2001년도 대한전기학회 하계학술대회 논문집 2001.7.18-20

하이퍼 카오스 회로에서의 카오스 비밀통신

배영철
여수대학교

Secure Communication in Hyper-Chaos Circuit

Young-Chul Bae
Nat'l Yosu University

Abstract - In this paper, a transmitter and a receiver using two identical Hyper-Chaos that n-double scroll circuits are proposed and a hyper-chaos synchronizations and secure commnunication are investigated.
we are proposed unidirectional coupling of identical n-double scroll cell for hyper-chaos synchronization. We've shown that simulation result is synchronization and secure communication.

1. 서 론

최근에 카오스 현상에 대한 관심이 물리학, 화학, 생물학, 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다.. Chua는 간단한 전자 회로로 카오스 현상이 존재함을 증명하였다. Chua 회로는 매우 단순한 자율, 3차계 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.

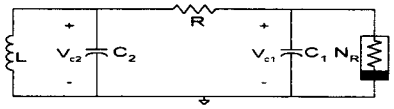


그림 1. Chua 회로
Fig. 1 Chua's circuit

Matsumoto에 의해 제안된 Chua 회로[1]를 그림 1에 나타냈으며 상태방정식은 다음과 같이 표시할 수 있다.

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

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

$$L\frac{di_L}{dt} = -v_{C_2} \qquad (1)$$

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

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

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

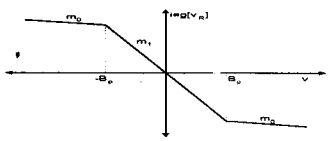


그림 2. 비선형 저항의 전압 전류 특성
Fig. 2 v-i characteristic of nonliner resistor

그림2의 비선형 저항을 그림3과 4와 같이 구성하면 n-double scroll cell을 가진 카오스 신호보다 더 복잡한 신호가 나오게 되는데 이를 하이퍼 카오스 신호라고 한다.

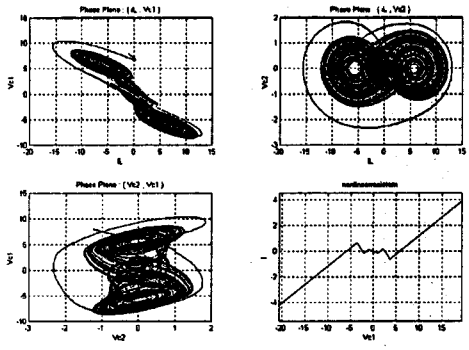


그림 3. 2-double scroll 위상공간과 비선형 저항
Fig. 3 phase plane of 2-double scroll and nonliner resistor

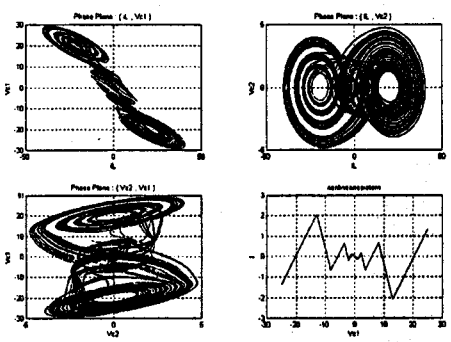


그림 4. 3-double scroll 위상공간과 비선형 저항
Fig. 4 phase plane of 3-double scroll and nonliner resistor

n-double scroll 에 관련된 상태방정식을 식(3)에 나타내고 그림 3의 비선형저항의 관계식을 식(4)에 나타내었다.

$$\dot{x} = \alpha[y - h(x)]$$
$$\dot{y} = x - y + z \qquad (3)$$
$$\dot{z} = -\beta y$$

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

그림 3과 4에서 보는 바와 같이 2(2n-1)개의 breakpoint를 가지며 $\alpha=9, \beta=14.286$ 라 할 때, 여러 가지 n-double scroll이 발생하게 된다.

본 연구에서는 동일한 2개의 n-double scroll 회로를 이용한 카오스 동기화 기법에 기법에 기반을 둔 카오스 비밀통신에 관한 연구를 하였다.

2. 하이퍼카오스 동기화

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

송신부의 상태방정식

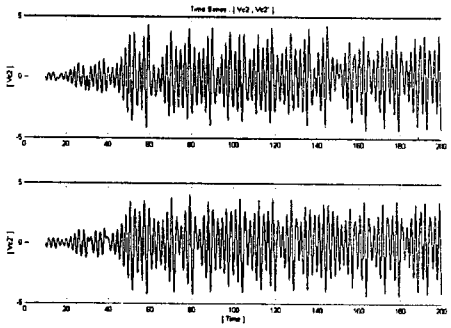
$$\dot{x} = \alpha[y - h(x)]$$
$$\dot{y} = x - y + z + K_{j-1}(y - y') \qquad (5)$$
$$\dot{z} = -\beta y$$

