

임베딩 구동 동기화를 이용한 비밀통신

Secure Communication using Embedding Drive Synchronization

배영철, 김주완, 김이곤
 여수대학교 전기공학과

Youngchul Bae, Juwan Kim, Yigon Kim
 Yosu National University
 E-mail : ycbae@yosu.ac.kr

요 약

본 논문에서는 임베딩 구동 동기화를 이용한 비밀통신회로를 구성하고 검증하였다. 임베딩 구동 동기는 Chua 회로의 미분방정식의 세 가지 상태 변수 중 전류성분과 같이 동기화와 신호 합성에 어려운 상태변수를 전압 성분으로 분리하여 각각의 CNN 성분으로 다룰 수 있는 SC-CNN을 이용하여 구성하였다.

Embedding Drive Synchronization(임베딩 구동동기)은 구동동기에서 한 미분상태변수를 완전히 대체하지 않고 동일한 시스템상의 일부 성분으로 구성하여 동기화를 이루고 비밀통신에 적용한 후 그 결과를 검증하였다.

1. 서론

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 3 구분 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(universality) 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.

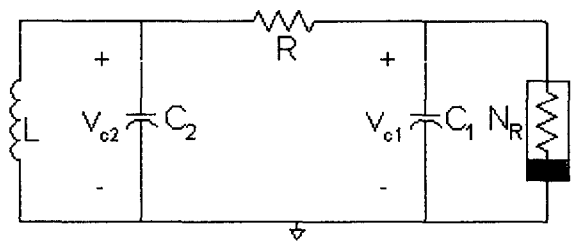


그림 1. Chua 회로
 Fig. 1. Chua's circuit

$$C_1 \frac{dv_{c1}}{dt} = G(v_{c2} - v_{c1}) - g(v_{c1})$$

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

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

여기서 $G = 1/R$, $g(v_{C_1})$ 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.

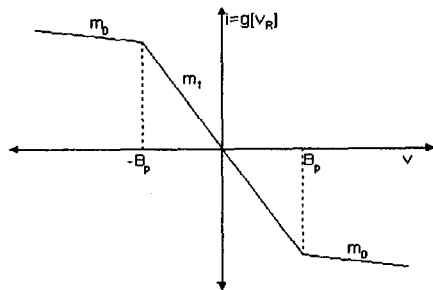


그림 2. 비선형 저항의 전압 전류 특성
Fig. 2 v-i characteristic of nonlinear resistor

Chua 회로는, 잡음과 유사한 카오스 특성을 이용하여 카오스 신호에 정보 신호를 혼합하여 송신부에서 전송한 후 수신부에서 정보 신호와 카오스 신호를 분리하는 카오스 비밀통신에 주로 이용하고 있다[5,6].

카오스 신호를 이용한 카오스 비밀통신을 위해서는 동기화가 선행되어야 하며 이를 위한 동기화 기법으로 결합동기, 구동동기 방법[9,10] 등이 제시되었다.

결합동기는 시스템이 안정하지 않으면 결합 저항을 찾지 못하는 단점과 구동동기는 송신부와 수신부의 파라미터 값에 따라 구동하지 못하는 결점을 가지고 있다.

이에 본 연구에서는 Chua 회로를 기반으로 구성된 SC-CNN(State-Controlled CNN) 회로를 이용하여 카오스 회로를 구성하고 새로운 임베딩 구동 동기를 이용한 비밀통신기법을 제안하였다.

2. SC-CNN 회로

2.1 SC-CNN 모델 [12,13]

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

$$\dot{x}_j = -x_j + a_j y_j + G_o + G_s + i_j \quad (3)$$

여기서 j 는 셀 수, x_j 는 상태 변수, y_j 는 셀 출력을 나타낸다. i_j 는 임계값(threshold value)이다. 식(3)에서 G_o 는 출력의 선형 조합이며, G_s 는 연결 셀의 상태 변수이다. 비선형성 출력은 식(4)과 같은 새로운 출력 PWL 방정식을 이용한다.

$$y_j = \frac{1}{2} \sum_{k=1}^{2n-1} n_k (|x + b_k| - |x - b_k|) \quad (4)$$

여기서 b_k 는 차단점(break point)이며 n_k 는 선형 구간의 기울기와 관련된 계수이다.

