SC-CNN을 이용한 하이퍼카오스 동기화와 비밀통신

배영철* · 임정석** · 황인호** · 김주완*

Synchronization and Secure Communication in Hyper-chaos system using SC-CNN

Young-Chul Bae* · Lim Jeong Seok** · Hwang In Ho** · Ju-Wan Kim*

요 약

본 연구에서는 간단한 전자회로로 카오스 특성을 나타내는 Chua 회로 대신 더욱 유연성이 있는 SC-CNN(State-Controlled CNN)을 이용해서 2-double scroll 과 3-double scroll 회로를 구성하고 이를 이용하여 하이퍼카오스 회로를 제작하였다. 제작된 하이퍼카오스 회로로 두 개 이상의 카오스 어트렉터가 약한 결합을 하는 과정에서 발생하는 위상차를 이용하여 동기화를 이루고, 동기화된 하이퍼카오스 신호에 정보신호를 합성하여 전송한 후 수신부에서 이를 복조하는 하이퍼카오스 비밀통신을 수행하였다.

ABSTRACT

In this paper, we use hyper chaos circuit which is made through the phase differences which is generated during the process of weak-coupling of CNN between two and more chaos attractors. Notwithstanding the complexity of the hyper chaos, we could do the synchronization and according to it, Secure communication through this method could be accomplished.

On this research, we cofigurated 2-double scroll and 3-double scroll circuit ,not using Chua circuit, but SC-CNN(State-Controlled CNN) which is more flexible to configure the system

키워드

하이퍼카오스, 카오스, 동기화, 암호통신, SC-CNN, 비밀통신

Ⅰ. 서 론

Chua 회로와 같은 카오스 회로는 잡음과 같은 카오스 특성을 이용하여 카오스 신호에 정보 신호를 혼합하여 송신부에서 전송한 후 수신부에서 정보 신호와 카오스 신호를 분리하는 카오스 암호통신에 이용하는 방법이 연구되어 왔으나[5,6] 카오스 신호 자체의 동특성으로 인하여 완벽하게 정보를 보호하지 못하고 도청되는 것으로 알려져 있다.[8,9]

따라서 카오스 신호보다 더 복잡한 하이퍼카오스

*여수대학교 전기 및 반도체 공학과 **전자통신연구원
접수일자 2001년 10월 16일

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. 이에 본 연구에서는 Chua 회로를 변형한 SC-CNN을 이용하여 N-Double scroll 회로를 만든 다음 이를 이용하여 하이퍼카오스 회로를 구성하고, 동일한 하이퍼카오스 회로를 송수신부로 정한 후 하이퍼카오스 회로의 송신부와 수신부 회로의 신호가 일치하도록 하는 하이퍼카오스 동기화 기법과 비밀통신을 제안하고 그 타당성을 검증하였다.

II. n-double scroll 회로

하이퍼카오스 회로를 얻기 위하여 Chua 회로의 변형인 n-double scroll 어트렉터를 고려하였다. n-double scroll을 얻기 위한 전기회로는 Arena에 의해 구현되었으며 상태방정식은 식(1)과 같이 주어지고 비선형 저항의 관계식은 식(2)에 나타내었다.

$$\begin{aligned} \dot{x} &= \alpha[y - h(x)] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{1}$$

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

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

$m_0 = -1/7, \quad m_1 = 2/7, \quad m_2 = -4/7,$

$m_3 = m_1, \quad m_4 = m_2, \quad m_5 = m_3, \quad c_1 = 1,$

$c_2 = 2.15, \quad c_3 = 3.6, \quad c_4 = 8.2, \quad c_3 = 13$

III State-Controlled CNN

(1)과 (2)의 식은 다음과 같이 SC-CNN의 일반식으로 변환할 수 있다.

$$\dot{x}_j = x_j + a_j y_j + G_o + G_s + i_j \tag{3}$$

여기서 j 는 셀 인덱스, x_j는 상태변수, y_j는 다음과 같이 주어지는 셀의 출력,

$$y_j = 0.5 \times (\,|x_j + B_p| - |x_j - B_p|\,) \tag{4}$$

a_j는 상수파라미터, i_j는 문턱값, G_o는 출력들의 선형결합, G_s는 고려되고 있는 연결된 셀들의 상태변수를 나타낸다.