수신부의 상태방정식

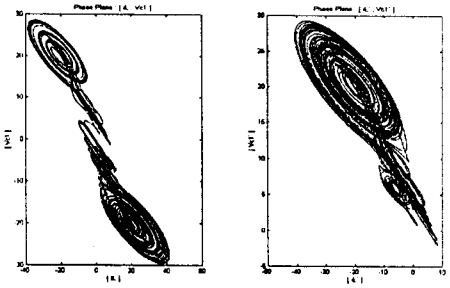
$$\dot{x}' = \alpha[y' - h(x')]$$
$$\dot{y}' = x' - y' + z' + K_{j-1}(y' - y) \qquad (6)$$
$$\dot{z}' = -\beta y'$$

송신부와 수신부의 시스템이 안정하도록 차시스템(difference system)을 이용하여 결합계수를 결정하면 $K<-1.3$의 범위에서 동기화가 이루어진다.

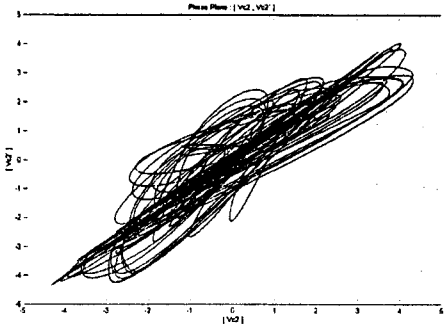
그림5에 동일한 하이퍼카오스회로에 대한 동기화 결과를 나타내었다.



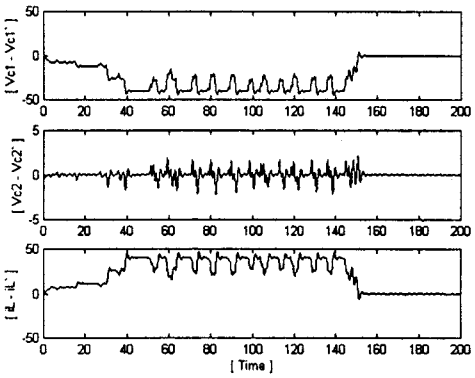
(a)송신부의 시계열 데이터(y-y')
(a) Time Series of transmitter and receiver



(b) 송수신부의 위상공간(x-z,x'-z')
(b) Phase Plane of transmitter and receiver



(c) 동기화척도(y-y')
(c) Synchronization degree



(d) 송수신부 차시스템
(d) difference system

그림 5 하이퍼 카오스 동기화 결과
Fig. 5 Synchronization result of Hyper-Chaos

그림 5에서 확인하듯이 일정시간이 지난후 동기화가 이루어졌음을 알 수 있다.

3. 하이퍼 카오스 비밀통신

동일한 n-double scroll회로를 이용하여 송수신회로를 구성하고 송신부의 복잡한 하이퍼카오스 회로에 정보신호를 실어 수신부로 전송한 후 수신부에서 복조하는 하이퍼카오스 비밀통신을 행하였다.
그림 6 과 7에 하이퍼카오스 비밀통신의 결과를 나타내었다.

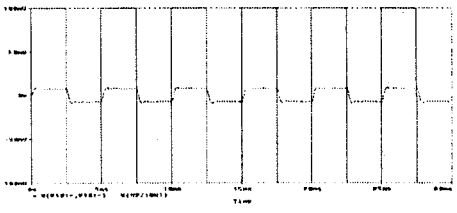


그림 6. 송수신부 파라미터 일치시의 결과
Fig. 6 The result of parameter match of transmitter and receiver

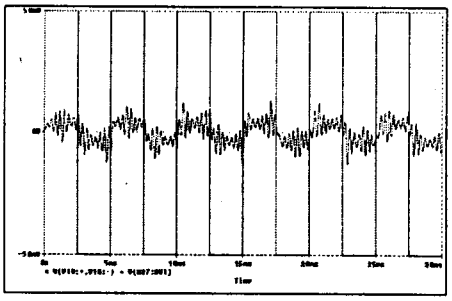


그림 7. 송수신부 파라미터 불일치시의 결과
Fig. 7 The result of parameter mismatch of transmitter and receiver

그림 6과 7에서 보는 바와 같이 하이퍼 카오스 회로에서 비밀통신이 이루어짐을 확인할 수 있었다.
하이퍼 카오스 회로는 카오스 회로에 비해 카오스 비밀통신에 적용할 경우 그 보안성이 매우 우수한 것으로 알려져있다.

4. 결 론

본 연구에서는 두 개의 동일한 하이퍼카오스 회로를 이용하여 결합동기에 의한 동기화 및 이를 이용한 암호통신를 행하였다. 앞으로 강건한 동기화 이론과 이를 암호통신에 적용하기 위한 방법과 파라미터 불일치 할 경우 강인한 비밀통신에 대한 연구는 계속 진행되어야 할 것으로 생각한다.

[참 고 문 헌]

[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.