전송선로를 가진 카오스 회로에서의 카오스 암호화 통신

배영철

여수대학교

Chaos Secure communication of Chaos Circuit with Transmission Line

Young-chul Bae

Nat'l Yosu University

E-mail : ycbae@yosu.yosu.ac.kr

요 약

Pecora와 Carroll[10]이 제시한 구동 동기 이론을 적용하여 전송선로를 가진 Canonical Chua 회로에서 카오스 암호화 통신이 이루어짐을 확인하였다.
본 논문에서는 이 구동 동기 이론에 따른 불필요한 부분을 제거하고 이를 선로로 치환하여 Chua 회로의 구동부와 응답부 사이에 놓아 전송선로를 구성하였으며 송신부에서 구형파의 정보 신호를 카오스 신호에 합성하여 전송선로를 통하여 전송하고 수신부에서 정보 신호와 카오스 신호를 복조하는 카오스 암호 통신을 행하였다.

ABSTRACT

This paper investigates the chaos secure communication with transmission line. The secure communication of chaos in two coupled canonical Chua's circuit with transmission line systems are studied.. We expected that to be available to apply this secure communication with digital communication.

Ⅰ. 서 론

최근에 카오스 현상에 대한 관심이 물리학, 화학, 생물학, 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다[1-3]. 간단한 전기 및 전자 회로를 구성하여 카오스 현상이 존재함을 증명하는 논문도 발표되고 있으며[4-5] 이를 대표하는 것으로 Chua 회로를 들 수 있다[6-9]. Chua 회로는 다양한 카오스 현상을 관찰할 수 있을 뿐만 아니라 카오스 동기화, 카오스 제어, 암호 통신 등에 이용할 수 있다.

Chua 회로를 이용하여 카오스 암호 통신을 구현하고자 하는 노력이 계속되고 있으며 몇몇 관심있는 발표도 나오고 있다[10-11].
Chua와 Itoh[11]는 Chua 회로와 canonical Chua 회로를 이용하여 카오스 변조 통신을 행하였다.
본 논문에서는 Chua 회로를 일반화한 Canonical Chua 회로에서 Pecora와 Carroll[10]이 제시한 구동 동기 이론을 적용하여 불필요한 회로를 없애 전송선로를 구성한 후 송신부에서 카오스 신호에 정보 신호를 합성하여 전송 선로 통하여 전송하고 이를 수신부에서 분리하는 카오스 암호화 통신 방법을 제안하였다.

Ⅱ. Chua 회로와 Canonical Chua 회로

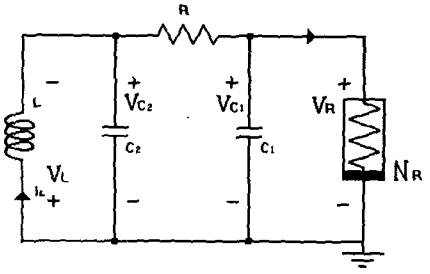
Chua 회로는 매우 단순한 자율, 3차계 시스템으로 Reciprocal이며 1개의 비선형 소자인 3 구분 선형 저항(3 segment piecewise - linear resistor)과 4개의 선형 소자인(R, L, C_1, C_2)로 구성되는 발진회로다.
Chua 회로의 카오스 어트렉터는 Matsumoto [6]가 컴퓨터 시뮬레이션으로 처음 제시하였으며 이후 실험에 의한 Chua 회로의 카오스 어트렉터를

증명한 연구[9]도 있었다.

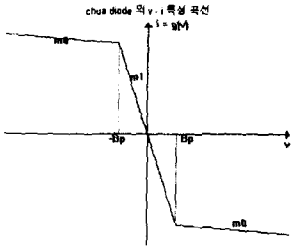
Matsumoto에 의해 제안된 Chua 회로[6]를 그림 1(a)에 나타냈으며 상태방정식은 다음과 같이 표시할 수 있다.

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

여기서 $G = 1/R$, $g(\cdot)$는 식 (2) 와 같이 표현되는 구분 선형 함수(piecewise-linear function)이며 그림 1(b)에 나타내었다.



(a) Chua 회로



(b) 구분 선형 함수

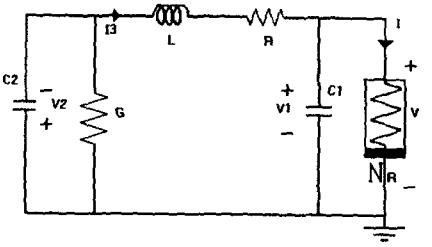
그림 1. Chua 회로와 구분 선형 함수

Canonical Chua 회로는 Chua 회로를 일반화하기 위해 구성한 회로로서 그림 2와같이 나타낼 수 있으며 회로의 상태 방정식은 다음과 같다.