여기에 Chua 회로의 관계식을 적용하면

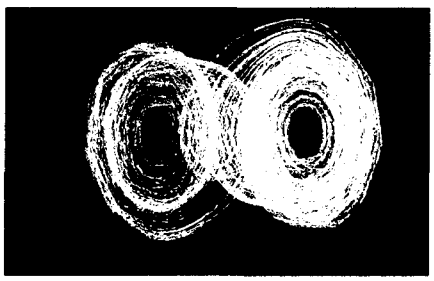
$$\begin{aligned} \dot{x}_1 &= -x_1 + y_1 - 1.5714x_1 + 9x_2 \\ \dot{x}_2 &= -x_2 + x_1 + x_3 \\ \dot{x}_3 &= -x_3 - 14.286x_2 + x_3 \end{aligned} \tag{5}$$

그리고

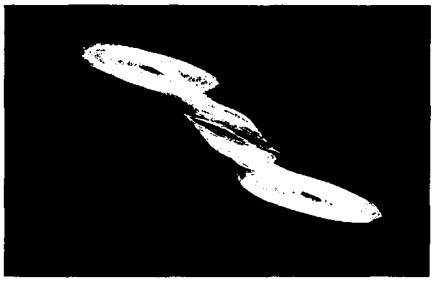
$$\begin{aligned} y_1 = {} & 3.857 \times 1/2(\,|x+1| - |x-1|\,) \\ & - 7.714 \times 1/2(\,|x+2.16| - |x-2.16|\,) \\ & + 7.714 \times 1/2(\,|x+3.6| - |x-3.6|\,) \end{aligned} \tag{6}$$

이 된다.

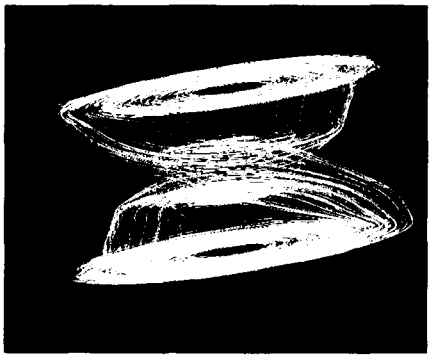
그림 1 에 2-double scroll에 사용하는 비선형 소자의 특성을, 그림 2 에 3-double scroll의 비선형 소자의 특성과 3-double scroll 어트렉터를 각각 나타내었다.



(a)

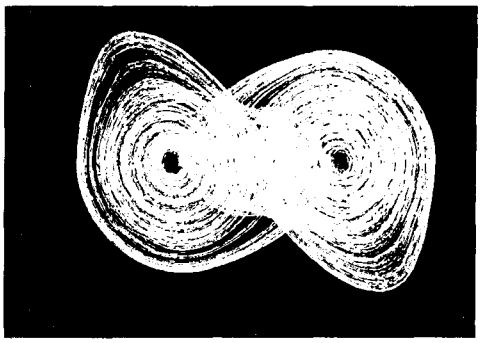


(b)

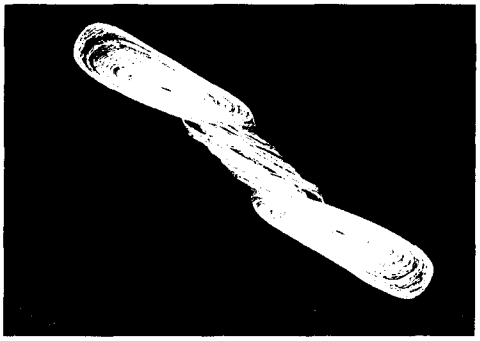


(c)

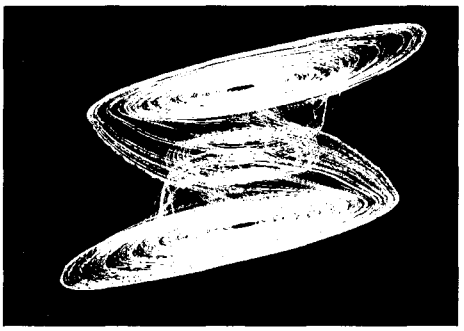
(d)



