손실 전송 선로를 가진 Chua 회로에서의 카오스 암호화 통신에 관한 연구

A Study on Chaotic Secure Communication of Chua's Circuit with Lossy Transmission Line

배 영 철 Young Chul Bae
Department of Electrical Engineering Yosu University

요 약

본 논문에서는 RLCG 전송선로를 가진 Chua 회로에서의 카오스 동기화 방법 및 암호화 통신 방법에 대하여 연구하였다. 두 개의 동일한 Chua 회로에 전송 선로를 두어 RLCG 전송로를 구성한 후 송신부와 전송선로 사이는 구동-결합 동기 이론을, 전송선로와 수신부 사이는 결합 동기 이론을 적용한 동기화 방법을 제시하였으며, 이 동기화된 회로에 암호 통신방법을 적용하여 송신부에서 가산기에 의한 정보 신호와 카오스 신호를 합성하고 수신부에서 정보 신호와 카오스 신호를 분리하는 복조 방법을 제시하였으며, 선로 중간에서 정보 신호를 도청한 것과 수신부에서 복원된 신호를 비교하여 암호화 통신의 성능을 검증하였다.

Abstract

In this paper, a transmitter and a receiver using two identical Chua's circuits are proposed and a wire secure communications are investigated.

A secure communication method in which the desired information signal is synthesized with the chaos signal created by the Chua's circuit is proposed and information signal is demodulated also using the Chua's circuit.

The proposed method is synthesizing the desired information with the chaos circuit by adding the information signal to the chaos signal in the wire transmission system.

After transmitting the synthesized signal through the wire transmission system, it is confirmed the feasibility of the secure communication from result of demodulated signals and recovered wire tapped signals.

Ⅰ. 서 론

최근에 카오스 현상에 대한 관심이 물리학, 화학, 생물학, 의학 및 공학 등에서 높아지고 있으며 이에 대한 응용이 활발하게 진행되고 있다.[1 5] 또한 간단한 전기 및 전자 회로를 구성하여 카오스를 생성하는 논문이 다수 발표되고 있으며[6 8] 이를 대표하는 것으로 Chua 회로를 들 수 있다.[9 10]

Chua 회로는 매우 단순한 자율 3차계 시스템으로 가역적(reciprocal)이며 1개의 비선형 소자인 3구분 선형 저항(3-segment piecewise-linear resistor)과 4개의 선형 소자 (R, L, C_1, C_2)로 구성되는 발진 회로이다.

카오스 암호화 통신을 위해서는 카오스 동기화가 선행되어야 하며 Chua 회로를 이용하여 카오스 동기화를 구현하고자 하는 노력이 계속되고 있으며 몇몇 관심있는 발표도 나오고 있다.[11 14]

카오스 동기화 방법은 결합 동기 이론[13], 구동 동기 이론[11]이 제시되어 있으나 결합 동기의 경우 단순히 결합 저항을 연결하여 동기화를 이루며 구동 동기 이론은 구동부(송신부)와 응답부(수신부)가 안정하지 않으면 구동이 되지 않고 실제 전송 선로에 적용하기 어려운 문제점이 있으며 암호화 통신 연구로는 카오스 신호에 정보 신호를 합성하는 방법이 제시되어 있으나 이는 정보 신호가 카오스 신호에 비하여 매우 작아야하며, 전송 선로의 영향을 고려하지 못하는 단점이 있다.

이에 본 논문에서는 유선 선로의 동기화 및 암호화 통신에 쉽게 적용할 수 있는 RLCG 전송 선로를 가진 회로의 동기화 방법을 구동-결합 동기와 결합 동기 방식을 써서 새로이 제시하고 Pspice로 구현해 보였다.

본 논문에서는 RLCG 전송 선로를 대상으로 가산기를 이용하여 정보 신호와 카오스 신호를 합성하였으며 통신 신호에서 정보 신호와 카오스 신호를 분리하는 복조 방법을 제시하였다.