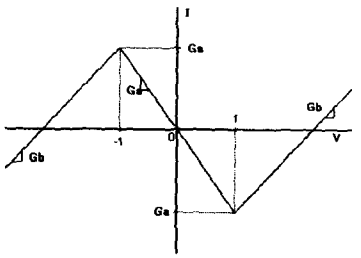
$$\frac{dv_1}{dt} = \frac{1}{C_1}[-f(v_1)+i_3]$$
$$\frac{dv_2}{dt} = \frac{1}{C_2}[-Gv_2+i_3] \qquad (2)$$
$$\frac{di_3}{dt} = -\frac{1}{L}[v_1+v_2+Ri_3]$$

여기서

$f(v) = G_b v + \frac{1}{2}(G_a - G_b)(|v+1|-|v-1|)$이다



(a) Canonical Chua 회로



(b) 구분 선형 함수

그림 2. Canonical Chua 회로와 구분 선형 함수

III. 구동 동기 이론[10]

Pecora와 Carroll[10]에 의해 제시된 구동 동기 이론은 동기될 한쌍의 카오스 회로에서 첫 번째 카오스 회로를 구동 시스템(drive system) 이라 하고 두 번째 카오스 회로를 응답 시스템(response system)이라 한다면 구동 시스템 상태 변수 중 몇 개의 상태 변수 만을 응답 시스템으로 전송하면 전송된 몇 개의 상태 변수들에 의해 전송되자 않는 나머지 상태 변수들로 응답 시스템에 나타남으로써 동기를 이루는 방법이다.

구동 동기 이론에 의한 동기화 결과는 응답 시스템의 CLE(Conditional Lyapunov exponent)가 모두 음수일 때 동기화가 이루어진 것으로 본다. 즉 상태 방정식의 고유값을 $(\lambda_1, \lambda_2, \cdots, \lambda_{n-m})$이라 할 때 이들 고유값의 실수부가 CLE가 된다.

이때 CLE의 모든 값이 음수이면 $\lim_{t\to\infty}\zeta(t)=0$ 되어 부시스템은 동기화, CLE가 양수이면 부시스템은 동기화 되지않음을, CLE가 0이라면 수렴도 발산도 하고 초기 조건에 의한 일정거리를 유지함을 나타내기 때문에 CLE 값으로 동기화를 판정할 수 있다.

Chua[12] 등은 Pecora와 Carroll[10]에 의해 제시된 구동 동기 이론을 Chua 회로에 적용하였으나 본 논문에서는 전송선로의 치환이 용이한 Canonical Chua에 구동 동기 이론을 적용하였으며 파라미터 값을 식(3)과 같이 정하였다.

$$C_1=1$$
$$C_2=-0.632,\quad G=-0.0033,\quad L=-1.02,$$
$$G_a=-0.419,\quad G_b=0.839,\quad R_0=-0.33 \qquad (3)$$

그림 3에 Canonical Chua 회로의 V_1구동 동기화 회로를 나타내었으며 상태방정식은 식(4),(5)과 같이 정리된다.

$$\frac{dv_1}{dt}=\frac{1}{C_1}[-f(v_1)+i_3]$$
$$\frac{dv_2}{dt}=\frac{1}{C_2}[-Gv_2+i_3] \qquad (4)$$
$$\frac{di_3}{dt}=-\frac{1}{L}[v_1+v_2+Ri_3]$$

$$\frac{dv_2'}{dt}=\frac{1}{C_2}[-G(v_2')+i_3'] \qquad (5)$$
$$\frac{di_3'}{dt}=-\frac{1}{L}[v_1'+v_2'+Ri_3']$$

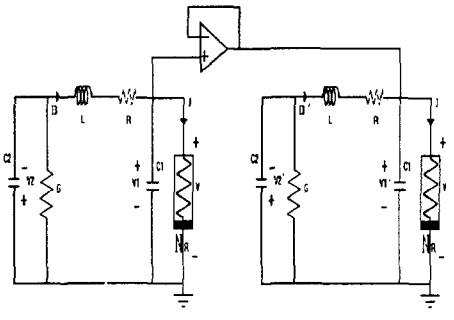
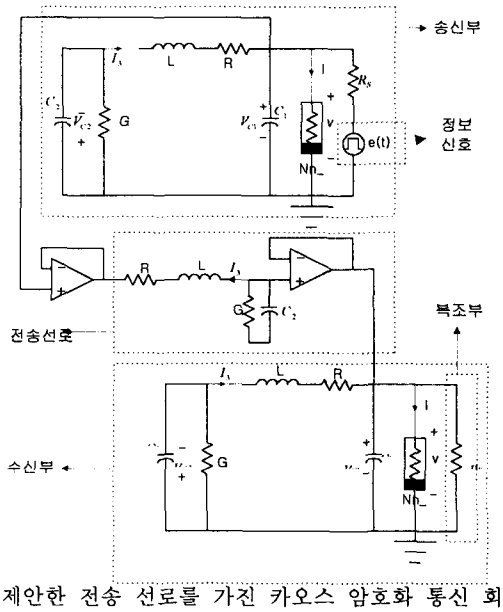


