 처음에는 동기화가 이루어지지 않았다가 일정시간이 지난 후 동기화가 이루어졌음을 알 수 있다.

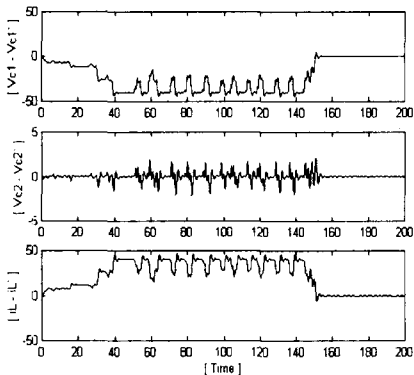


그림 7. 송수신 시계열 데이터 차

Fig. 7 The difference of time-series data between the transmitter and receiving

V. 결론

본 연구에서는 하이퍼카오스를 이용한 동기화 기법에 대하여 살펴보았다. 일반적인 카오스 회로에서와 같이 하이퍼카오스 회로에서도 동기화가 이루어짐을 확인하였으며 이를 이용한 비밀 통신이 과제로 남는다.

* 본 연구는 ETRI 부설 국가보안연구소 지원에 의한 것이며 관계자 여러분에게 감사 드립니다.

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", 한국자동제어학회 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, " Experimental 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] K.M. Cuomo, A.V. Oppenheim & S.H. Strogatz " Robustness and signal recovery in a synchronized chaotic system" Int. J. Bifurcation and Chaos, vol. 3, no. 7, pp. 1629-1638, 1993.
- [9] K.M. Short "Signal extraction from chaotic communication" Int. J. Bifurcation and Chaos, vol. 7, no. 7, pp. 1579-1597, 1997.