Ⅱ. Chua 회로

저항, 콘덴서, 인덕터로 구성된 자율회로(autonomous circuit)가 카오스 현상을 나타내기 위해서는 적어도 하나의 비선형소자와 하나의 국소적 능동(locally active) 저항 및 3개의 에너지 저장 소자를 가져야한다.[9] Chua 회로는 이 조건을 만족하는 가장 간단한 회로이다.

Chua 회로는 매우 단순한 자율, 3차계 시스템으로 가역성(reciprocal)의 성질을 가지며 1개의 비선형 소자인 3구분 선형 저항(3-segment piecewise-linear resistor) 과 4개의 선형소자 (R, L, C_1, C_2)로 구성되는 발진회로이다.

Matsumoto에 의해 제안된 Chua 회로[9]를 그림1에 나타냈으며 상태방정식은 식 (1)과 같이 표현할 수 있다.

그림 1. Chua 회로 (Chua's circuit)

$$C_1\frac{dv_{c_1}}{dt} = G(v_{c_2} - v_{c_1}) - g(v_R)$$

$$C_2\frac{dv_{c_2}}{dt} = G(v_{c_1} - v_{c_2}) + i_L \tag{1}$$

$$L\frac{di_L}{dt} = -v_{c_2}$$

여기서 v_{c_1}, v_{c_2}는 각각 콘덴서 C_1, C_2의 양단 전압, i_L은 인덕터 L에 흐르는 전류, $G=\frac{1}{R}$, g(·)는 비선형 저항으로써 식 2와 같이 표현되는 3구분 선형 함수(3-segment piecewise-linear function)이며 그림 2에 나타내었다.

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

여기서 m_0는 외부 영역의 기울기, m_1은 내부 영역의 기울기, $\pm B_p$는 break-point이다.

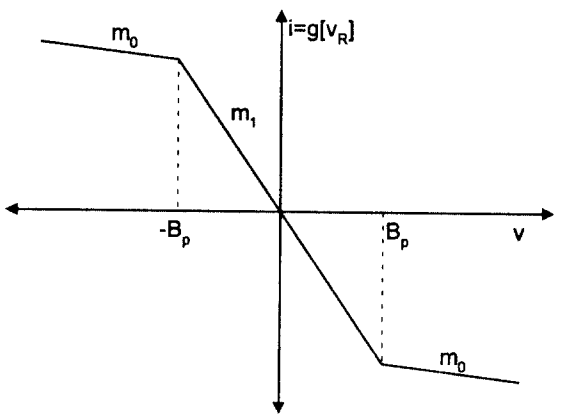
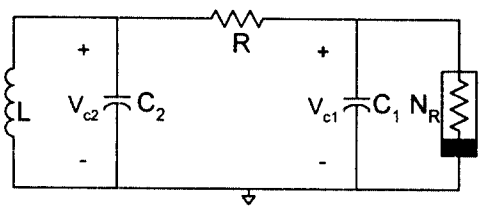


그림 2. 비선형 저항 특성 (Nonlinear resistor characteristic)

Ⅲ RLCG 전송선로의 카오스 암호화 통신



카오스 신호에 정보 신호를 합성하여 송신하는 카오스 암호화 통신은 복조가 어려워 높은 보안성을 유지할 수 있어서 그 필요성이 증대되고 있다[3]. 이것은 송신부에서 잡음과 같은 불규칙한 카오스 신호에 정보 신호를 실

어서 보내고 수신부에서 정보 신호를 분리하는 통신 방법이다. 정보신호가 카오스 신호보다 월등히 큰 경우가 아니면 통신 신호는 카오스 신호가 주류를 이룰 것이며 일반적인 필터링이나 복조 방법으로 정보 신호 분리가 불가능 하므로 수준 높은 암호화 통신 수단이 될 수 있다.

이러한 암호화 통신 연구로 카오스 신호에 정보 신호를 합성하는 방법[45]이 제시되었으나 정현파 정보 신호를 인가하고 있어서 특정 주파수 특성에 한정되어 있으며 정보신호가 카오스 신호에 비하여 너무 작고 전송선로의 영향을 고려하지 않고 있어서 활용화에 미흡한 감이 있다.

