# 하이퍼카오스 동기화를 이용한 비밀통신

배영철

여수대학교 전자통신 · 전기 · 반도체공학부

## 목 차



## Ⅰ. 서 론

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 doubl- ing), 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.

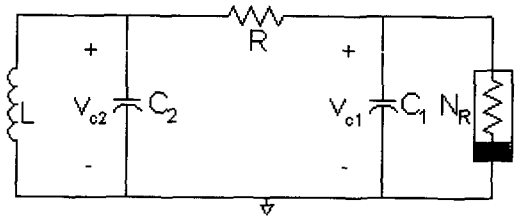



그림 1. Chua 회로

$$\begin{aligned} C_1\frac{dv_{C_1}}{dt} &= G\,(v_{C_2}-v_{C_1})-g(v_{C_1}) \\ C_2\frac{dv_{C_2}}{dt} &= G\,(v_{C_1}-v_{C_2})+i_L \\ L\frac{di_L}{dt} &= -v_{C_2} \end{aligned} \tag{1}$$

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.

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

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

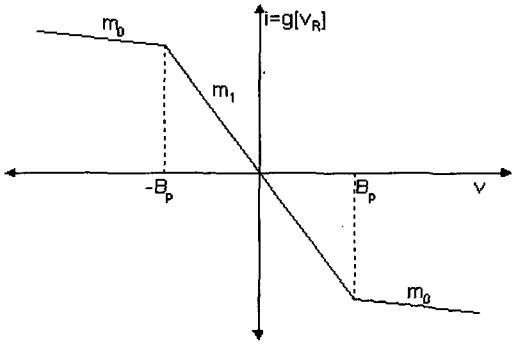



그림 2. 비선형 저항의 전압 전류 특성

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.

카오스 신호를 이용한 카오스 비밀통신을 위해서는 동기화가 선행되어야 하며 이를 위한 동기화 기법으로 결합동기, 구동동기 방법[9,10] 등이 제시되어 있다. 결합동기는 시스템이 안정하지 않으면 결합저항을 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 카오스회로를 구성하고 새로운 임베딩 구동 동기를 제안하였으며, 이 방식을 이용한 비밀통신기법을 제안하였다.

## II. SC-CNN 회로 및 하이퍼카오스 회로

### 2.1 N-double scroll 회로

하이퍼카오스 회로를 얻기 위하여 Chua 회로의 변형인 n-double scroll 어트렉터를 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.

$$\begin{aligned} \dot{x} &= \alpha[y - h(x)] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{3}$$

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

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

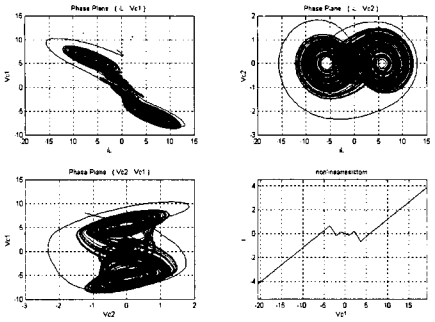


그림 3. 2-double scroll 위상공간과 비선형 저항

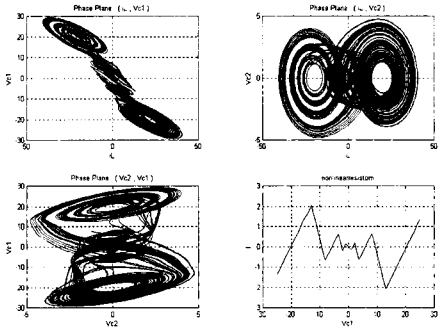


그림 4. 3-double scroll 위상공간과 비선형 저항

### 2.2 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(5)에 x-확산 결합, 식(6) y-확산 결합식으로 나타내었다.

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

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

여기서 L은 셀의 수를 나타낸다.