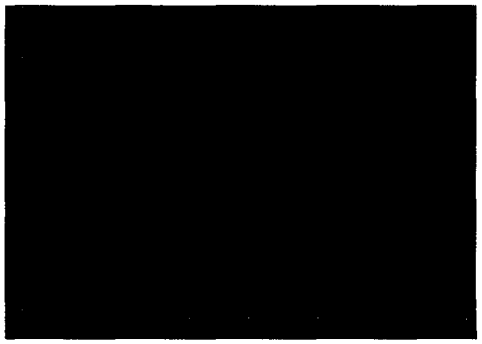
(a)



(b)



(c)



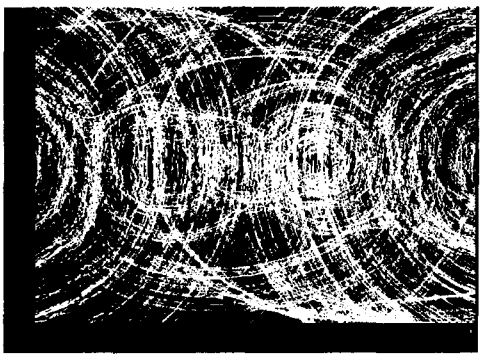
(d)

그림 1. PSpice를 이용한 2-double 스크롤 어트렉터 결과와 비선형 소자특성

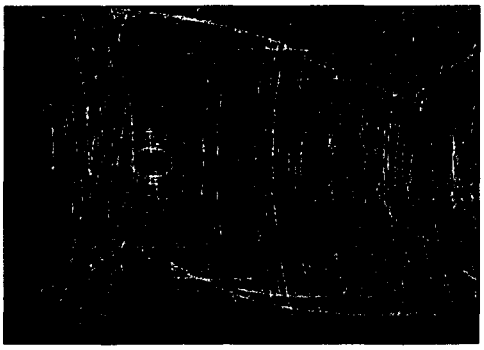
Fig. 1 2-double scroll attractor and nonlinear unit characteristic of 2-double scroll using PSpice

그림 2. PSpice를 이용한 3-double 스크롤 어트렉터와 비선형 소자특성
Fig. 2 3-double scroll attractor and nonlinear unit characteristic of 3-double scroll using PSpice

그림 3에 3-double 어트렉터의 중심부 확대를 나타내었다. 그림 2의 (a) 중심부를 확대한 것이 그림 3(a)이며, 그림 3의 (a)를 확대한 것이 그림 3(b)이다. 그림 3에서 보는바와 같이 3개의 스크롤이 존재함을 확인할 수 있다. 또한 그림3과 같은 확대 영역을 살펴보면 카오스의 자기유사성(self-simility)가 존재함을 확인할 수 있다.



(a)



(b)

그림 3. 3-double 스크롤 어트렉터 확대
Fig. 3 Enlarge of 3-double scroll attractor

Ⅳ. 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(7)에 x-확산 결합, 식(8) y-확산 결합식으로 나타내었다.

$$\begin{aligned} \dot{x}^{(j)} &= \alpha[y^{(j)} - h(x^{(j)}] \\ &\quad + D_x(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ \dot{y}^{(j)} &= x^{(j)} - y^{(j)} + z^{(j)} \\ \dot{z}^{(j)} &= -\beta y^{(j)}, \qquad j = 1,2,\ldots\ldots L \end{aligned} \tag{7}$$

$$\begin{aligned} \dot{x}^{(j)} &= \alpha[y^{(j)} - h(x^{(j)}] \\ \dot{y}^{(j)} &= x^{(j)} - y^{(j)} + z^{(j)} + \\ &\quad D_y(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ \dot{z}^{(j)} &= -\beta y^{(j)}, \qquad j = 1,2,\ldots\ldots L \end{aligned} \tag{8}$$

여기서 L은 셀의 수를 나타낸다.