분포정수를 가진 유선 선로의 통신에서의 카오스 암호화 통신 회로를 그림 3에 나타내었다. 송신부에서 카오스 신호와 정보 신호의 합성은 가산기를 이용하였으며 선로 중간에 신호 도청을 가정하고 이로 인한 수신 신호의 크기를 보상하기 위한 증폭 회로로 구성하였다. 송신부와 RLCG 전송선로는 구동-결합 동기 방법을, RLCG 전송선로와 수신부는 결합 동기 방법을 써서 동기화를 이루었으며 수신부에서 결합 저항과 병렬로 콘덴서를 연결하여 불필요 신호를 제거하는 회로를 구성하였다.

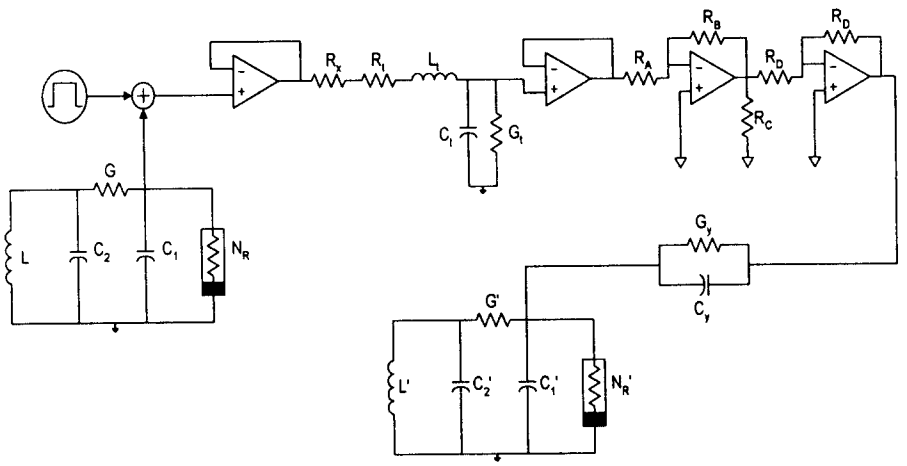


그림 3. 유선 선로의 카오스 암호화 통신 회로
(Chaos secure communication circuit with wire transmission line)

그림 3 회로의 상태 방정식은 다음과 같다.

송신부의 상태 방정식

$$C_1\frac{dv_{c_1}}{dt} = G(v_{c_2} - v_{c_1}) - g(v_{c_1})$$

$$C_2\frac{dv_{c_2}}{dt} = G(v_{c_1} - v_{c_2}) + i_L \qquad (3)$$

$$L\frac{di_L}{dt} = -v_{c_2}$$

RLCG 전송선로의 상태방정식

$$L_t\frac{di_{L_t}}{dt}=v_{c_1}-(R_t+R_x)i_{L_t}-v_{c_t}+S(t)$$

$$C_t\frac{dv_{c_t}}{dt}=i_{L_t}-(G_0+G_t)v_{c_t} \tag{4}$$

증폭부 및 결합 저항부의 상태방정식

$$C_y\frac{dv_{c_y}}{dt}=-\frac{R_B}{R_AR_D}v_{c_t}-G_yv_{c_y}$$

$$C_1\frac{dv_{c_1}'}{dt}=G(v_{c_2}'-v_{c_1}')-g(v_{c_1}')-\frac{R_B}{R_AR_D}v_{c_t} \tag{5}$$

수신부의 상태방정식

$$C_1'\frac{dv_{c_1}'}{dt}=G'(v_{c_2}'-v_{c_1}')-g(v_{c_1}')+G_y(v_{c_t}-v_{c_1}')$$

$$C_2'\frac{dv_{c_2}'}{dt}=G'(v_{c_1}'-v_{c_2}')+i_L' \tag{6}$$

$$L'\frac{di_L'}{dt}=-v_{c_2}'$$

$v_x=v_{c_1}-v_{c_1}'$, $v_y=v_{c_2}-v_{c_2}'$, $i_z=i_L-i_L'$라 정의하고 식(3), 식(4), 식(5), 식(6)에서 차 시스템(Difference System)을 구하면 식(7)과 같이 5차 시스템으로 정리 할 수 있다.

