N-double scroll을 이용한 하이퍼카오스 회로에서의 암호 통신

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

요 약

최근 카오스현상에 대한 연구가 지속적으로 이루어지고 있다. 카오스 현상을 이용하여 많은 분야에서 다양하게 연구되고 있는바 본 논문에서는 1차원 CNN을 구성하여 하이퍼카오스 신호를 생성하고 하이퍼카오스 동기화에 기반을 둔 암호화 통신을 적용하여 구현하는데 초점을 맞추었다.

ABSTRACT

Nowadays there are being done many researches on chaos phenomenon among an assortment of group. Currently, already many applications has been developed, applying this phenomenon to engineering problem. now we are to show how we achieved 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. 서 론

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 하이퍼카오스 회로를 이용하여 하이퍼카오스 동기화를 통한 비밀 통신 기법을 제안하고자 한다.

II. n-double scroll 회로

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

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

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

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

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

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

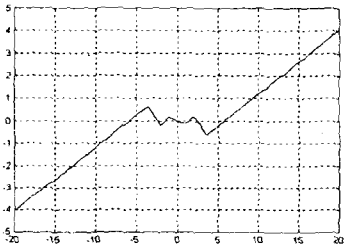


그림 1. 2-double scroll 비선형저항

Fig. 1 Nonlinear resistor of 2-double scroll

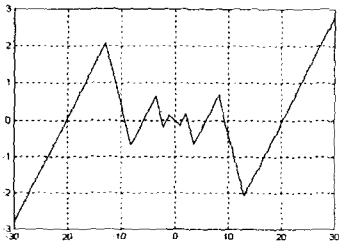


그림 2. 3-double scroll 비선형저항

Fig. 2 Nonlinear resistor of 3-double scroll

III. 하이퍼카오스 회로

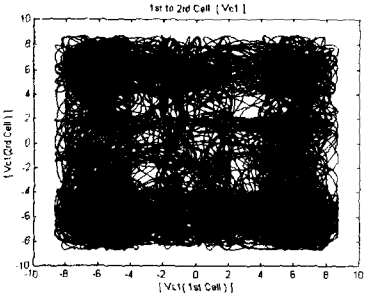
하이퍼카오스를 구성하기 위해서는 동일한 n-Double scroll 셀로 구성된 1차원의 셀룰러 신경망(CNN)의 회로로 구성하고 셀 사이를 서로 결합하여야만 한다. 셀 사이를 결합하는 결합 방법에는 단방향 결합(unidirectional coupling)과 확산 결합이 있으나[7], 본 연구에서는 확산 결합을 이용하여 하이퍼카오스 회로를 구성하였다. n-double scroll 셀들을 가진 1차원 CNN을 구성하기 위한 관계식을 식(3)에 x-확산 결합, 식(4) y-확산 결합식으로 나타내었다.

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

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

여기서 L은 셀의 수를 나타낸다.

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



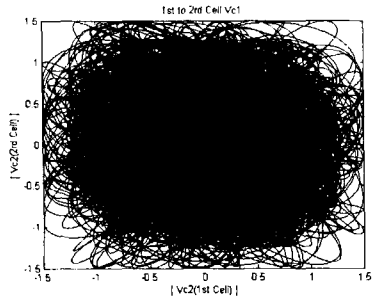


그림 4. 2-double scroll 시스템의 2개의 CNN을 이용한 하이퍼카오스 어트렉터
Fig. 4 Hyper-chaotic attractor using 2 CNNs of 2 double scroll system

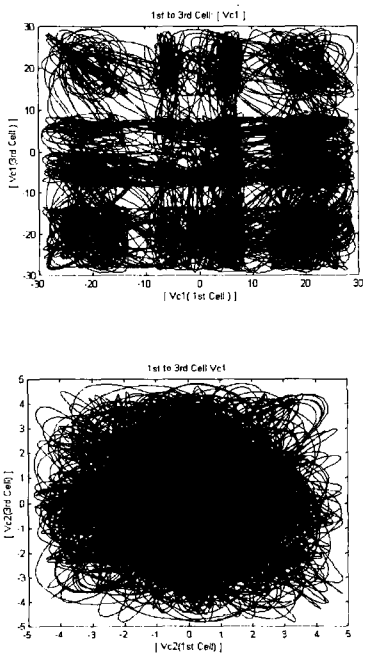


그림 5. 3-double scroll 시스템의 4개의 CNN을 이용한 하이퍼카오스 어트렉터
Fig. 5 Hyper-chaotic attractor using 4 CNNs of 3-double scroll system

Ⅳ. 하이퍼카오스 회로 비밀 통신

하이퍼카오스 비밀통신을 위해서 본 연구에서는 두 개의 동일한 2- double scroll 2 CNN 하이퍼카오스 회로를 이용하여 송수신부를 구성한 후 송수신수 결합동기에 의한 동기화를 이룬 후 송신부의 복잡한 하이퍼카오스 회로에 정보신호를 가산하여 채널을 통하여 수신부로 전송한 후 수신부에서 정보 신호와 하이퍼카오스 신호를 분리하는 복조 방법을 행하였다. 정보 신호는 정현파를 이용하였다.
그림 6에 하이퍼카오스 비밀 통신에 대한 흐름도를 나타내었다.

