복잡계를 이용한 비밀 통신

배영철*

The Secure Communication using Complexity

Youngchul Bae*

본 논문은 2003년도 정보통신부 정보통신연구진흥원에서 지원하고 있는
정보통신기초기술연구지원 사업의 연구결과입니다

요 약

본 논문에서는 복잡계를 이용한 비밀통신 방법을 제시한다. 복잡계 회로는 N-Double Scroll CNN 회로를 이용하였다. 동일한 여러 개의 셀을 가진 N-Double Scroll 회로를 이용하여 복잡계의 송·수신부를 구성하고 이 복잡계 송·수신부 사이에 임베딩 동기화 기법을 이용하여 동기화를 이루고, 송신부에서 정보 신호를 복잡계 신호에 합성하여 채널을 통하여 수신부에 송신 한 후 수신부에서 정보 신호와 복잡계 신호를 분리하는 기법을 제시하여 비밀 통신 가능성을 확인하였다.

ABSTRACT

In this paper, complexity secure communication was presented. The complexity circuit is used to State-Controlled Cellular Neural Network(SC-CNN). We make a complexity circuit using SC-CNN with the N-double scroll. A complexity circuit is created by applying identical n-double scrolls with coupled method, to each cell. complexity synchronization was achieved using drive response synchronization between the transmitter and receiver about each state in the SC-CNN. From the result of the recovery signal through the demodulation method in the receiver, We shown that recovery quality in the receiver is the similar to other secure communication methods.

키워드

Complexity, SC-CNN, Secure Communication, Synchronization

Ⅰ. 서 론

최근에 복잡계 현상에 대한 관심이 물리학, 화학, 생물학, 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다. 복잡계 시스템은 카오스, 하이퍼카오스 등이 포함되며 복잡계 시스템은 여러 개의 카오스 회로 또는 하이퍼카오스 회로를 연결하여 구성된다. 따라서 복잡계 시스템은 카오스 회로 또는 하이퍼카오스 회로를 이용하여 네트워크를 구성함으로서 일반적으로 얻을 수 있다. 대표적인 카오스 시스템으로 인정되고 있는 Chua 회로는 매우 단순한 자율, 3차 시스템으로 가역성을 가지며 1개의 비선형 소자인 3 구분 선형 저항(3 - segment piecewise - linear resistor)과 4개의 선형 소자인 (R, L, C1, C2)로 구성되는 발진회로다.

* 여수대학교 공과대학 전자통신전기공학부
접수일자 : 2004. 4. 2

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.

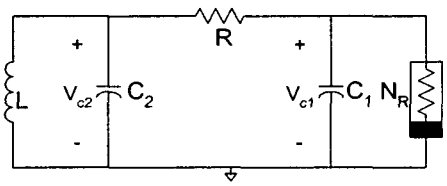


그림 1. Chua 회로
Fig. 1 Chua's circuit

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

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

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

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

$$g(v_R)=m_0v_R+\frac{1}{2}(m_1-m_0)[|v_R+B_P|-|v_R-B_P|] \qquad (2)$$

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

식(1)과 식(2)의 상태방정식 또는 그림 1을 이용한 하드웨어 구현에 의해 그림 2와 같은 어트렉터를 얻을 수 있다.

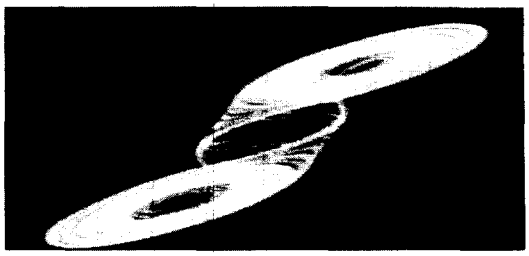


그림 2. Chua's 카오스 어트렉터
Fig. 2 Chua's chaos attractor

그림 1과 같은 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 복잡계 시스템의 신호를 이용하면 도청의 우려없이 정보 신호를 원하는 장소까지 실어 보낼 수 있으나 복잡계 신호를 생성하기 위한 장치와 비밀 통신을 실행하기 위한 송수신부 동기화 기법의 어려움으로 연구가 활발하지 못한 실정이다.

이에 본 연구에서는 비밀 통신 특성이 우수한 복잡계 회로를 이용한 동기화 및 비밀 통신 방법을 제안하고 그 타당성을 검토하였다.

II. 복잡계 회로

복잡계 회로를 얻기 위하여 n-double scroll 어트렉터를 이용한 SC-CNN 회로를 고려하였다.

2-1. N-double 스크롤 회로

n-double scroll을 얻기 위한 전기회로는 Arena[12]에 의해 구현되었으며 상태방정식은 식(3)과 같이 주어지고 비선형 저항의 관계식은 식(4)에 나타내었다.

$$\dot{x}=\alpha[y-h(x)]$$

$$\dot{y}=x-y+z \qquad (3)$$

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

식(4)는 2(2n-1)개의 breakpoint를 가지며 $\alpha = 9, \beta = 14.286$ 라 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

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

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 3에 Pspice로 구현한 2-double scroll 어트렉터와 그림 4에 3-double scroll 어트렉터를 각각 나타내었다.