식(8)을 이용하여 구성한 하이퍼카오스 어트렉터를 그림 4~그림 5에 나타내었다. 그림 4는 2-double scroll 시스템의 2개의 CNN을 이용한 하이퍼카오스 어트렉터를, 그림 5는 3-double scroll 시스템의 4개의 CNN을 이용한 하이퍼카오스 어트렉터를 각각 나타내었다. 2-double scroll 시스템의 4개의 CNN과 3-double scroll 시스템의 2개의 CNN을 이용한 것들에서도 비슷한 닮은 형의 결과를 가져왔다.

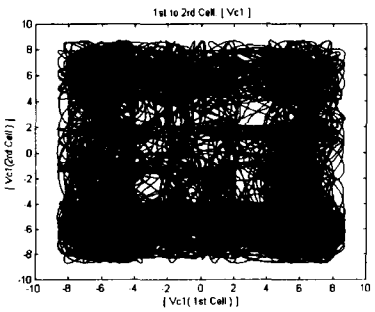


그림 4. 2-double scroll 시스템의 2개의 CNN을 이용한 하이퍼카오스 어트렉터
Fig. 4 Hyper-chaotic attractor using 2 CNNs of 2 double scroll system

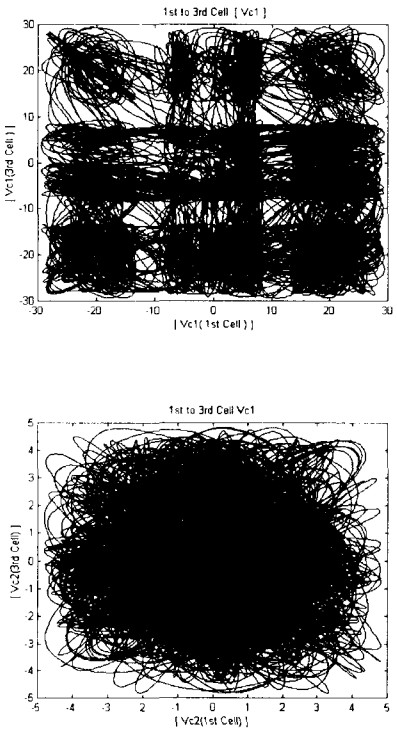


그림 5. 3-double scroll 시스템의 4개의 CNN을 이용한 하이퍼카오스 어트렉터
Fig. 5 Hyper-chaotic attractor using 4 CNNs of 3-double scroll system

V. 하이퍼카오스 회로 동기화

n-double scroll 하이퍼카오스 회로의 동기화를 위하여 동일한 n-double scroll 카오스 회로를 송수신부로 놓고 결합동기에 의한 동기화를 이루었다. 송신부의 상태방정식은 식(9)와 같으며 수신부의 상태방정식은 식(10)과 같다.

송신부의 상태방정식

$$\begin{aligned} \dot{x}^{(j)} &= \alpha[y^{(j)} - h(x^{(j)}] \\ &\quad + D_x(x^{(j-1)} - 2x^{(j)} + x^{(j+1)}) \\ \dot{y}^{(j)} &= x^{(j)} - y^{(j)} + z^{(j)} + K_{j-1}(y^{(j)} - y'^{(j)}) \\ \dot{z}^{(j)} &= -\beta y^{(j)}, \quad j = 1,2,\ldots\ldots L \end{aligned} \tag{9}$$

수신부의 상태방정식

$$\begin{aligned} \dot{x}'^{(j)} &= \alpha[y'^{(j)} - h(x'^{(j)}] \\ \dot{y}'^{(j)} &= x'^{(j)} - y'^{(j)} + z'^{(j)} \\ &\quad + D_y(x'^{(j-1)} - 2x'^{(j)} + x'^{(j+1)}) \\ &\quad + K_{j-1}(y'^{(j)} - y^{(j)}) \\ \dot{z}'^{(j)} &= -\beta y'^{(j)}, \quad j = 1,2,\ldots\ldots L \end{aligned} \tag{10}$$

본 연구에서는 동일한 2개의 2-double scroll 시스템의 2 CNN을 이용하여 송신부와 수신부를 구성한 후 송신부와 수신부의 시스템이 안정하도록 차 시스템(difference system)을 이용하여 결합계수를 결정하면 $K < -1.3$의 범위에서 동기화가 이루어진다.