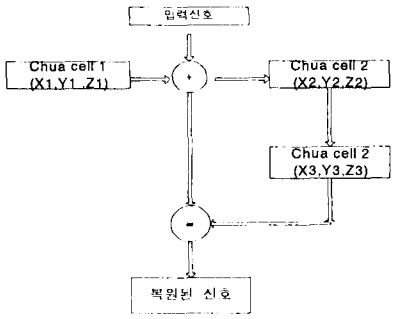


그림 6. 하이퍼카오스 비밀 통신 흐름도
Fig. 6 The Flowchart of hyperchaos secure communication

그림 7에 송신부에서 캐리어로 이용한 하이퍼카오스 신호의 시계열 데이터를 나타내었으며 그림 8에 정현파의 정보 신호를 나타내었다.

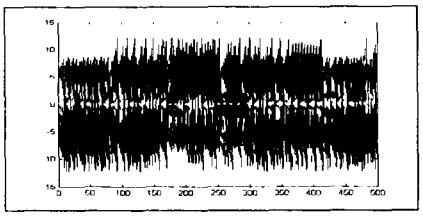


그림 7. 송신부의 캐리어 신호
Fig. 7 The carrier signal of transmitter

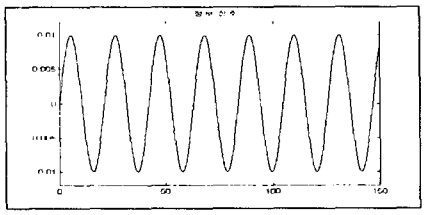


그림 8. 정보 신호
Fig. 8 The information signal

그림 7과 8을 합성하여 합성된 신호를 채널을 통하여 수신부에 전송하고 동기화 기법으로 송수신부를 동기화 시킨 후 수신부의 동기화된 신호에

서 캐리어 신호와 정보 신호를 분리하는 방법을 행하였다. 본 연구에서는 채널을 잡음과 왜곡이 없는 이상적인 채널로 가정하였다.
그림 9는 채널 중간에서 도청한 신호이다. 도청된 신호는 하이퍼카오스 신호로 적당한 신호 처리를 하여도 정보 신호를 복원하지 못하는 것을 알려져 있다.

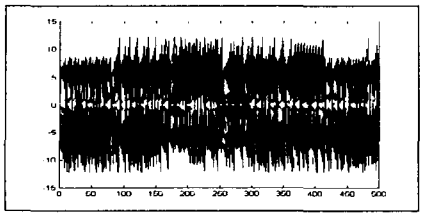


그림 9 중간에 도청한 신호
Fig. 9 The wiretapped signal during transmission

그림 10은 정보 신호와 캐리어 신호를 수신부에서 분리 복조한 신호이다. 그림 10에서 보는 바와 같이 잡음이 많이 포함되어 있음을 확인 할 수 있다.

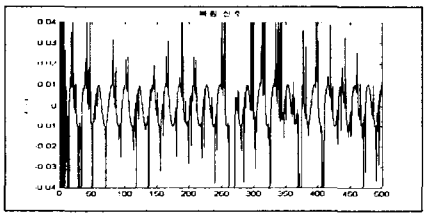


그림 10. 필터링 전 복원 신호 그림
Fig. 10 the recovered signal before filtering

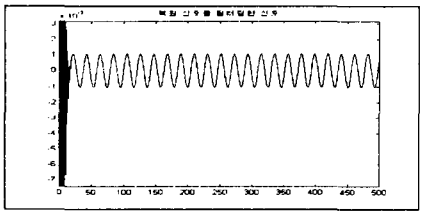


그림 11. 필터링 후 복원 신호
Fig. 11 The recovered signal after filtering

그림 11은 그림 10의 신호를 필터를 이용하여 잡음을 제거한 신호이다. 그림 8의 정보 신호에 근접된 신호가 복원되었음을 확인 할 수 있다.

V. 결 론

본 연구에서는 하이퍼카오스를 이용한 비밀 통신에 대하여 살펴보았다. 일반적인 카오스 회로에서 도청된 가능했던 신호가 하이퍼카오스 회로에서는 도청의 의미가 없음을 확인하고 이를 비밀통신에 적용할 가능성이 있음을 확인하였다. 앞으로 강건한 동기화와 음성 및 디지털 통신에 적용할 수 있는 범용적인 하이퍼카오스 회로와 동기화 기법, 비밀 통신 복조 기법 등이 연구과제로 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", 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] 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 communicarion" Int. J. Bifurcation and Chaos, vol. 7, no. 7, pp. 1579-1597, 1997.