2003년도 대한전기학회 하계학술대회 논문집 2003.7.21-23

SC-CNN을 이용한 하이퍼카오스 회로에서의 비밀 통신

배영철, 김주완
여수 대학교 전자통신, 전기 반도체공학부

Secure Communication of HyperChaos Circuits using SC-CNN

Youngchul Bae, Juwan Kim
Division of Electronic Communication and Electrical Engineering of Yosu National University

Abstract - 본 논문에서는 동일동기화(Identical Synchronization)과 일반동기화 (General Synchronization)를 이용한 하이퍼카오스 시스템을 구성하고 검증하였다. 단일 카오스 모듈을 이용한 통신은 많은 보안의 취약점을 가진 것으로 알려져 있다. 이에 이런 취약점을 보안하기 위해 여러 방법들이 도입되었다. 본 논문은 두 개의 2-double scroll Chua 회로와 두 개의 2-doubl scroll Chua 오실레이터를 이용하여 하이퍼카오스 회로의 송수신단을 구성하고 동기화를 이룬 후 송신단에서 정보신호를 실어 채널을 통해 보내어 수신단에서 이를 복조하는 방법을 제안하였다

1. 서 론

최근에 카오스 회로의 동기화에 관한 많은 관심이 높아지고 있으며 이에 대한 연구가 활발하게 진행되고 있다. 대표적인 카오스회로인 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 회로[1]를 그림 1에, Chua 오실레이터[17]를 그림 3에 나타냈으며 상태방정식은 식(1)~식(4)와 같이 각각 표시된다.

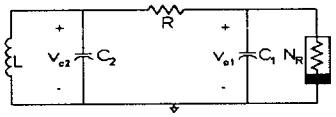

그림 1. Chua 회로
Fig. 1 Chua's circuit

$$C_1\frac{dv_{C_1}}{dt}=G\,(v_{C_2}-v_{C_1})-g(v_{C_1})$$
$$C_2\frac{dv_{C_2}}{dt}=\;G\,(v_{C_1}-v_{C_2})+i_L \qquad (1)$$
$$L\frac{di_L}{dt}=\;-v_{C_2}$$

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

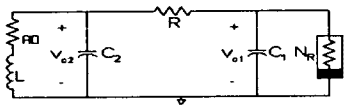

그림 2. Chua 오실레이터
Fig. 2 Chua Oscillator

$$C_1\frac{dv_{C_1}}{dt}=G\,(v_{C_2}-v_{C_1})-g(v_{C_1})$$
$$C_2\frac{dv_{C_2}}{dt}=\;G\,(v_{C_1}-v_{C_2})+i_L \qquad (3)$$
$$L\frac{di_L}{dt}=\;-v_{C_2}-R_0i_3$$

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

여기서 m_0 는 외부 영역의 기울기, m_1 은 내부 영역의 기울기, $\pm B_P$ 는 break-point이다. 그리고 Chua Oscillator 는 그림 2와 식 (3)에 나타내었다.

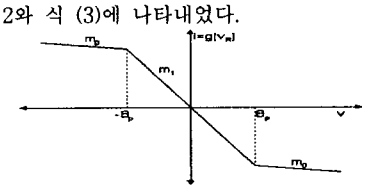

그림 3. 비선형 저항의 전압 전류 특성
Fig. 3 v-i characteristic of nonliner resistor

카오스 동기화 기법은 카오스 암호화나 비밀통신에 이용하기 위한 필수적인 단계이나 카오스 암호화나 비밀통신의 안전성이 카오스 신호 자체의 동특성으로 인하여 보장받지 못하고 있는 실정이다.[15] 이에 본 연구에서는 카오스신호보다 복잡성이 큰 하이퍼카오스 회로에서의 동기화 기법을 제안하고자 한다. 이를 위하여 Chua 회로 2개를 하나의 서브시스템으로, Chua 오실레이터를 2개를 하나의 서브시스템으로 구성하여 GS(Generalized Synchronization) 동기화를 한 후 이것으로 송신단과 수신단을 각각 구성하여 IS(Identical Synchronization)동기화를 적용한 후 정보신호를 송신단에서 하이퍼카오스 신호에 합성하고 수신단에서 이를 복조하는 기법을 제시하였다.