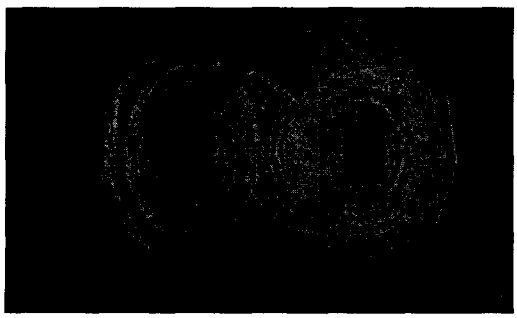


그림 3. 2-double scroll 위상공간과 비선형 저항
Fig. 3 phase plane of 2-double scroll and nonlinear resistor

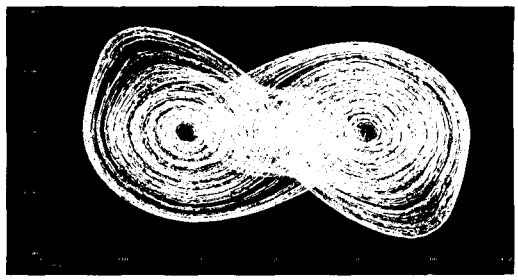


그림 4. 3-double scroll 위상공간과 비선형 저항
Fig. 4 phase plane of 3-double scroll and nonlinear resistor

2-2. 복잡계 회로

복잡계 회로를 구성하기 위해서는 동일한 n-Double scroll 셀로 구성된 1차원의 셀룰러 신경망(CNN) 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 복잡계 회로를 구성하였다. n-double scroll 셀들을 가진 1차원 CNN을 구성하기 위한 관계식을 식(5)에 x-확산 결합, 식(6) y-확산 결합식으로 나타내었다.

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

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

여기서 L은 셀의 수를 나타낸다.

식(5)-(6)에 의해 구성한 복잡계 어트렉터를 그림 5와 6에 나타내었다.

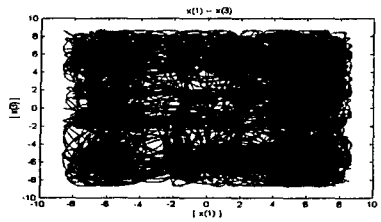


그림 5. 2-double scroll 복잡계 위상공간
Fig. 5 phase plane of 2-double scroll complexity

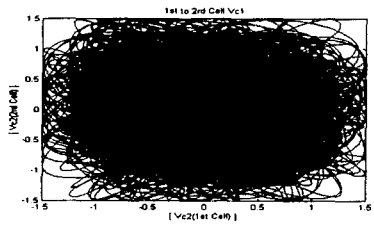


그림 6. 2-double scroll 복잡계 위상공간
Fig. 6 phase plane of 2-double scroll complexity

III. 복잡계 시스템의 동기화

복잡계 시스템의 동기화를 위하여 동일한 2개의 복잡계 회로를 송·수신부로 놓고 구동 동기에 의한 동기화를 이루었다. 그림 7에 복잡계 회로의 동기화 회로에 대한 블록 다이어그램을 나타내었으며 이에 대한 송수신부의 상태방정식은 식(7), (8)과 같다.

송신부의 상태방정식

$$x^{\cdot}(j) = \alpha[y^{(j)} - h(x^{(j)}]$$

$$y^{\cdot}(j) = x^{(j)} - y^{(j)} + z^{(j)} + D_y(x^{(j-1)} - 2x^{(j)} + x^{(j+1)})$$

$$z^{\cdot}(j) = -\beta y^{(j)}, \qquad j = 1,2,\ldots..L \qquad (7)$$

수신부의 상태방정식

$$x'^{\cdot}(j) = \alpha[y'^{(j)} - h(x'^{(j)})]$$

$$y'^{\cdot}(j) = x'^{(j)} - y'^{(j)} + z'^{(j)} + D_y(x'^{(j-1)} - 2x'^{(j)} + x'^{(j+1)})$$

$$z'^{\cdot}(j) = -\beta y'^{(j)}, \quad j = 1,2,\ldots..L \qquad (8)$$

이 때, $x'^{(1)} = x^{(L)}$이 되어 구동동기가 이루어진다.

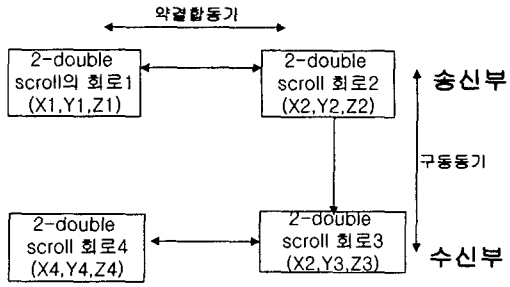


그림 7. 복잡계 시스템의 동기화 개략도
Fig. 7 The block diagram of complexity system synchronization

그림 8과 9에 그림 7에 의한 복잡계 시스템의 동기화 결과와 송수신부의 시계열데이터 차를 각각 나타내었다.