$$C_1\frac{dv_x}{dt}=G(v_y-v_x)-S_iv_x+G_y(v_{c_1}'-v_{c_t})$$

$$C_2\frac{dv_y}{dt}=G(v_x-v_y)+i_z$$

$$L\frac{di_z}{dt}=-v_y \tag{7}$$

$$C_t\frac{dv_{c_t}}{dt}=i_{L_t}+(G_0+G_t)v_{c_t}$$

$$L_t\frac{di_{L_t}}{dt}=v_{c_1}-v_{c_t}-(R_x+R_t)i_{L_t}+S(t)$$

식(7)에서 차 시스템은 시간이 지남에 따라 0으로 수렴해가는,

즉 $\lim_{t\to\infty}|v_x|=\lim_{t\to\infty}|v_y|=\lim_{t\to\infty}|i_z|=0$가 되면 동기화가 이루어지는 것이다.

식 (7)을 상태방정식 꼴로 고치고

$$\frac{dv_x}{dt} = -\frac{(G+S_i)}{C_1} v_x + \frac{G}{C_1} v_y + \frac{G_y}{C_1}(v_{c_1}' - v_{c_t})$$

$$\frac{dv_y}{dt} = \frac{G}{C_2} v_x - \frac{G}{C_2} v_y + \frac{1}{C_2} i_z$$

$$\frac{di_z}{dt} = -\frac{1}{L} v_y \tag{8}$$

$$\frac{dv_{c_t}}{dt} = \frac{(G_0+G_t)}{C_t} v_{c_t} + \frac{1}{C_t} i_{L_t}$$

$$\frac{di_{L_t}}{dt} = -\frac{R_t+R_x}{L_t} i_{L_t} + \frac{1}{L_t}(v_{c_1} - v_{c_t}) + \frac{1}{L_t} S(t)$$

간략화하기 위해 $x_1 = v_x$, $x_2 = v_y$, $x_3 = i_z$, $x_4 = v_{c_t}$, $x_5 = i_{L_t}$, $u = v_{c_t}' - v_{c_t}$
$= v_{c_1} - v_{c_t}$라 놓고 정리하면 식(9)와 같이 된다.

$$\dot{x}_1 = -\frac{(G+S_i)}{C_1} x_1 + \frac{G}{C_1} x_2 + \frac{G_y}{C_1} u$$

$$\dot{x}_2 = \frac{G}{C_2} x_1 - \frac{G}{C_2} x_2 + \frac{1}{C_2} x_3$$

$$\dot{x}_3 = -\frac{1}{L} x_2 \tag{9}$$

$$\dot{x}_4 = \frac{(G_t+G_0)}{C_t} x_4 + \frac{1}{C_t} x_5$$

$$\dot{x}_5 = -\frac{R_t+R_x}{L_t} x_5 + \frac{1}{L_t} u + \frac{1}{L_t} S(t)$$

이를 행렬로 나타내면 식(10)과 같다.

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \\ \dot{x}_5 \end{bmatrix} = \begin{bmatrix} -\frac{(G+S_i)}{C_1} & \frac{G}{C_1} & 0 & 0 & 0 \\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} & 0 & 0 \\ 0 & -\frac{1}{L} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{G_0+G_t}{C_t} & \frac{1}{C_t} \\ 0 & 0 & 0 & 0 & \frac{-R_t+R_x+1}{L_t} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} \frac{G_y}{C_1} \\ 0 \\ 0 \\ 0 \\ \frac{1}{L_t} \end{bmatrix} u \tag{10}$$

식 (10)에 L, $L' = 18\,mH$ $R_x = 780\,\Omega$ $C_t = 0.062\mu F$

C_1, $C_1' = 10\,mH$ $G_y = 0.01\,\Omega$ $G_t = 1.5\,\mu\mho$

C_2, $C_2' = 100\,mH$ $R_t = 89.7\,\Omega$

R, $R'=1.74K\Omega$ $L_t=0.04H$ 로 놓고 식(10)의 시스템이 안정하기 위한 조건의 값 $R_x=780[\Omega]$, $G_y=0.005[\mho]$, $C_y=1[\mu F]$으로 구하였으며 정보 신호로는 크기 -400[mV] ~ +400[mV], 주기 5[ms]의 구형파를 인가하여 암호화 통신 상태를 비교하였다.