SC-CNN 셀은 상태 방정식(3)과 출력 방정식(4)의 조합으로 식 (5)과 같은 n-Double scroll을 만들 수 있다.

$$\dot{x}_1 = -x_1 + a_{11} y_1 + a_{12} y_2 + a_{13} y_3 + \sum_{k=1}^3 s_{1k} x_k + i_1$$

$$\dot{x}_2 = -x_2 + a_{21} y_1 + a_{22} y_2 + a_{23} y_3 + \sum_{k=1}^3 s_{2k} x_k + i_2 \quad (5)$$

$$\dot{x}_3 = -x_3 + a_{31} y_1 + a_{32} y_2 + a_{33} y_3 + \sum_{k=1}^3 s_{3k} x_k + i_3$$

여기서 x_1, x_2, x_3 는 상태 변수이며, y_1, y_2, y_3 는 이에 대응한 출력 변수이다.

2.2 Embedding Drive Synchronization

Chua 회로를 SC-CNN의 Dimensionless 형태로 바꾸어 표현하면 다음과 같다.

$$\begin{aligned} \dot{x}_1 &= -x_1 + x_1 + \alpha(x_2 - g) \\ \dot{x}_2 &= -x_2 + x_1 + x_3 \end{aligned} \quad (6)$$

$$\dot{x}_3 = -x_3 - \beta x_2 + x_3$$

$$g_1 = m_3 x_i + \frac{1}{2} \sum_{k=0}^2 (m_k + m_{k+1}) (|x_1 + c_k| - |x_1 - c_k|)$$

$$\begin{aligned} \dot{x}_4 &= -x_4 + x_4 + \alpha(x_2 - g_2) \\ \dot{x}_5 &= -x_5 + x_4 + x_6 \end{aligned} \quad (7)$$

$$\dot{x}_6 = -x_6 - \beta x_5 + x_6$$

$$g_1 = m_3 x_i + \frac{1}{2} \sum_{k=0}^2 (m_k + m_{k+1}) (|x_1 + c_k| - |x_1 - c_k|)$$

x_4 의 전개항에 보면 x_2 가 포함되어 있는 것을 알 수 있다. 이렇게 미분방정식에서 오른쪽 항의 일부에만 연결하여 동기화를 시도하는 방법을 제안하였으며 임베딩 구동 동기화라 명하였다.

식(6)과 식(7)에서 x_1, x_2, x_3 가 송신부가 되고 x_4, x_5, x_6 가 수신부가 된다. 식(6)과 식(7)의 임

베딩 구동 동기화의 결과는 그림 3과 같다.

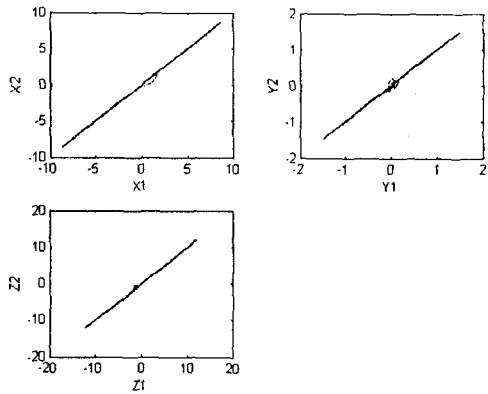


그림 3. 송신부와 수신부 SC-CNN의 위상일치도
Fig. 3 Phase portrait of synchronization of signals of transmitted and received part

그림 3에서 CNN 간에 임베딩에 의한 동기화가 이루어진 것을 알 수 있다

2.3 임베딩 동기화를 통한 비밀통신

식 (6)과 식 (7)의 동기화의 결과를 통하여 다음과 같이 송신부의 식(6)의 상태변수 x_2 에 그림 4와 같은 정현파 $\sin(2\pi \times 10t)$ 를 정보신호로 임베딩하여 입력하였다.

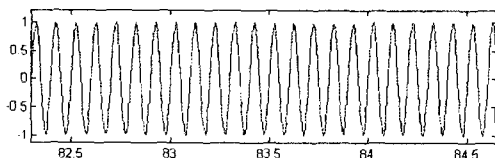
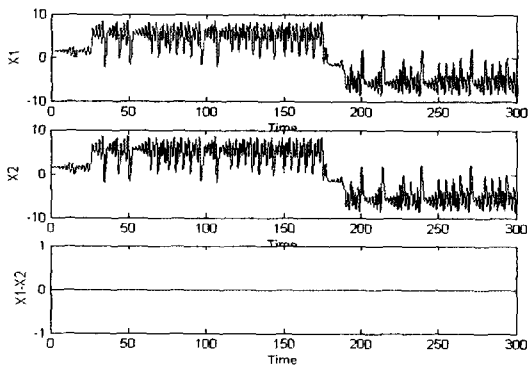
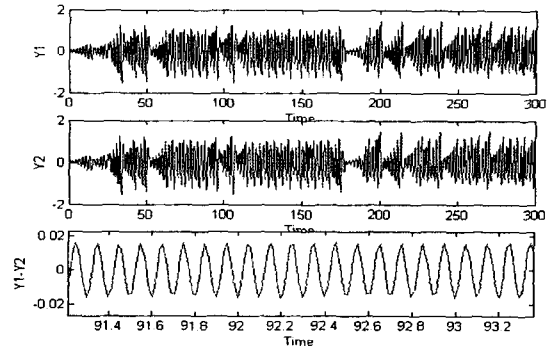