그림 3. Canonical Chua 회로의 V_1 구동 동기화 회로

V. 전송선로를 가진 카오스 암호화 통신

Chua 회로에 구동 동기 이론[12]을 적용하면 Chua 회로의 응답 시스템 중 불필요한 부분이 존재한다. Canonical Chua 회로에서도 Chua 회로와 동일하게 구동 동기 이론을 적용하면 불필요한 부분이 존재한다. 그림3에서 V_1구동 동기에 의한 불필요한 부분은 비선형 저항 N_R과 C_1 부분이다. 이 두 요소를 제거하면 전송선로와 동일한 회로가 구성됨을 알 수 있다.

본 논문에서는 이 불필요한 부분을 제거하여 전송 선로로 치환한 후 전송 선로를 중간에 두고 Canonical Chua를 양단에 두어 전송선로를 중심으로 왼쪽단은 구동회로(송신부)로 오른쪽단은 응답회로(수신부)를 구성하고 구성된 회로의 송신부에서 정보 신호와 카오스 신호를 합성하고 전송선로를 통하여 수신부에 전송한 후 정보 신호와 카오스 신호를 분리하는 카오스 암호화 통신 방법을 제안하였다.



제안한 전송 선로를 가진 카오스 암호화 통신 회로를 회로를 그림 4에 나타내었다.

그림 4. 전송 선로를 가진 카오스 동기화 회로

그림 4의 상태방정식을 다음과 같이 정리할 수 있다.

전송 시스템의 상태방정식

$$\frac{dv_1}{dt}=\frac{1}{C_1}[-f(v_1)+i_3+\frac{e(t)-v_1}{R_s}]$$

$$\frac{dv_2}{dt} = \frac{1}{C_2}[-Gv_2 + i_3] \quad (6)$$

$$\frac{di_3}{dt} = -\frac{1}{L}[v_1 + v_2 + Ri_3]$$

정보 신호로서 전압원 e(t)를 사용하였고, 전송 신호로서 카오스 신호인 $v_1(t)$ 신호를 사용하였다.

중간 전송 선로단의 상태방정식

$$\frac{dv_2'}{dt} = \frac{1}{C_2}[-G(v_2') + i_3']$$

$$\frac{di_3'}{dt} = -\frac{1}{L}[v_1' + v_2' + Ri_3'] \quad (7)$$

수신부의 상태방정식($V_1=V_1''$)

$$\frac{dv_1''}{dt} = \frac{1}{C_1}[-f(v_1'') + i_3'' + \frac{e(t)-v'_1}{R_s}]$$

$$\frac{dv_2''}{dt} = \frac{1}{C_2}[-Gv_2'' + i_3''] \quad (8)$$

$$\frac{di_3''}{dt} = -\frac{1}{L}[v_1'' + v_2'' + Ri_3'']$$

식(7)식으로부터 정보 신호 e(t)는 다음과 같이 얻을 수 있다.

$$e(t) = R_s[\ C_1\frac{dv_1}{dt} + f(v_1) - i_3 + \frac{v_1}{R_s}] \quad (9)$$

그림4의 j(t)는 다른 다음 관계식으로부터 구할 수 있다.

$$j(t) = \frac{e(t)}{R_s} = [\ C_1\frac{dv'_1}{dt} + f(v'_1) - i'_3 + \frac{v'_1}{R_s}] \quad (10)$$

VI. 시뮬레이션 및 결과 검토

구동 동기 이론을 이용하여 전송 선로를 가진 Canonical Chua 회로의 암호화 통신 방법은 방법은 그림5의 회로를 이용하여 PSpice로 컴퓨터 시뮬레이션을 수행하였다.
정보신호로 그림 6과 같은 다중 주파수의 크기 -50[mV]~+50[mV], 주기 5[ms]인 구형파 신호를 인가하였다..

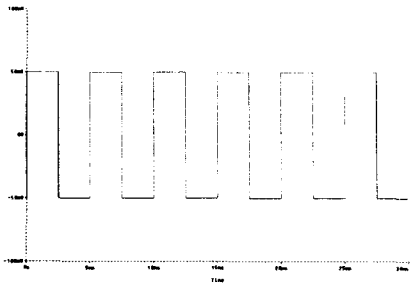


그림 5.정보 신호

그림6, 그림7에 송신부의 시계열 데이터와 수신부의 시계열 데이터를 나타내었으며 동기화기 이루어졌음을 확인 할 수 있다.