### 2.3 SC-CNN 모델[12,13]

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

$$\dot{x}_j = -x_j + a_j y_j + G_o + G_s + i_j \tag{7}$$

여기서 j는 셀 수, $x_j$는 상태 변수, $y_j$는 상태변수의 비선형 출력을 나타낸다. $i_j$는 임계값(threshold value)이다. 식(7)에서 $G_{oj}$는 상태변수의 선형 조합이며, $G_s$는 연결 셀의 상태 변수의 선형조합이다. 비선형 출력은 식(8)과 같은 새로운 출력 PWL 방정식을 이용한다.

$$y_j = \frac{1}{2}\sum_{k=1}^{2n-1} n_k(|x + b_k| - |x - b_k|) \tag{8}$$

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

SC-CNN 셀은 상태 방정식(7)과 비선형 출력 방정식(8)의 조합으로 식 (9)과 같은 n-Double scroll을 만들 수 있다.

$$\begin{aligned} \dot{x}_1 &= -x_1 + a_{11}y_1 + a_{12}y_2 + a_{13}y_3 + \sum_{k=1}^{3} s_{1k}x_k + i_1 \\ \dot{x}_2 &= -x_2 + a_{21}y_1 + a_{22}y_2 + a_{23}y_3 + \sum_{k=1}^{3} s_{2k}x_k + i_2 \\ \dot{x}_3 &= -x_3 + a_{31}y_1 + a_{32}y_2 + a_{33}y_3 + \sum_{k=1}^{3} s_{3k}x_k + i_3 \end{aligned} \tag{9}$$

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

2-double scroll 회로를 만들기 위해서는 $a_{12}=a_{13}=a_{21}=a_{22}=a_{23}=a_{32}=a_{33}=a_{31}=0$, $s_{13}=s_{31}=s_{22}=0$, $i_1=i_2=i_3=0$으로 하면 식(9)과 같은 형태로 바뀌게 된다.

식(9)에 기초한 PSpice를 이용한 CNN회로를 그림 5에 나타내었다.

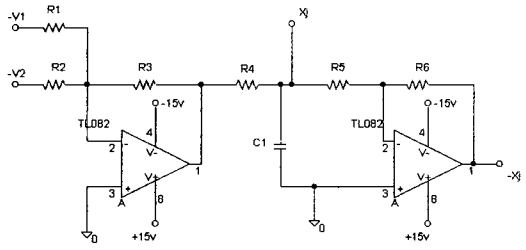



그림 5. CNN 회로도

그림 5의 상태방정식을 세우면 식 (10)과 같다.

$$C_j\dot{x}_j=-\frac{x_j}{R_4}+\frac{R_3}{R_1R_4}V_1+\frac{R_3}{R_2R_4}V_2 \qquad (10)$$

## III. 하이퍼카오스 회로 동기화

### 3.1 SC-CNN하이퍼카오스 동기화

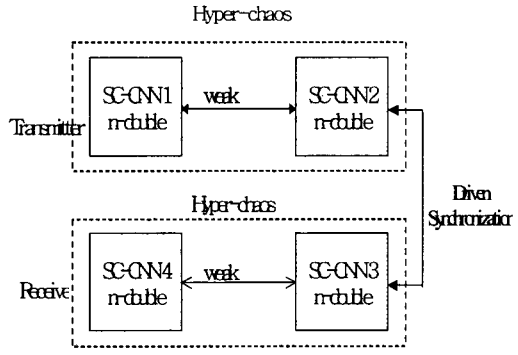



그림 6. 하이퍼카오스 회로의 동기화 개략도

SC-CNN 하이퍼카오스 회로의 동기화를 위하여 동일한 SC-CNN 회로를 송·수신부로 놓고 구동 동기에 의한 동기화를 이루었다.

그림 6에 SC-CNN을 이용한 하이퍼카오스 동기화 회로의 블록 다이어그램을 나타내었다.

그림 7에 그림 6에 의한 하이퍼카오스 회로의 동기화 결과를 나타내었다.

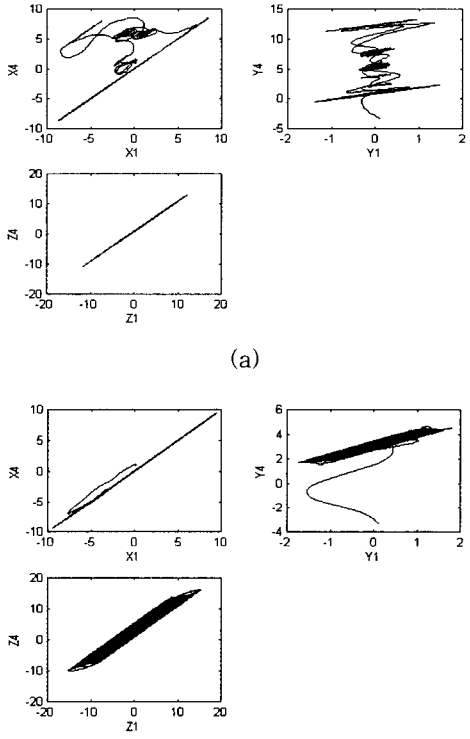



그림 7. (a) 동기화 결과 (b) 정보신호가 포함되었을 때의 동기화 결과

그림 7에서 하이퍼카오스 회로의 동기화가 상태 변수 $x_3$에서 완전하게 이루어 짐을 확인할 수 있다.

