Chua 회로를 이용한 카오스 암호화 통신

배 영 철**o · 고 재 호* · 방 성 윤* · 임 화 영*
광운대학교 공과대학 *제어 계측 공학과 **전기 공학과

Chaos Secure Communication Using Chua's Circuit

*Bae yeong - chul*** , *Ko jae - ho** *Bang sung - yun** , *Yim wha - yeong**
*Dept. of control and insrumentation Eng. ** Dept. of electrical Eng. Kwangwoon Univ.

Abstract
This paper investigates the chaos secure communication with RLCG transmission line. The synchronization of chaos in two coupled Chua's circuit with RLCG transmission line systems are also studied.

1. 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 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 어트랙터는 Matsumoto[6]가 컴퓨터 시뮬레이션으로 처음 제시하였으며 이후 실험에 의한 Chua 회로의 카오스 어트랙터를 증명한 연구[9]도 있었다.

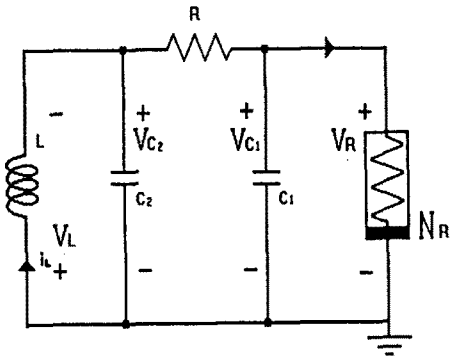
Matsumoto에 의해 제안된 Chua 회로[6]를 그림 1(a)에 나타냈으며 상태방정식은 다음과 같이 표시할 수 있다.

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

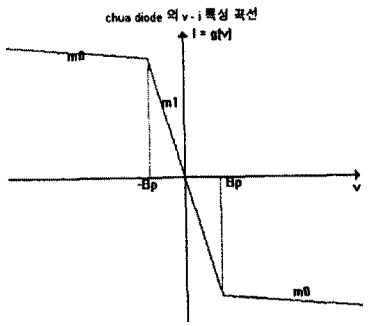
$$C_2\frac{dv_{C_2}}{dt} = G(v_{C_1}-v_{C_2}) + i_L$$

$$L\frac{di_L}{dt} = -v_{C_2} \quad (1)$$

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

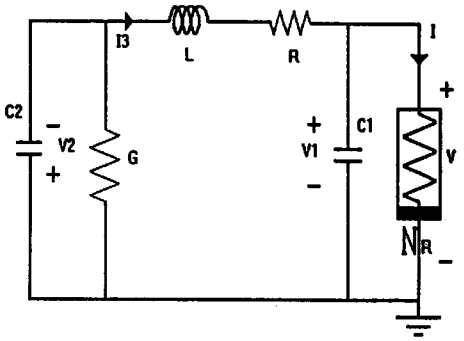
그림 1. Chua 회로와 구분 선형 함수
Fig. 1. Chua's circuit and piecewise linear function.

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.

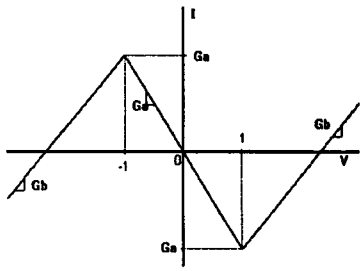
본 논문에서는 Canonical Chua 회로에서 Pecora와 Carroll[10]이 제시한 구동 동기 이론을 적용하여 RLCG 전송선로를 구성하고 카오스 동기화 방법 및 카오스 암호 통신 방법을 제안하였다.

2. Canonical Chua 회로

Canonical Chua 회로는 Chua 회로를 일반화하기 위해 구성한 회로로 그림 2와같이 나타낼 수 있다.



(a) Canonical Chua 회로



(b) 구분 선형 함수

그림 2. Canonical Chua 회로
Fig. 2. Canonical Chua circuit.

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

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

$$\frac{di_3}{dt}=-\frac{1}{L}[v_1+v_2+Ri_3] \qquad (2)$$

여기서

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

3. 구동 동기 이론

Pecora와 Carroll[10]에 의해 제시된 구동 동기 이론은 동기될 한 쌍의 카오스 회로에서 첫번째 카오스 회로를 구동 시스템(drive system)이라 하고 두 번째 카오스 회로를 응답 시스템(response system)이라 한다면 구동 시스템 상태 변수중 몇 개의 상태 변수만을 반응 시스템으로 전송하면 전송된 몇 개의 상태 변수들에 의해 전송되지 않은 나머지 상태 변수들로 응답 시스템에서 나타남으로써 구동 동기를 이루는 방법이다. 구동 동기 이론에 의한 동기화 결과는 반응 시스템의 Conditional Lyapunove exponent가 모두 음수일때 동기화가 이루어진 것으로 본다.

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

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

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

$$\frac{di_3}{dt}=-\frac{1}{L}[v_1+v_2+Ri_3] \qquad (3)$$

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

$$\frac{di_3'}{dt}=-\frac{1}{L}[v_1'+v_2'+Ri_3'] \qquad (4)$$

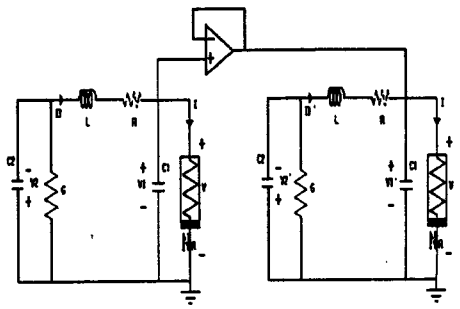


그림 3. Canonical Chua 회로의 X구동 동기화 회로
Fig. 3. X drive synchronization circuit of canonical Chua circuit.