그림 6과 7에 동일한 2개의 2-double scroll 시스템의 2 CNN에 대한 하이퍼카오스 회로의 동기화 결과를 나타내었다. 그림 6은 동기화 척도로 동일한 시계열 데이터를 겹쳐 놓은 것으로 일직선으로 나타낼 때 동기화가 완전하기 이루어 진 것으로 판단한다. 그림 6의 결과에서는 일정시간 동안 동기화를 이루기 못하다가 동기화가 이루어짐을 알 수 있다.

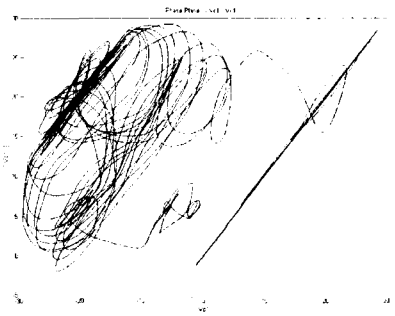


그림 6. 동기화 결과
Fig. 6 The result of synchronization

그림 7은 송수신부의 시계열 데이터의 차를 나타낸 것으로 그림 7에서 확인하듯이 처음에는 동기화가 이루어지지 않았다가 일정시간이 지난 후 동기화가 이루어졌음을 알 수 있다.

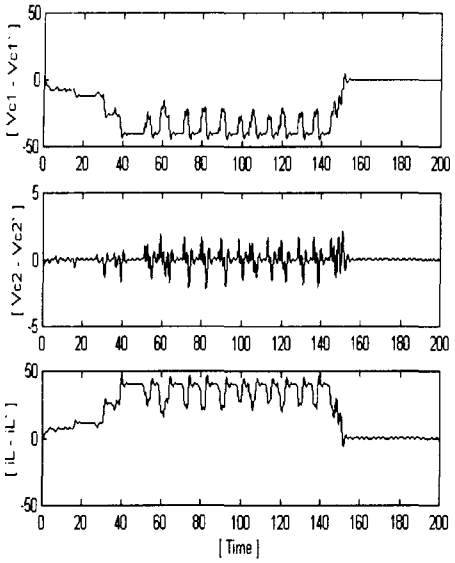


그림 7. 송수신 시계열 데이터 차
Fig. 7 The difference of time-series data between the transmitter and receiving

Ⅵ. 하이퍼카오스 회로 비밀 통신

하이퍼카오스 비밀통신을 위해서 본 연구에서는 두 개의 동일한 2- double scroll 2 CNN 하이퍼카오스 회로를 이용하여 송수신부를 구성하였다. 동일한 2개의 하이퍼카오스 회로에서 송수신수 결합동기에 의한 동기화를 이룬 후 송신부의 복잡한 하이퍼카오스 회로에 정보신호를 가산하여 채널을 통하여 수신부로 전송한 후 수신부에서 정보 신호와 하이퍼카오스 신호를 분리하는 복조 방법을 행하였다. 정보 신호는 정현파를 이용하였다.

그림 8에 하이퍼카오스 비밀 통신에 대한 흐름도를 나타내었다.

그림 9에 송신부에서 캐리어로 이용한 하이퍼카오스 신호의 시계열 데이터를 나타내었으며 그림 10에 정현파의 정보 신호를 나타내었다.

그림 9과 10을 합성하여 합성된 신호를 채널을 통하여 수신부에 전송하고 동기화 기법으로 송수신부를 동기화 시킨 후 수신부의 동기화된 신호에서 캐리어 신호와 정보 신호를 분리하는 방법을 행하였다. 본 연구에서는 채널을 잡음과 왜곡이 없는 이상적인 채널로