반송파인 송신부의 v_{c_1} 전압 파형을 그림 4에 나타내었으며

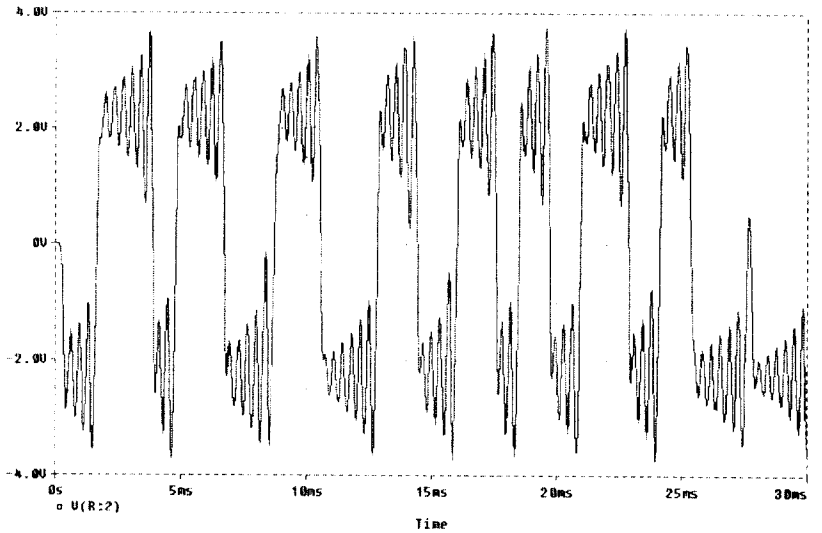


그림 4. 반송파 신호(송신부 신호) {Carrier signal (transmitter signal)}

수신부에서 동기화된 v_{c_1}'의 전압 파형을 그림 5에 나타내었다.

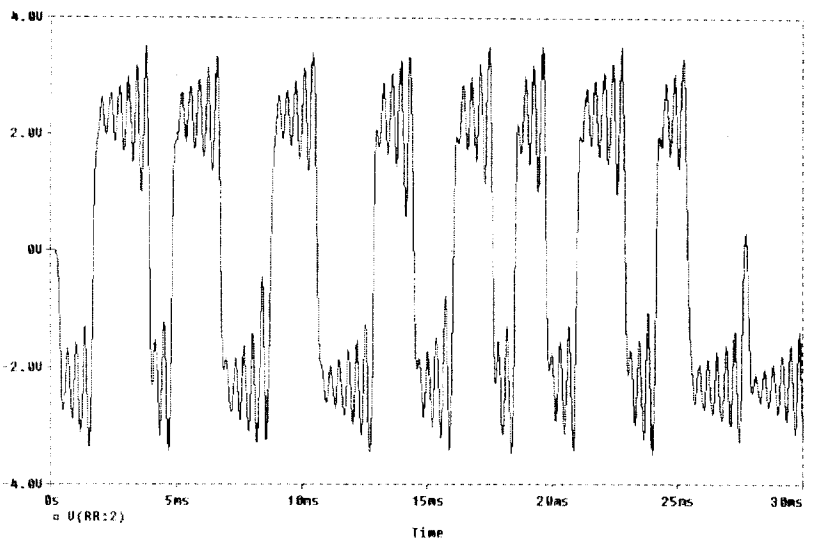


그림 5. 수신부의 카오스 신호 (Chaos signal of receiver signal)

그림 4와 5에서 송신 신호와 수신 신호가 같은 형태를 이루고 있어서 동기화 현상이 이루어짐을 알 수 있다.
도청을 가정하여 선로 중간에서 측정한 신호를 그림 6에 나타내었으며 구형파인 정보 신호와 월등히 다른 모양을 보이고 있어서 도청의 의미가 없음을 알 수 있다.