4. 전송 시스템

그림 4에 RLCG 전송선로를 가진 Canonical Chua 회로의 암호화 통신을 나타내었다.

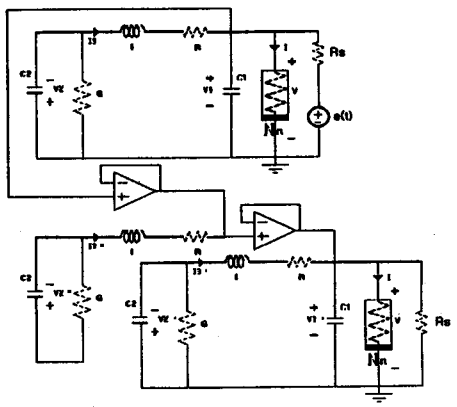


그림 4. Canonical Chua 회로의 암호화 통신 시스템
Fig. 4. Secure communication system which utilizes canonical Chua's circuit.

그림 4의 상태방정식을 다음과 같이 정리할 수 있다.

전송시스템의 상태방정식

$$C_1\frac{dv_1}{dt}=-g(v_1)+i_L+\frac{e(t)-v_1}{Rs}$$

$$C_2\frac{dv_2}{dt}=-Gv_2+i_L$$

$$L\frac{di_L}{dt}=-(v_1+v_2+R_0 i_L) \qquad (5)$$

정보 신호로써 전압원 e(t)를 사용하였고 전송 신호로써 $v_1(t)$를 사용하였다. 즉 $v_1(t)$는 카오스 신호로 변조된 전송 신호이다.

여기서 votage buffer를 사용하므로 $v_1 = v_1'$이다.

응답 시스템의 상태방정식

$$C_1\frac{dv_1'}{dt} = -g(v_1') + i_L' + \frac{e(t)-v_1'}{Rs}$$

$$C_2\frac{dv_2'}{dt} = -Gv_2' + i_L'$$

$$L\frac{di_L'}{dt} = -(v_1' + v_2' + R_0 i_L') \quad (6)$$

RLCG 전송 신호의 상태방정식

$$C_2\frac{dv_2''}{dt} = -Gv_2'' + i_L''$$

$$L\frac{di_L''}{dt} = -(v_1'' + v_2'' + R_0 i_L'') \quad (7)$$

(5)식으로 부터 정보 신호 e(t)는 다음과 같이 얻을 수 있다.

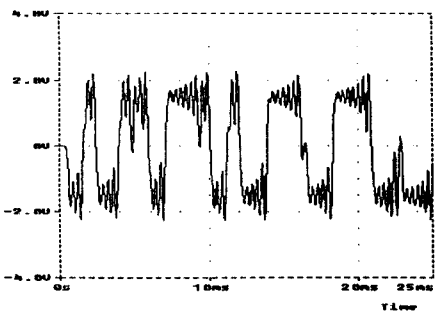
$$e(t) = Rs[C_1\frac{dv_1}{dt} + g(v_1) - i_L + \frac{v_1}{Rs}] \quad (8)$$

그림 4의 전류 j(t)는 다른 관계식으로 부터 구할 수 있다.

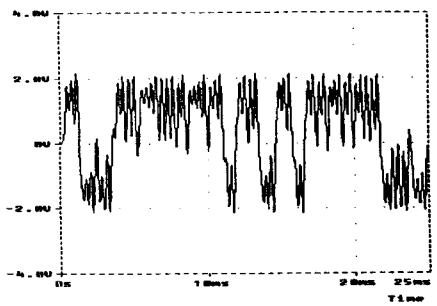
$$j(t) = \frac{e(t)}{Rs} = [C_1\frac{dv_1'}{dt} + g(v_1') - i_L' + \frac{v_1'}{Rs}] \quad (9)$$

5. 시뮬레이션 및 결과 검토

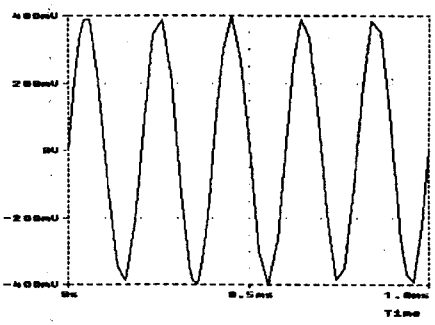
RLCG 전송 선로를 가진 Canonical Chua 회로의 암호화 통신을 위해 그림4의 회로를 이용하여 컴퓨터 시뮬레이션을 수행하였다. 시뮬레이션은 PSpice로 행하였으며 암호화 통신의 결과는 그림 5와 같다.



(a) 정보 신호가 없을 때의 전송 카오스 신호



(b) 정보 신호가 있을 때의 전송 카오스 신호



(c) 정보 신호

그림 5. 암호화 통신 결과
Fig. 5. The result of secure communication.

6. 결론

RLCG 전송 선로를 가진 canonical Chua 회로에서 구동 동기 개념을 이용한 동기화 방법 및 카오스 암호화 방법을 제안하였다. 컴퓨터 시뮬레이션 결과 카오스 암호화 통신이 정확하게 이루어짐을 알 수 있다.

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