### 3.2 Embedding Drive Synchronization

N-double Scroll 회로를 SC-CNN의 Dimension -less 형태로 바꾸어 표현하면 다음과 같다.

송신부의 상태 방정식

$$\begin{aligned}\dot{x}_1 &= -x_1 + x_1 + \alpha(x_2 - g)\\ \dot{x}_2 &= -x_2 + x_1 + x_3\\ \dot{x}_3 &= -\gamma x_3 - \beta x_2 + x_3\\ g_1 &= m_3 x_i + \frac{1}{2}\sum_{k=0}^{2}(m_k + m_{k+1})\\ &\quad \cdot (|x_1 + c_k| - |x_1 - c_k|)\end{aligned} \tag{11}$$

수신부의 상태 방정식

$$\begin{aligned}\dot{x}_4 &= -x_1 + x_1 + \alpha(x_2 - g_2)\\ \dot{x}_5 &= -x_5 + x_4 + x_6\\ \dot{x}_6 &= -\gamma x_6 - \beta x_5 + x_6\\ g_1 &= m_3 x_i + \frac{1}{2}\sum_{k=0}^{2}(m_k + m_{k+1})\\ &\quad \cdot (|x_1 + c_k| - |x_1 - c_k|)\end{aligned} \tag{12}$$

$\dot{x}_4$의 전개 항을 보면 $x_2$가 포함되어 있는 것을 알 수 있다. 이와 같은 방법으로 미분방정식에서 오른쪽 항의 일부에만 전송신호를 임베딩 하여 동기화를 시도하는 방법을 제안하였으며 임베딩 구동 동기화(embedding synchronization)라 명하였다.

식(11)과 식(12)에서 $x_1, x_2, x_3$가 송신부가 되고 $x_4, x_5, x_6$가 수신부가 된다. 식(11)과 식(12)의 임베딩 구동 동기화의 결과는 그림 8, 그림 9, 그림 10과 같다. 그림 8는 송신부의 어트렉터를 그림 9은 수신부의 어트렉터를, 그림 10은 송신부와 수신부의 위상 일치도를 나타내었다.

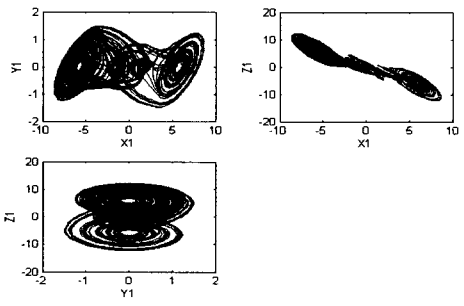


그림 8. 송신부 SC-CNN의 2-double scroll 어트랙터

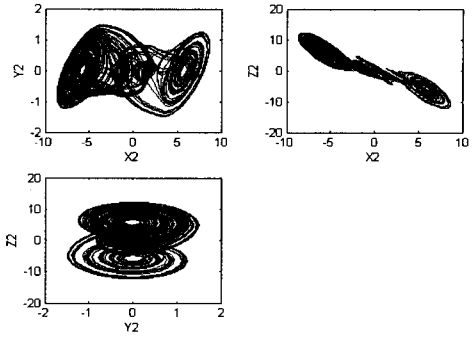


그림 9. 수신부 SC-CNN의 2-double scroll 어트랙터

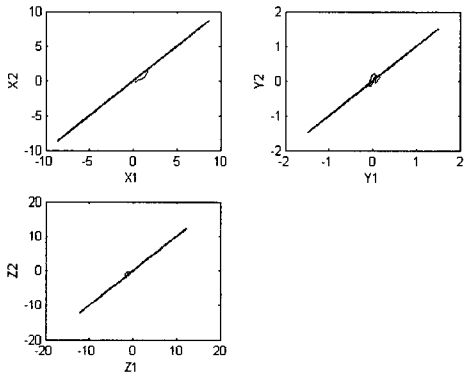


그림 10. 송신부와 수신부 SC-CNN의 위상일치도

그림 10의 송신부와 수신부의 위상 일치도에서 CNN 사이에 임베딩에 의한 동기화가 이루어 진 것을 확인할 수 있다.