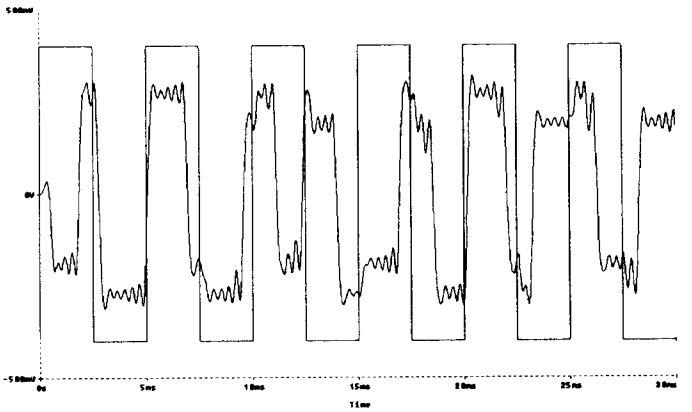


그림 6. 선로 중간에서 도청한 신호 (Wiretapping signal)

그림 7에 수신단의 결합 저항에 흐르는 전류 신호의 검출에 의해 복조한 결과를 나타내었다. 복조된 신호는 필터링을 하기 전의 신호로 전송선로 특성에 의한 잡음이 있으며 어느 정도 구형파에 가까운 신호를 복원되었음을 알 수 있다.

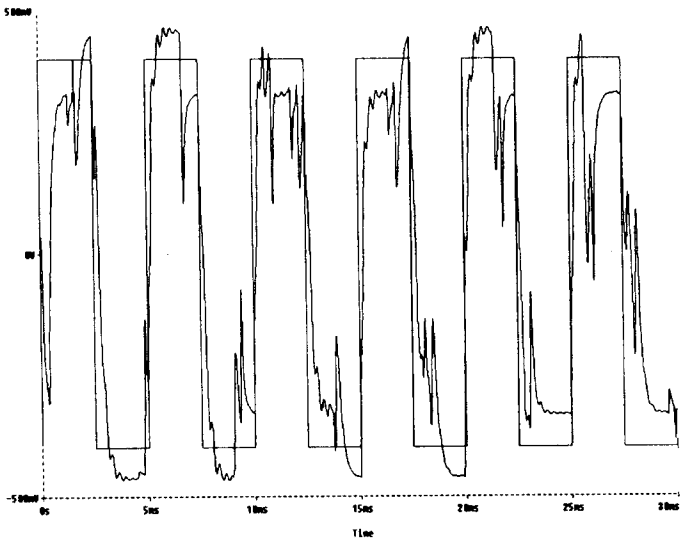


그림 7. 필터링하기 전의 복원 신호 (Recovery signal before filtering)

그림 7의 신호를 3[kHz]의 차단 주파수를 가진 저역 통과 필터를 이용하여 필터링한 결과를 그림 8에 나타내었다. 필터링 결과 구형파 형태로 어느 정도 복원 할 수 있었으나 전송선로의 L, C에 의한 동기화의 영향 때문에 복조 성능이 우수하지 않음을 알 수 있다.

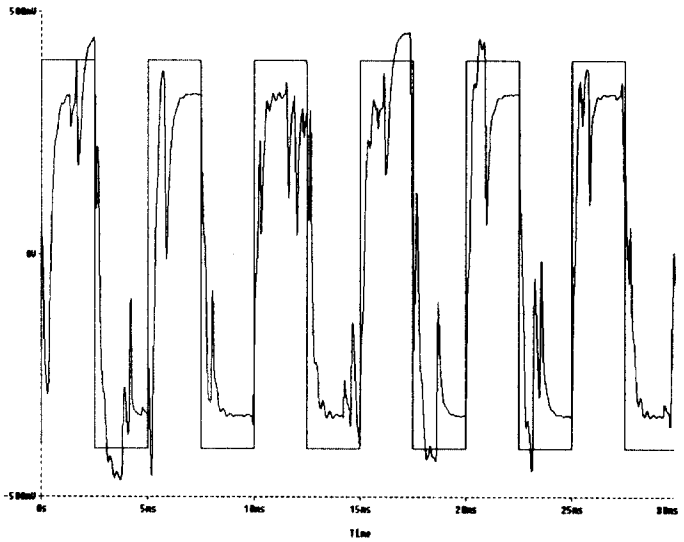


그림 8. 필터링한 후의 복원 신호 (Filtered recovery signal)

그림 8에서 보는 바와 같이 RLCG 전송 선로를 이용한 카오스 암호 통신은 전송선로의 L, C에 의한 시간 지연이 있는 동기화 때문에 수신단에서 완전한 정보 신호를 복원할 수 없었으나 신호의 크기와 주파수 제한을 둔 디지털 정보 신호의 암호화 통신에 충분히 적용할 수 있겠다.