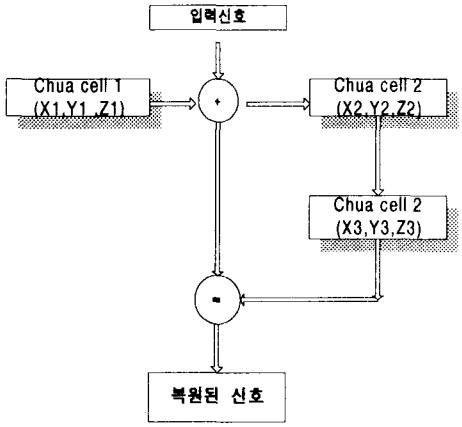


그림 8. 하이퍼카오스 비밀 통신 흐름도
Fig. 8 The Flowchart of hyperchaos secure communication

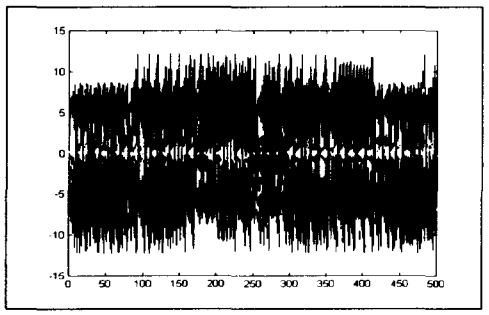


그림 9. 송신부의 캐리어 신호
Fig. 9 The carrier signal of transmitter

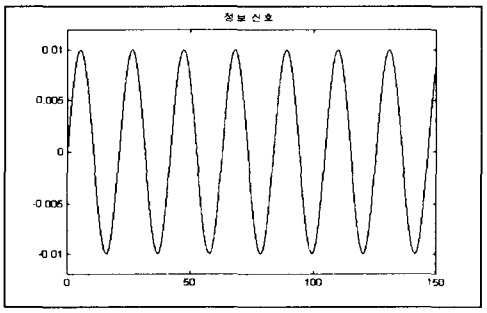


그림 10. 정보 신호
Fig. 10 The information signal

가정하였다.

그림 11은 채널 중간에서 도청한 신호이다. 도청된 신호는 하이퍼카오스 신호로 적당한 신호 처리를 하여도 정보 신호를 복원하지 못하는 것을 알려져 있다.

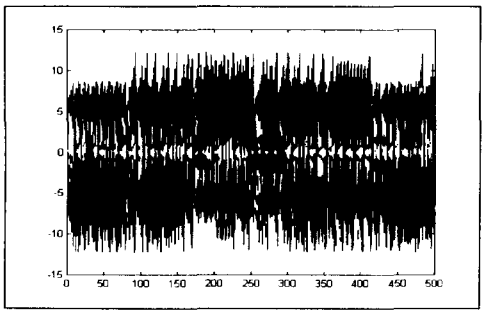


그림 11 중간에 도청한 신호
Fig. 11 The wiretapped signal during transmission

그림 12는 정보 신호와 캐리어 신호를 수신부에서 분리 복조한 신호이다. 그림 11에서 보는 바와 같이 잡음이 많이 포함되어 있음을 확인 할 수 있다.

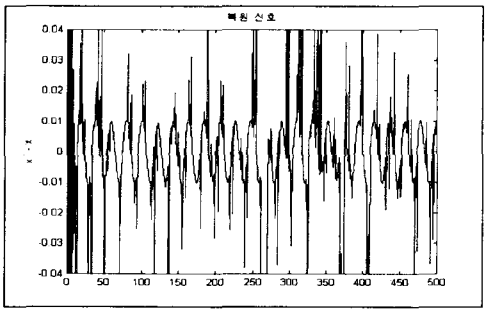


그림 12. 필터링 전 복원 신호 그림
Fig. 12 The recovered signal before filtering

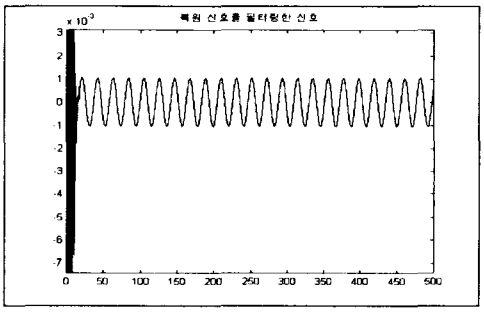


그림 13. 필터링 후 복원 신호
Fig. 13 The recovered signal after filtering

그림 13은 그림 11의 신호를 필터를 이용하여 잡음을 제거한 신호이다. 그림 9의 정보 신호에 근접된 신호가 복원되었음을 확인 할 수 있다.