## Ⅳ. 하이퍼카오스 회로 비밀 통신

### 4.1 SC-CNN 하이퍼카오스에서의 비밀 통신

SC-CNN 하이퍼카오스 회로의 동기화를 위하여 동일한 SC-CNN 회로를 송·수신부로 놓고 정보 신호를 각 상태에 실어서 송신부에서 전송 한 후 수신부에서 이를 복원하는 방법을 제안하였다.

정보 신호로는 정현파를 이용하였으며, 이 정보신호를 하이퍼카오스 신호인 SC-CNN의 각 상태 변수 $x_1, x_2, x_3$에 더하여 송신하고 수신기에서 복

조하였으며 각 상태 변수에 따른 복원 결과를 확인하였다.
그림 11에 SC-CNN을 이용한 하이퍼카오스 비밀 통신 회로 블록 다이어그램을 나타내었다.

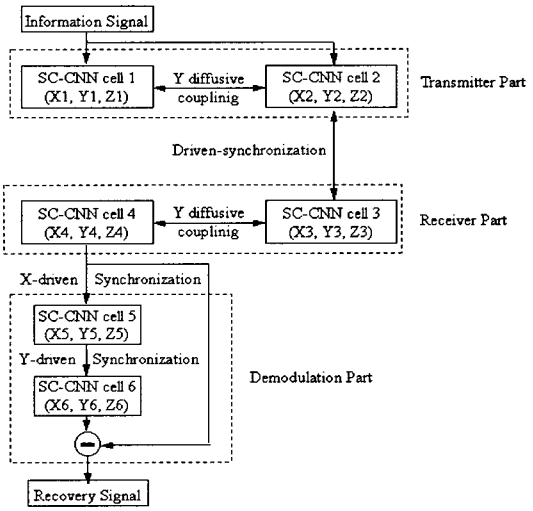



그림 11. 하이퍼카오스 회로의 동기화 개략도

그림 12에 정보 신호를 상태변수 $x_1$의 하이퍼카오스 신호를 합성하고 송신부와 수신부의 동기화에 따른 어트렉터를 나타내었다.

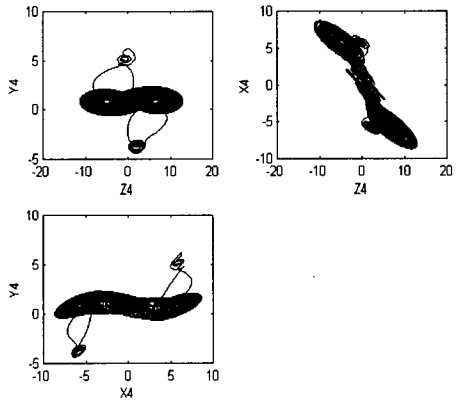


그림 12. 정보 신호를 상태변수 $x_1$에 합성하였을 때의 어트렉터

그림 13에 정보 신호를 상태변수 $x_3$의 하이퍼카오스 신호를 합성하고 송신부와 수신부의 동기화에 따른 어트렉터를 나타내었다.

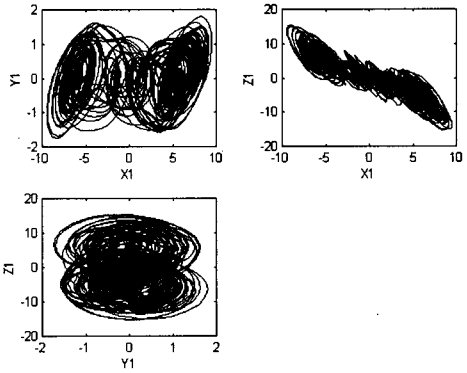


그림 13. 정보 신호를 상태변수 $x_3$에 합성하였을 때의 어트렉터

그림 12과 13을 비교해 보면, 상태 변수 $x_3$를 사용한 경우 $x_1$에 비하여 어트렉터 구성이 단순함을 알 수 있으며, 이는 복조시 보다 완벽한 복조 성능과도 관계됨을 확인할 수 있다.
그림 14에 그림 11에 의한 하이퍼카오스 회로의 중 상태변수 $x_1$에 의한 비밀 통신 결과를 나타내었다.