Ⅳ. 결 론

본 논문에서는 전송선로를 가진 Chua 회로에서의 카오스 암호화 방법에 대하여 연구하였다. 두 개의 동일한 Chua 회로에 전송 선로를 두어 RLCG 전송로를 구성한 후 송신부와 전송선로부 사이는 구동-결합 동기 이론을 전송선로와 수신부 사이는 결합 동기 이론을 적용한 동기화 방법을 제시하였으며, 송신부에서 가산기를 이용하여 정보 신호와 카오스 신호를 합성하고 수신부에서 이들 신호를 분리하는 암호화 통신을 행하였다. 앞으로 디지털 방식에 의한 동기화와 전송 선로 정수에 의한 암호화 통신의 질적인 향상이 과제로 남는다.

참 고 문 헌

1. 배영철, " 카오스의 응용" 전자저널, pp.110-112. 1993.1.20.
2. 배영철, 임화영, "주기적 외력을 인가한 Bonhoeffer-Van der Pol 오실레이터 모델에서의 카오스 현상 해석에 관한 연구 " 한국통신학회논문지, 20권 11호, pp. 2991 - 3000, 1995.
3. T. S. Parker and L. O. Chua, " Chaos: A Tutorial for Enginees" Proc. IEEE, vol. 75, no. 8, pp. 982-1008. 1987.
4. 合原一幸, "바이오 카오스 정보와 그 공학적 응용" 電子工業月報, 제34권, 1호, pp. 30-39, 1993.
5. 제임스 글레리크 "CHAOS: Making A New Science" 동문사.
6. M. Kuramitsu and K. I. Mori, "A simple Electric Circuit Generating chaos" Technical Report IEICE, NLP 93 - 68, pp. 31-38, 1994.
7. Y. Ueda and N. Akamatsu, "Chaotically Transitional phenomena, in the Forced Negative-Resistance Oscillator" IEEE Trans. Circuit and Systems, vol. CAS-28, pp. 217 - 224, 1981.
8. 고재호, 배영철, 임화영, "주기적 외력을 인가한 Bonhoeffer - Van der Pol 오실레이터 모델에서의 카오스 현상 해석에 관한 연구", 1995 제어계측연구회 학술발표회 논문집, pp. 100 - 102, 1995.
9. T. Matsumoto, "A chaotic attractor from Chua's circuit" IEEE Trans. Circuits and Systems, vol. CAS-31, no. 12, pp. 1055-1058, 1984.
10. G. O. Zhong and F. Ayrom, "Experimental confirmation of chaos from Chua's circuit", Int. J. Circuit Theory and Applications, vol. 13, no. 1, pp. 93-98, 1985.
11. L. M. Pecora and T. L. Carroll "Synchronization in Chaotic System" Phy. Rev. Lett., vol. 64, no. 8, pp. 821-824, 1990.
12. 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.
13. L. O. Chua, M. Itoh, L. Kocarev, and K. Eckert, "Chaos Synchronization in Chua's Circuit" J. Circuit. Systems and Computers, vol. 3, no. 1, pp. 93-108, 1993.
14. R. He, P. G. Vaidya, " Analysis and Synthesis of Synchronous Periodic and Chaotic Systems" Phys. Rev. A, vol. 6, no. 12. pp. 7387-7392. 1992.
15. L. Kocarev, U. Parlitz. "Generized Synchronization, Predictability, and Equivalence of Unidirectionally Coupled Dynamical System" Phys. Rev. Lett. vol. 76, no. 11, pp. 1816-1819, 1996.