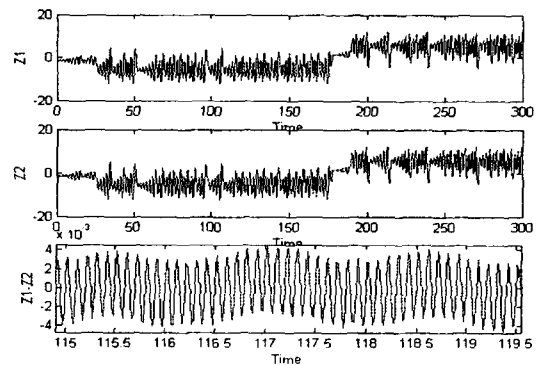
그림 4. 입력 정보 신호
Fig. 4 input information signal



(a)



(b)

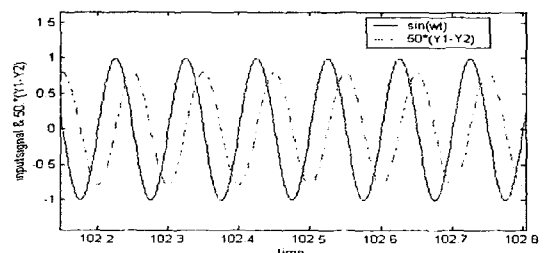


(c)

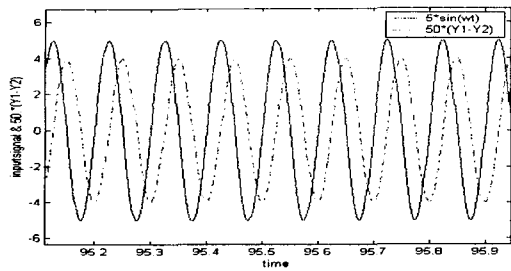
그림 4. 정보신호가 포함되었을 때의 각 상태 변수의 신호비교 (a) x_1 과 x_4 (b) x_2 과 x_5 (c) x_3 과 x_6

Fig. 4 Comparison of the signal of each state variables of both sides when information signal included.(a) x_1 and x_4 (b) x_2 and x_5 (c) x_3 and x_6

그림 5에서 $X1, X2, X3$ 은 각각 송신부의 상태변수 x_1, x_2, x_3 를 나타내며, $Y2, Z2$ 는 각각 수신부의 상태변수 x_4, x_5, x_6 를 나타낸다. 그림 5를 살펴보면 x_1 과 x_4 는 거의 완전히 동기화 하는 반면 x_2 와 x_5 , 그리고 x_3 과 x_6 에서는 그 차에서 정보신호를 찾을 수 있음을 알 수 있다.



(a)



(b)

그림 6. 정보신호와 복원신호의 비교. 입력신호가

(a) $\sin(2\pi 10t)$ (b) $5\sin(2\pi 10t)$ 일 때

Fig. 6 comparison of transmitted and received signals when (a) $\sin(2\pi 10t)$, (b) $5\sin(2\pi 10t)$ was applied as information signal

그림 6에 정보신호와 복원된 정보신호를 비교하여 나타내었다. (a)는 $\sin(2\pi 10t)$ 를 입력신호로 사용하였을 때이며, (b)는 $5\sin(2\pi 10t)$ 를 사용하였을 때이다. 그림 6의 결과를 보면 (a), (b) 모두 복원된 정보신호는 입력신호의 약 1/60인 것을 알 수 있다.

일반적으로 Chua 회로에서 정보를 담기 위해서는 정보신호의 크기를 아주 작게 해야 한다는 것과는 달리 아주 큰 진폭을 가진 신호를 입력신호로 사용할 수 있다는 결과를 얻을 수 있었다.

3. 결론

SC-CNN은 Chua 회로에서 전류와 전압 성분이 혼합된 미분방정식에서의 세 가지 상태 변수 중 전류성분과 같이 동기화와 신호 합성에 어려운 상태변수를 전압성분으로 대체하여 다룰 수 있는 방법을 제공하였다. 새로운 임베딩 구동 동기기법을 이용한 비밀통신의 결과를 검증하여 만족할 만한 결과를 얻었다.

4. 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, " 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] 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, Chua's 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. Fundamentals. 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.