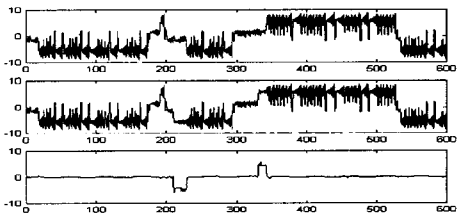


그림 14. 상태 변수 $x_1$에 의한 비밀 통신 복원 결과

그림 15에 그림 11에 의한 하이퍼카오스 회로의 중 상태변수 $x_3$에 의한 비밀 통신 결과를 나타내었다.

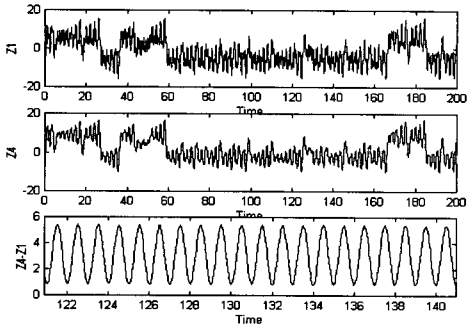



그림 15. 상태 변수 $x_3$에 의한 비밀 통신 복원 결과

그림 14과 그림 15를 비교해 보면 상태변수 $x_3$를 이용한 경우가 복조 성능이 우수함을 확인할 수 있었다.

### 4.2 임베딩 동기화를 통한 비밀통신

식 (11)과 식 (12)의 동기화의 결과를 통하여 다음과 같이 송신부의 식(11)의 상태변수 $x_2$에 그림 8와 같은 정현파 $\sin(2\pi\times 10t)$를 정보신호로 임베딩하여 입력하였다.

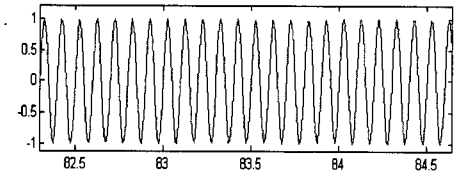


그림 16. 정보 신호

임베딩 동기화를 통한 비밀 통신의 개념을 그림 17에 나타내었다. 임베딩 그림 17은 송수신부의 모든 상태 변수를 구동시키는 기법을 이용하는 대신 하나의 상태 변수만을 송신부에서 임베딩하여 적용한 것이다.

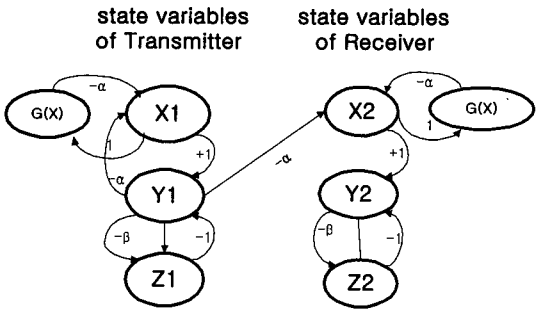
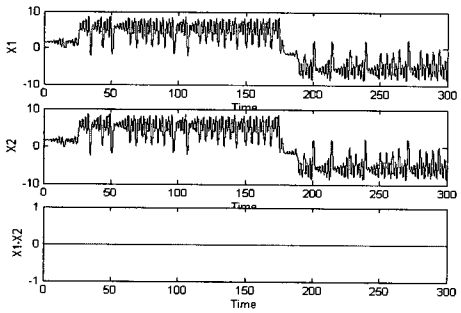
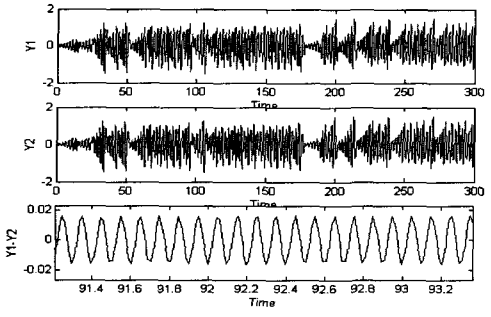