Ⅶ. 결 론

본 연구에서는 하이퍼카오스를 이용한 동기화와 비밀 통신에 대하여 살펴보았다. 일반적인 카오스 회로에서 도청된 가능했던 신호가 하이퍼카오스 회로에서는 도청의 의미가 없음을 확인하고 이를 비밀통신에 적용할 가능성이 있음을 확인하였다. 앞으로 강건한 동기화와 음성 및 디지털 통신에 적용할 수 있는 범용적인 하이퍼카오스 회로와 동기화 기법, 비밀 통신 복조 기법 등이 연구과제로 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", 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.

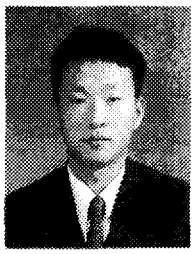
[8] K.M. Cuomo, A.V. Oppenheim & S.H. Strogatz " Robustness and signal recovery in a synchronized chaotic system" Int. J. Bifurcation and Chaos, vol. 3, no. 7, pp. 1629-1638, 1993.

[9] K.M. Short "Signal extraction from chaotic communicarion" Int. J. Bifurcation and Chaos, vol. 7, no. 7, pp. 1579-1597, 1997.
[10] J.Guckenheimer and P.Holmes, Nonlinear Oscillations, Dynamical System, and Bifurcations of vector Field. New York ; Springer - Verlag, 1983.
[11] L.O.Chua, M.Komuro, and T.Matsumoto, "The Double Scroll Family, Part I, and II.", IEEE Trans. on Circuit and System, Vol. CAS - 33, pp. 1073 - 1118, 1988.
[12] T. Matsumoto, L. O. Chua, and M. Komuro, "The Double Scroll" IEEE Trans. on Circuit and System, Vol. CAS-32, pp. 798 - 818, 1985.
[13] T. Matsumoto, "A chaotic Attractor from chua's circuit", IEEE Trans. on Circuit and System, Vol. CAS-31, pp. 1055 - 1058, 1984.
[14] M. Kuramitsu and K. I. Mori, "A simple Electric Circuit Generating chaos" Technical report IEICE, NLP 93 - 68, pp. 31 - 38, 1994.
[15] T. S. Parker, and L. O. Chua, "The Dual Double Scroll Equation" IEEE Trans. on Circuit and System, Vol. CAS-32, pp. 1059 - 1073, 1987.
[16] Y. Ueda & N. Akamatsu, "Chaotically Transitional phenomena, in the Forced Negative - Resistance Oscillator" IEEE Trans. on Circuit and System, Vol. CAS-28, pp. 217 - 224, 1981.
[17] G. O. Z'hong and F. Ayrom, "Experimental Confirmation of chaos from chua's circuit" International Journal of Circuit Theory Apply, Vol. 13, pp. 93 - 98, Jan, 1985.
[18] P. Arena, S. Baglio, L.Fortuna and G. Manganaro, "Generation of n-Double Scrolls via Cellular Neural Networks", Int. J. Circuit Theory and Applications, vol. 24, pp. 241-252, 1996.

배영철(Young-Chul Bae)
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

임정석(Lim Jeong Seok)
1987년 2월 : 한양대학교 전자통신공학과(공학사)
1989년 2월 : 한양대학교 전자통신공학과(공학석사)
2000년 2월 : 한양대학교 전자통신공학과(박사과정 수료)
1989년 2월~2000년 1월 국방과학연구소
2000년 2월~현재 한국전자통신연구원
※주관심분야 : 부호이론,암호이론

황인호(Hwang In Ho)
1980년 2월 : 한양대학교 전자통신공학과(공학사)
1982년 2월 : 중앙대학교 전자공학과(공학석사)
1982.6~1985.12 : 군복무
1986년 2월~2000년 1월 국방과학연구소
1992.3~1999.2 : 한국과학기술원(공학박사)
2000년 2월~현재 한국전자통신연구원
※주관심분야 : 통신 시스템, 신호처리



김주완(Kim Ju Wan)
1998년 2월 : 순천대학교 전자공학과(공학사)
2001년 2월~: 여수대학교 대학원 석사과정