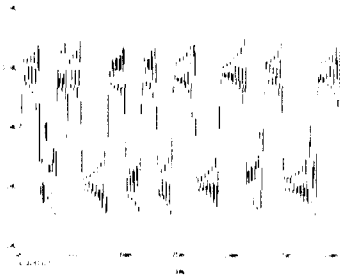


그림6. 송신부의 시계열 데이터

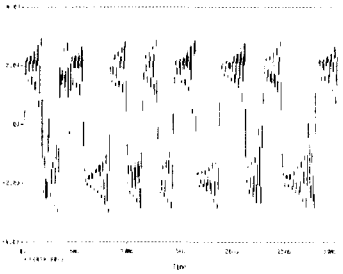


그림7. 수신부의 시계열 데이터

그림8은 중간에서 도청한 신호를 나타낸 그림으로 카오스 신호가 도청이 됨을 알 수 있다

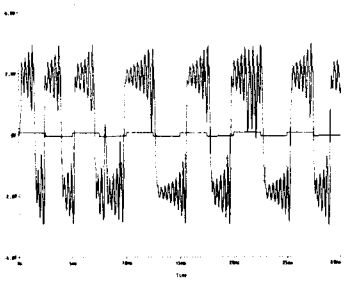


그림8. 중간에서 도청한 신호

그림9에 정보 신호와 수신부에서 복원한 복원 신호를 비교하여 나타내었다. 복권 결과 우수한 복원 성능이 있음을 확인할 수 있다.

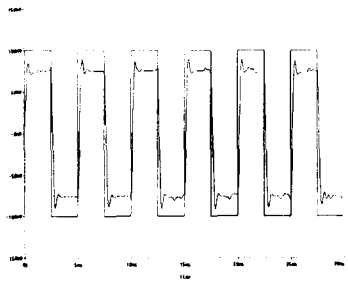


그림9. 정보 신호와 복원 신호의 비교

Ⅵ. 결 론

본 논문에서는 Chua 회로의 구동 동기 개념을 Canonical Chua 회로에 적용하여 불필요한 부분을 제거하여 전송 선로를 구성한 후 전송선로 양단에 Canonical Chua 회로의 구동부와 응답부를 구성한 후 구동동기 개념을 이용한 카오스 암호화 통신 방법을 제안하였다. 컴퓨터 시뮬레이션 결과 수신부에서 완전하게 정보 신호가 복원되었음을 확인할 수 있었다. 제안한 방법을 이용하여 전송 선로를 가진 회로에서 암호화 통신에 적용할 수 있을 것으로 보이며 실선로에 적용이 과제로 남는다.

참고문헌

[1] 배영철, 카오스의 응용, 전자 저널, pp 110 - 112, 1993.

[2] 배영철, 임화영 "주기적 외력을 인가한 Bonhoeffer - Van der Pol 오실레이터 모델에서의 카오스 현상 해석에 관한 연구" 1995 한국통신학회지 제20권 11호 pp 2991 - 3000, 1995

[3] 고재호, 배영철, 임화영 "연속시간 시스템에서의 카오스 피드백 제어 " 1995 제어계측연구회 학술 발표회 논문집, pp 112 - 114, 1995

[4] M. Kuramitsu and K. I. Mori "A simple Electric Circuit Generating chaos" Technical report IEICE, NLP 93 - 68, pp 31 - 38, 1994

[5] Y. Ueda & N. Akamatsu "Chaotically Transitional phenomena, in the Forced Negative - Resistance Oscillator" IEEE Trans, Circuit Syst., Vol. CAS-28, No. 3, pp 217 - 224, 1981

[6] T. Matsumoto "A chaotic Attractor from chua's circuit", IEEE Trans. Circuit Syst., Vol. CAS-31, No. 12,. pp 1055 - 1058, 1984

[7]T. S. Parker, and L. O. Chua "The Dual Double Scroll Equation" IEEE Trans. Circuit Syst., Vol. CAS-32, No. 9, pp 1059 - 1073, 1987

[8] G. O. Z'hong and F. Ayrom "Experimental Confirmation of chaos from chua's circuit" Int. J. Circuit Theory Appl. Vol. 13, pp 93 - 98, Jan, 1985

[9] T. Matsumoto, L. O. Chua, and M. Komuro. "The Double Scroll" IEEE. Trans. Circuit Syst. Vol. CAS-32, No. 8, pp 798 - 818, 1985

[10] L. M. Pecora and T. L. Carroll "Synchronization in Chaotic System" Phy. Rev. Lett. Vol. 64, No.8, pp. 821-824, 1990

[11] M. Itoh, H. Murakami, L. O. Chua "Communication System Via Chaotic Modulations" IEICE. Trans. Fund. Vol. E77-A, No.6, pp. 1000-1005, 1994