2. 관 계 이 론

2.1 N-double scroll 회로

본 논문에서는 Chua 회로의 변형인 n-double scroll 어트렉터를 적용하였다. n-double scroll을 얻기 위한 전기회로는 Arena[12]에 의해 구현되었으며 상태방정식은 식(5)과 같이 주어지고 비선형 저항의 관계식은 식(4)에 나타내었다.

$$\dot{x}=\alpha[y-g(x)]$$
$$\dot{y}=x-y+z \qquad (5)$$
$$\dot{z}=-\beta y$$

$$g(x)=m_{2n-1}x+\frac{1}{2}\sum_{i=1}^{2n-1}(m_{i-1}-m_i)(|x+c_i|-|x-c_i|) \qquad (6)$$

식(6)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

$m_0=-1/7,\quad m_1=2/7,\quad m_2=-4/7,$
$m_3=m_1,\quad c_1=1,\quad c_2=2.15,\quad c_3=3.6$
(7)

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 4에 2-double scroll 어트렉터와 비선형 저항을 나타내었다.

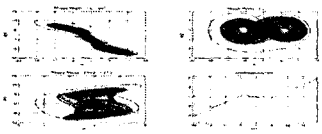

그림 4. 2-double scroll 위상공간과 비선형 저항
Fig. 4 phase plane of 2-double scroll and nonlinear resistor

2.2 SC-CNN

본 논문에서는 Chua 회로와 Chua 오실레이터 시스템의 흐름을 보다 쉽게 구현할 수 있는 SC-CNN 회로를 사용하였다. 문헌[12,13]에서 다음과 같은 일반화된 셀 모델을 만들 수 있다.

$$\dot{x}_j=-x_j+a_jy_j+G_o+G_s+i_j \tag{8}$$

여기서 j는 셀 수, x_j는 상태 변수, y_j는 비선형 소자의 셀출력을 나타내며 a_j는 상수 파라미터, i_j는 임계값(threshold value)이다

식(7)에서 G_o는 출력의 선형 조합이며, G_s는 연결 셀의 상태 변수이다. 식 (8)의 출력 비선형 출력은 식(9)과 같은 새로운 출력 PWL 방정식을 이용한다..

$$y_j=\frac{1}{2}\sum_{k=1}^{2n-1}n_k(|x+b_k|-|x-b_k|) \tag{9}$$

여기서 b_k는 차단점(break point)이며 n_k는 선형 구간의 기울기와 관련된 계수로서 식(7)에 나타나 있다.
SC-CNN 셀은 상태 방정식(8)과 출력 방정식 (9)의 조합으로 식 (10)과 같은 n-Double scroll을 만들 수 있다.

$$\dot{x}_1=-x_1+a_{11}y_1+a_{12}y_2+a_{13}y_3+\sum_{k=1}^{3}s_{1k}x_k+i_1$$
$$\dot{x}_2=-x_2+a_{21}y_1+a_{22}y_2+a_{23}y_3+\sum_{k=1}^{3}s_{2k}x_k+i_2 \tag{10}$$
$$\dot{x}_3=-x_3+a_{31}y_1+a_{32}y_2+a_{33}y_3+\sum_{k=1}^{3}s_{3k}x_k+i_3$$

여기서 x_1,x_2,x_3는 상태 변수이며, y_1,y_2,y_3는 이에 대응한 출력 변수이다. 2-double scroll 회로를 만들기 위해서는 $a_{12}=a_{13}=a_{21}=a_{22}=a_{23}=a_{32}=a_{33}=a_{31}=0$
$s_{13}=s_{31}=s_{22}=0$, $i_1=i_2=i_3=0$로 하면 식(5)과 같은 형태로 바뀌게 된다.
식(10)에 기초한 PSpice를 이용한 CNN회로를 그림 4에 나타내었다.