그림 17. 비밀통신 신호 흐름도

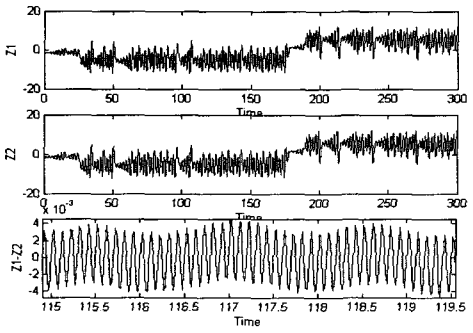
그림 18은 임베딩 동기화에 수신부에서 정보를 복원한 결과를 나타내었다. 그림 18에서 $X1, X2, X3$는 각각 송신부의 상태변수 $x_1, x_2, x_3$를 나타내며, $X2, Y2, Z2$는 각각 수신부의 상태변수 $x_4, x_5, x_6$를 나타낸다. 그림 18의 (a)를 살펴보면 $x_1$과 $x_4$의 신호는 완전히 일치하여 정보신호를 찾을 수 없는 반면 (b),(c)에서는 $x_2$와 $x_5$ 그리고 $x_3$과 $x_4$의 차이 신호에서 정보신호를 복원할 수 있었다.




(a)



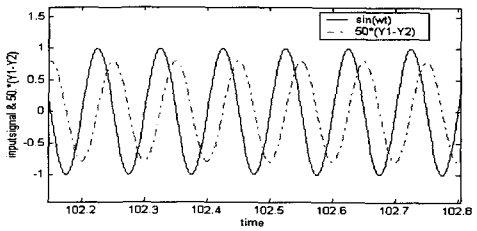

(b)



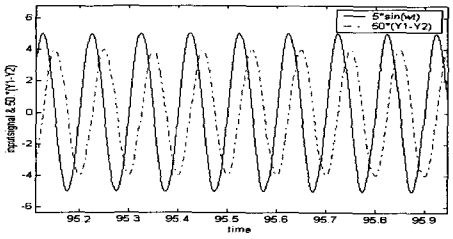

(c)

그림 18. 정보 신호가 포함되었을 때의 각 상태 변수의 신호 비교 (a) $x_1$과 $x_4$ (b) $x_2$과 $x_5$ (b) $x_3$과 $x_6$

그림 19에 정보신호와 복원된 정보신호를 비교하여 나타내었다. 그림 19의 (a)는 $\sin(2\pi 10t)$를 입력신호로 사용하였을 때이며, (b)는 $5\sin(2\pi 10t)$ 를 사용하였을 때이다. 그림 20의 결과를 보면 (a), (b )모두 복원된 정보신호는 입력된 정보 신호의 약 1/60 인 것을 알 수 있다. 즉 카오스 신호에서 시스템 신호와 다른 성질의 신호를 강하게 제거하는 필터의 역할을 하고 있음을 알 수 있다.




(a)




(b)

그림 20. 정보신호와 복원신호의 비교. 입력신호가 (a) $\sin(2\pi 10t)$ (b) $5\sin(2\pi 10t)$일 때

그림 20의 결과를 통하여 일반적으로 Chua 회로에서 정보를 담기 위해서는 정보신호의 크기를 카오스 신호에 충분히 숨길 수 있도록 작게 해야 한다[5]는 내용과 달리 본 연구에서는 아주 큰 진폭을 가진 신호를 정보 신호로 사용할 수 있다는 결과를 얻을 수 있었다.

## V. 결 론

본 연구에서는 SC-CNN을 이용한 하이퍼카오스를 비밀통신과 임베딩 동기화에 의한 비밀 통신 기법에 대하여 살펴보았다. 두 방법에서 정보신호를 하이퍼카오스 신호와 합성할 때 상태 변수 $x_1, x_2, x_3$를 이용하였으며, 이들 각각의 복조 결과를 비교하였다. 상태 변수 $x_3$에 의한 방법은 Chua 회로에서는 하드웨어 구현의 불가능으로 이용하지 못한 방법이었으나 각각의 츄아회로의 상태방정식을 각각의 회로로 재구성하여 다시 이것을 재합성하는 SC-CNN을 적용한 하이퍼카오스 회로에서는 이용할 수 있는 방법임을 제시하

였다. 앞으로 강건한 동기화와 음성 및 디지털 통신에 적용할 수 있는 범용적인 하이퍼카오스 회로와 동기화 기법, 비밀 통신 복조 기법 등이 연구 과제로 남는다.

## 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.

[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.Maganaro," 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*, pp. 7-21. 2001.


### 저 자 소 개


배영철

1984년 2월 광운대학교 전기공학과 졸업
1997년 광운대학교 대학원 전기공학과 졸업(공학박사)
1986-1991 한국전력공사
1991-1997 산업기술정보원 책임연구원
1997- 현재 여수대학교 전기공학과 조교수
※관심분야: 퍼지 및 신경망, 카오스