

SC-CNN을 이용한 카오스 임베딩 구동 동기화

Embedding Drive Synchronization using SC-CNN

배영철, 김주완, 김이곤
 여수대학교 전기공학 및 반도체공학과
 Youngchul Bae, Juwan Kim, Yigon Kim
 Yosu National University
 E-mail : ycbae@yosu.ac.kr

요 약

본 논문에서는 SC-CNN의 특성을 이용한 임베딩 구동 카오스 동기화 방법을 소개한다. SC-CNN은 Chua 회로의 미분방정식에서의 세가지 상태변수중 전류성분과 같이 동기화와 신호 합성에 어려운 상태변수를 전압성분으로 분리하여 다룰 수 있는 방법을 제공하고 있다. 여기서 지금까지 이용되 오던 결합 동기나 구동동기화의 방법에 새로운 임베딩 구동 동기방식을 제안한다.

제안하는 Embedding Drive Synchronization(임베딩 구동동기)은 구동동기에서 미분상태변수를 완전히 대체하는 것이 아닌 한 성분만을 대체하여 구성되며 그 타당성을 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.

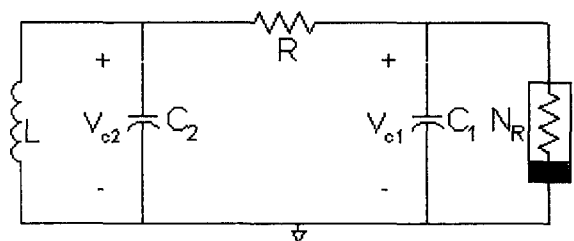


그림 1. Chua 회로

Fig. 1 Chua's circuit

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

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

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

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.

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

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

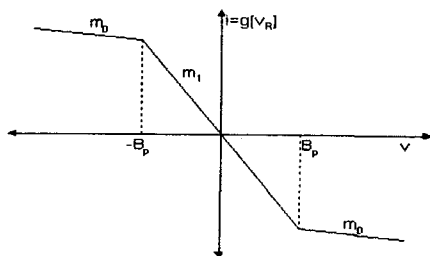


그림 2. 비선형 저항의 전압 전류 특성

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 결합저항을 찾지 못하는 단점과 구동동기는 송신부와 수신부의 파라미터값에 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 제안하였다.

2. SC-CNN 회로

2.1 N-double scroll 회로

SC-CNN 회로를 얻기 위하여 Chua 회로의 변형인 n-double scroll 어트랙터를 고려하였다. n-double scroll을 얻기 위한 전기회로는 Arena[12]에 의해 구현되었으며 상태방정식은 식 (3)과 같이 주어지고 비선형 저항의 관계식은 식

(4)에 나타내었다.

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

$$\dot{y} = x - y + z$$

$$\dot{z} = -\beta y$$

(3)

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

식(4)는 $2(2n-1)$ 개의 breakpoint를 가지며 $\alpha=9, \beta=14.288$ 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

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

그림 3에 2-double scroll 어트랙터와 비선형 저항향을 그림 4에 3-double scroll 어트랙터와 비선형 저항을 각각 나타내었다.

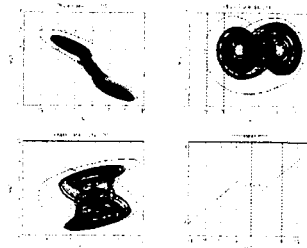


그림 3. 2-double scroll 위상공간과 비선형 저항

Fig. 3 phase plane of 2-double scroll and nonlinear resistor

2.2 SC-CNN 모델 [12,13]

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

$$\dot{x}_j = -x_j + a_j y_j + G_o + G_s + i_j \quad (5)$$

여기서 j 는 셀 수, x_j 는 상태 변수, y_j 는 셀 출력수를 나타내며 다음 식과 같이 주어진다.

$$y_j = 0.5(|x_j - j + 1| - |x_j - 1|) \quad (6)$$

여기서 a_j 는 상수 파라미터, i_j 는 임계값 (threshold value)이다

식(5)에서 G_o 는 출력의 선형 조합이며, G_s 는 연결 셀의 상태 변수이다. 식 (6)의 출력 비선형

성출력은 식(7)과 같은 새로운 출력 PWL 방정식을 이용한다..

$$y_j = \frac{1}{2} \sum_{k=1}^{2n-1} n_k (|x + b_k| - |x - b_k|) \quad (7)$$

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

SC-CNN 셀은 상태 방정식(5)과 출력 방정식(7)의 조합으로 식(8)과 같은 n-Double scroll을 만들 수 있다.

$$\begin{aligned} \dot{x}_1 &= -x_1 + a_{11}y_1 + a_{12}y_2 + a_{13}y_3 + \sum_{k=1}^3 s_{1k}x_k + i_1 \\ \dot{x}_2 &= -x_2 + a_{21}y_1 + a_{22}y_2 + a_{23}y_3 + \sum_{k=1}^3 s_{2k}x_k + i_2 \\ \dot{x}_3 &= -x_3 + a_{31}y_1 + a_{32}y_2 + a_{33}y_3 + \sum_{k=1}^3 s_{3k}x_k + i_3 \end{aligned}$$

여기서 x_1, x_2, x_3 는 상태 변수이며, y_1, y_2, y_3 는 이에 대응한 출력 변수이다. 식(8)에 기초한 PSpice를 이용한 CNN회로를 그림 4에 나타내었다.