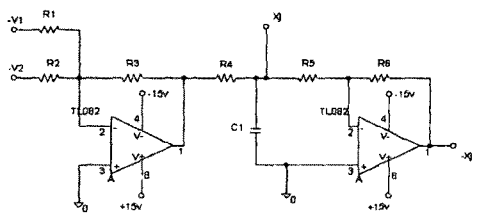

그림 5. CNN 회로도
Fig. 5 CNN circuit

그림 4의 상태방정식을 세우면 식 (9)와 같다.

$$C_j\dot{x}_j=-\frac{x_j}{R_4}+\frac{R_3}{R_1R_4}V_1+\frac{R_3}{R_2R_4}V_2 \tag{11}$$

식(6)에서처럼 V_{C_1}, V_{C_2}, i_L의 상태변수로 표현되는 SC-CNN 회로에서는 시스템내에서의 상태변수의 결합과 조정이 훨씬 간단하게 될 수 있다.

2.3 Secure Communication of HyperChaotic Circuit

SC-CNN을 기반으로 한 하이퍼카오스 회로를 다음과 같이 구성하였다. 하이퍼카오스는 카오스 회로 두 개 이상이 함께 연결되어 구성하는데, 여기에서는 2개의 2-double scroll Chua 회로와 2개의 Chua 오실레이터가 송신단을 구성하고 같은 방식으로 수신단이 구성된다.

$$\dot{x}=Ax+g(w),$$
$$g(w)=[g(x_1+K_1\times x_7)\ 0\ 0\ g(x_1+K_2\times x_{10})\ 0\ 0]^T$$
$$\dot{x}'=Ax'+g'(x')+F(x,x') \tag{12}$$
$$\dot{y}=Ay+g(x)$$
$$g(x)=[g(x_1)\ 0\ 0\ g(x_7)\ 0\ 0];$$
$$\dot{y}'=A'y'+g'(y')+F(y,y') \tag{13}$$

여기서 $x=[x_1,\ldots,x_6]^T=[y_1,\ldots,y_6]^T$ 2-double scroll Chua 회로의 상태변수를, $x'=[x'_1,\ldots,x'_6]^T=[y'_1,\ldots,y'_6]^T$는 2-double scroll Chua Oscillator이다. $g(x)$는 비선형 소자로서 식(4)로 표현된다. A, A'는 다음과 같다.

$$A=\begin{bmatrix}0&\alpha&0&0&0&0\\1&-1-K&1&0&K&0\\0&-\beta&0&0&0&0\\0&0&0&-\alpha&\alpha&0\\0&K&0&1&-1-K&1\\0&0&0&0&-\beta&0\end{bmatrix} \tag{14}$$

$$A'=\begin{bmatrix}0&\alpha&0&0&0&0\\1&-1-K&1&0&K&0\\0&-\beta&\gamma&0&0&0\\0&0&0&-\alpha&\alpha&0\\0&K&0&1&-1-K&1\\0&0&0&0&-\beta&\gamma\end{bmatrix} \tag{15}$$

$F(x,x')$는 선형 피드백을 통한 Chua 회로와 Chua 오실레이터사이에 GS 동기화를 위한 함수벡터이며 다음과 같다[16]

$$F(x,x')=[M(x_1+x_4-x'_1),0,0,$$
$$M(x_1+x_4-x'_1-x'_4),0,0]^T \tag{16}$$
$$F(y,y')=[M(y_1+y_4-y'_1),0,0,$$
$$M(y_1+y_4-y'_1-y'_4),0,0]^T$$

이 때 GS동기화가 될 수 있는 조건을 결합계수 M이 식(17)의 조건일 때 보조시스템 들의 결합에서 GS동기화가 이루어진다.[18]

$$M>\frac{\alpha'}{K'+1}+\alpha'(\max\{|a|,|b|\}-1) \tag{17}$$

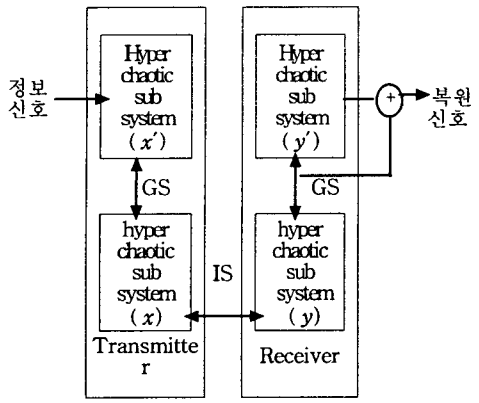

그림 6. 하이퍼카오스 비밀통신의 개략도
Fig. 6 The diagram of the hyperchaotic secure communication

그림 6에서 x'는 상태변수의 입력단이며 송신부와 수신부는 IS를 적용하였고 각 송수신부의 부시스템은 GS동기화 기법을 적용하였다.