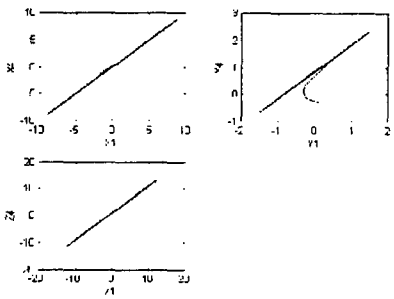


그림 8. 복잡계 시스템의 동기화 결과
Fig. 8 Synchronization result of complexity

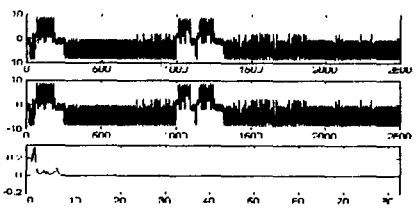


그림 9. 송수신부의 시계열데이터 차
Fig. 9 The difference between of transmitter and receiver

그림 8과 9를 통하여 복잡계 시스템 동기화가 완전하게 이루어짐을 확인할 수 있다.

IV. 복잡계 시스템의 비밀 통신

복잡계 시스템의 비밀 통신을 위하여 두 개의 동일한 복잡계 시스템에서 동기화를 이룬 후 송신부의 복잡계 시스템에 송신 하고자 하는 정보 신호를 합성 한 후 수신 부에서 이를 복조 하는 기법을 제안하였다.

그림 10에 복잡계를 이용한 비밀통신 회로 블록 다이어그램을 나타내었다.

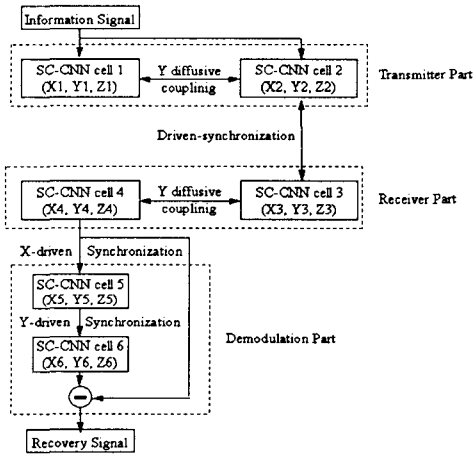
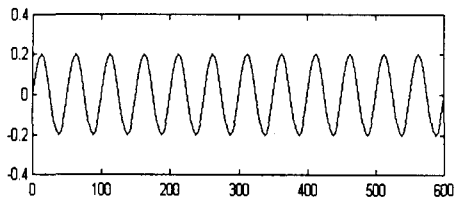
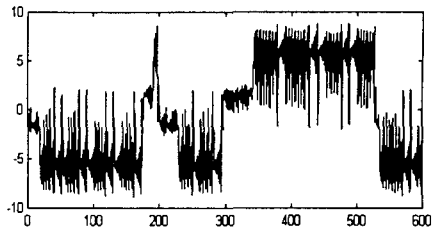


그림 10. 복잡계 시스템의 비밀통신 개략도
Fig. 10 The block diagram of complexity secure communication

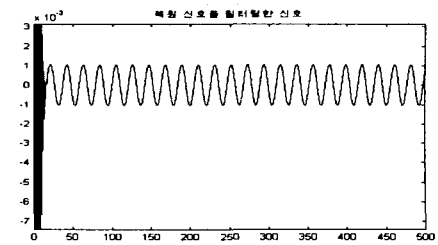
그림 10에 따른 복잡계 시스템의 송신부의 정보 신호와 정보 신호에 합성하기 위한 복잡계 신호 및 수신부에서 복조된 신호를 그림 11에 나타내었다.



(a)



(b)



(c)

그림 11. 비밀 통신 결과: 정보신호(a), 캐리어 신호(b), 복원신호(c)
Fig. 10. The result of secure communication: (a) Information signal, (b) carrier signal, (c) recovery signal

그림 11에서 송신부의 정보 신호와 수신부에 복원한 복원신호가 일치함을 확인할 수 있다.

IV. 결 론

본 연구에서는 복잡계 시스템에서의 비밀통신에 대하여 살펴보았다. 정보신호를 복잡계 신호와 합성한 후 이 신호를 채널을 통하여 전송하고 수신부에서 복조 회로를 이용하여 복원하였으며 만족할 만한 결과를 얻었다. 앞으로 강건한 동기화와 음성 및 디지털 통신에 적용할 수 있는 범용적인 복잡계 시스템의 동기화 기법, 비밀 통신 복조 기법 등이 연구 과제로 남는다.

참고 문헌

[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", 한국자동제어학술회의 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.

저자 소개

배영철(Young-Chul Bae)

1984년 2월 광운대학교 전기공학과 졸업
1986년 2월 광운대학교대학원 전기공학과졸업(공학석사)
1997년 2월 광운대학교대학원 전기공학과 졸업(공학박사)
1986-1991 한국전력공사
1991-1997 산업기술정보원 책임연구원
1997- 현재 여수대학교 전자통신전기공학부 부교수
※ 관심분야 : 퍼지 및 신경망, 카오스 동기화 및 암호화, 카오스 로봇 설계 및 제어, Small World