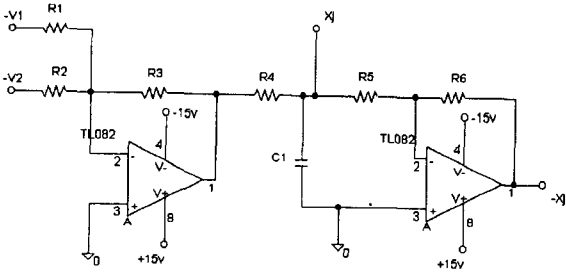


그림 4. CNN 회로도
Fig. 4 CNN circuit

그림 4의 상태방정식을 세우면 식(9)와 같다.

$$C_j \dot{x}_j = -\frac{x_j}{R_4} + \frac{R_3}{R_1 R_4} V_1 + \frac{R_3}{R_2 R_4} V_2 \quad (9)$$

2.3 Embedding Drive Synchronization

동기화의 방식에는 결합동기법과 구동동기법이 널리 쓰이고 있다. 여기에서는 SC-CNN의 장점인 회로구현에서의 상태변수의 분리구현을 이용하여 임베딩 구동 동기화를 소개하였다.

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

$$\begin{aligned} \dot{x}_1 &= -x_1 + x_1 + \alpha(x_2 - g) \\ \dot{x}_2 &= -x_2 + x_1 + x_3 \end{aligned} \quad (10)$$

$$\begin{aligned} \dot{x}_3 &= -x_3 - \beta x_2 + x_3 \\ g_1 &= m_3 x_i + \frac{1}{2} \sum_{k=0}^2 (m_k + m_{k+1})(|x_1 + c_k| - |x_1 - c_k|) \\ \dot{x}_4 &= -x_1 + x_1 + \alpha(x_2 - g_2) \\ \dot{x}_5 &= -x_5 + x_4 + x_6 \\ \dot{x}_6 &= -x_6 - \beta x_5 + x_6 \end{aligned} \quad (11)$$

$g_1 = m_3 x_i + \frac{1}{2} \sum_{k=0}^2 (m_k + m_{k+1})(|x_1 + c_k| - |x_1 - c_k|)$
두 번째 CNN에서 x_4 의 전개항에 보면 x_2 가 포함되어 있는 것을 알 수 있다. 이렇게 미분방정식에서 오른쪽 항의 일부에만 임베딩하여 동기화를 시도하는 방법이 결합동기와 구동동기화를 하는 방법에 더 추가할 수 있다.

식(10)과 식(11)에서 x_1, x_2, x_3 가 송신부가 되고 x_4, x_5, x_6 가 수신부가 된다.

이렇게 수식을 구성하고 그 결과를 보면 다음과 같이 동기화가 완전하게 이루어짐을 알 수 있다.

x_1, x_2, x_3 의 초기값은 각각 0.21, .171, -.31 그리고 x_4, x_5, x_6 의 초기값은 -0.22131, .111, -.31231으로 하였다.

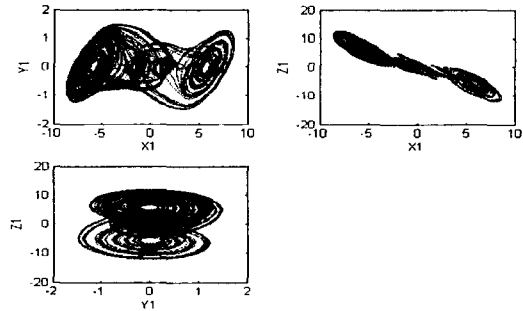


그림 5. 송신부 SC-CNN의 2-double scroll 어트랙터

Fig. 5 Attractor of 2-double scroll of SC-CNN

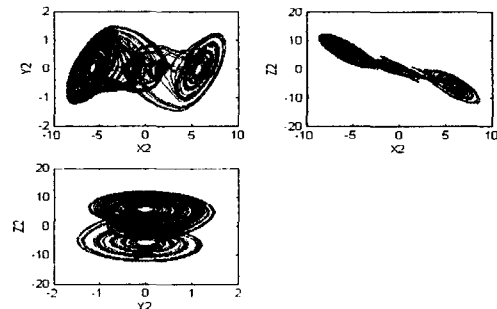


그림 6. 수신부 SC-CNN의 2-double scroll 어트랙터

Fig. 6 Attractor of 2-double scroll of SC-CNN

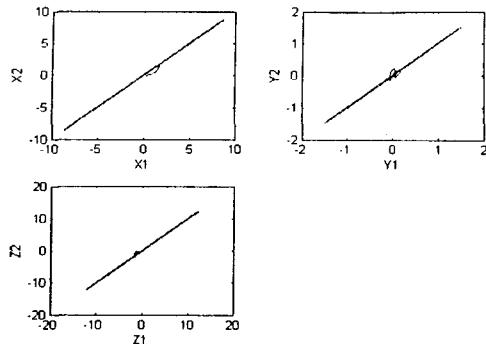


그림 7. 임베딩 구동동기를 이용한 SC-CNN의 송신부와 수신부의 동기화 결과

Fig. 7 Synchronization result of Transmission and Receiving part through Embedding Drive Synchronization

그림 7을 통해 CNN 간에 동기화가 이루어짐을 확인할 수 있다

3. 결론

SC-CNN은 Chua회로에서 전류와 전압성분이 혼합된 미분방정식에서의 세 가지 상태 변수 중 전류성분과 같이 동기 기법과 신호 합성에 어려운 상태변수를 전압성분으로 대체하여 다룰 수 있는 방법을 제공하고 있다. 이 방법을 이용하여 지금까지 이용된 결합 동기나 구동동기화의 방법에 임베딩 구동 동기를 제안하고 그 결과를 검증하였다.

Embedding Drive Synchronization(임베딩 구동 동기)은 구동동기의 동기화 기법과 유사한 결과를 보였다. 앞으로 이 동기화 기법을 비밀통신에 적용될 수 있을지에 대한 연구가 진행되어야 할 것으로 생각한다.

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 학술회의 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.