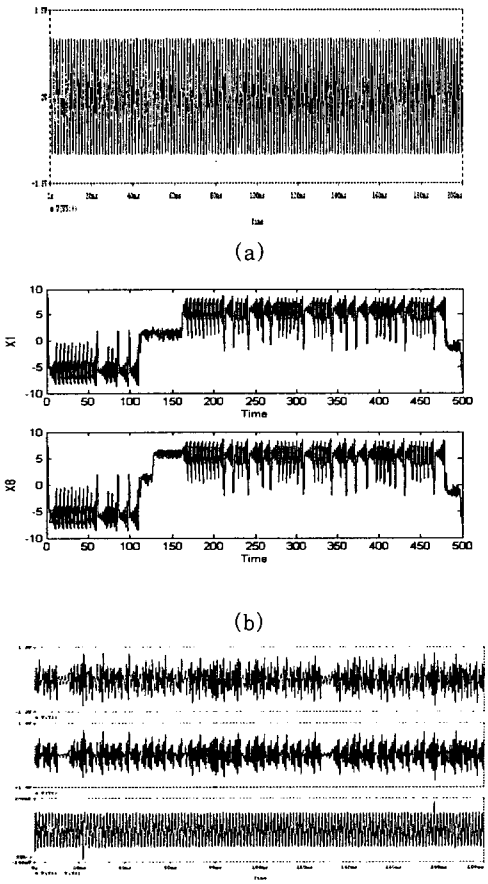

그림7. 송수신신호의 비교(a)입력신호($\sin(2\pi ft)$)
(b)합성된신호(c)복원된 신호
Fig. 7 The timeseries comparision of the transmitted and received signal.(a)Information signal($\sin(2\pi ft)$)
(b)synthesized signal(c)restored signal

그림 7은 하이퍼카오스 회로의 동기화 결과를 바탕으로 비밀통신에 적용하여 그 결과를 나타낸 것으로 제안한 방법이 적용됨을 확인하였다.

3. 결 론

본 연구에서는 송신단과 수신단 각각에 2개의 Chua 회로와 Chua 오실레이터회로를 이용하여 각각 2개의 하이퍼카오스 회로를 만들고 Chua회로와 Chua오실레이터사이에 GS동기화 기법과 송수신단 사이에는 IS(Identical Synchronization)동기화 기법을 적용하여 비밀통신에 적용하였다.

[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] 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.
[7] L. O. Chua "Chua's circuit 10 Years Later", Int. J. Circuit Theory and Application, vol. 22, no. pp 79-305, 1994
[8] M. Itoh, K. Komeyama, A. Ikeda and L. O. Chua, " Chaos Synchronization in Coupled Chua Circuits", IEICE. NLP. 92-51. pp. 33-40. 1992.
[9] K. M. Cuomo, " Synthesizing Self - Synchronizing Chaotic Arrays", Int. J.Bifurcation and Chaos, vol. 4, no. 3, pp. 727-736, 1993.
[10] L. M. Pecora and T. L. Carroll "Synchronization in Chaotic System" Phy. Rev. Lett., vol. 64, no. 8, pp. 821-824, 1990.
[11] 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.
[12] 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.
[13] 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.
[14] L. Kocarev, Chaos-based cryptography: A brief overview, IEEE, Vol. pp. 7-21. 2001.
[15] Michele Brucoli, "Design of a hyperchaotic cryptosystem based on identical and generalized synchronization", Intl' Journal of Bifurcation and Chaos, Vol 9, No. 10, 1999 ,2027-2037.
[16] Kocarev, . & Parlitz, U.,"Generalized synchronization, predictability and equivalence of unidirectionally coupled dynamical systems." Phys. Rev. Lett. 76(11),1816-1819.
[17] Tao Yang & Leon O Chua,"Secure Communication via Chaotic parameter modulation", IEEE transaction on Circuit and Systems,Vol 43,No. 9, 1996.
[18]Abarbanel,H.D.I.,Rulkov,N.F. &Sushchik, M.M. "Generalized synchronization of chaos: The auxiliary system approach",Phys.Rev. E53(5), 4528-4535, 1996.