전자기술연구지, 경북대 공대, vol. 16-2, 1995.

카오스 동기화를 이용한 비화통신

이 익 수*, 정 호 선**

Secure Communication Using Chaos Synchronization

Ik-Soo Lee and Ho-Sun Chung

Abstract In this paper, chaotic synchronization in chaotic neural network and its possible application to secure communication are discussed. Toshimitsu Ushio has recently shown that it is possible to synchronize one-dimensional chaotic neural networks with uni-directional connection using feedback control. Thus we designed chaotic synchronization with three neurons connection using successive and simultaneous synchronization. These chaotic synchronization concepts are useful for applying to speech private communication system. In the experiment, we demonstrated the mutual chaotic synchronization and speech signal modulation and recovery in the spread-spectrum communication.

I. 서 론

자연계에서의 카오스 현상은 일반적이며 비선형시스템에서 널리 보인다. 카오스 시스템은 초기값에 매우 민감한 특성을 보이고, 전형적으로 카오스 끌개(chaotic attractor)는 불안정 주기궤도를 무한대로 순환하는 형태로 위상공간에 표현된다. 이러한 카오스의 현상은 바람직하지 않으며 제어하기 곤란한 문제로 간주했으나, 최근 카오스 신호를 제어하려는 시도가 수학, 물리학, 공학, 생체공학 등의 여러 분야에 시도되고 있다[1,2].

카오스적 불규칙적인 운동을 서로 동기화시키는 카오스 동기화(chaos synchronization)는 실질적으로 중요한 문제이며, 전송시스템에 응용이 가능하다고 보고되고 있다. Pecora와 Carroll[3] 은 동일한 카오스 시스템 S_1, S_2를 구성한 후에 S_2와 동일하며 리아푸노프(Lyapunov) 지수가 음이 되는 안정한 부시스템 S_2' 을 구성하여 S_2'에 S_1의 입력을 가하면 동기화가 되는 것을 보였다. 그러나 Pecora와 Carroll의 방법은 고차원 시스템에 적용을 하여야 하며, 부시스템에 다른 연결이 있는 동기화 시스템에는 적용할 수 없는 단점이 있다.

Ott, Grebogi, Yorke 등은 불안정 주기궤도를 작은 제어입력에 의해 안정한 주기궤도로 제어하는 OGY[4] 방법을 제안하였다. 그러나 OGY 방법은 카오스 시스템에서의 안정한 궤도를 찾아내어 제어상태를 계속적인 피드백의 계산적 입력를 가해야 한다는 단점이 있다. Metha와 Lai[5]는 OGY 방법을 수정하여 동기화를 행했다. 동특성이 같은 두개의 부시스템을 제어하지 않으면 독립적으로 동작하지만 제어입력을 가하면 제어입력이 있는 시스템에 추종하도록 하는 동기화가 행해진다. Metha와 Lai는 각 부시스템은 일차원 이산시간으로 이루어지며 일정하게 연결된 복수개의 부시스템의 상태를 동기화 시키도록 하는 피드백 구성법을 제안하였다. 또한 Pyragas[6]는 연속적인 피드백 제어를 통하여 카오스 시스템의 동기화를 행했다.

1995년 7월 1일 접수
* 경북대학교 대학원 전자공학과 박사과정
** 경북대학교 공과대학 전자공학과 교수

본 연구에서는 한방향(uni-directional)으로 연결이 있는 일차원적인 카오스 동기화를 행한 Toshimitsu Ushio[7]의 방법을 도입하여 카오스 동기화를 행한다. 일차원 시스템은 카오스신경망(chaotic neural network)을 대상으로 하여 뉴론과 뉴론간의 순방향 및 지역적 역방향(local backword)의 연결을 갖는 3개의 뉴론을 동기화 시키는 실험을 행했다. 첫번째로 국소적인 피드백으로 순차적 동기화 방향이 한방향으로 진행되는 축차동기(successive synchronization)를 행했으며, 두번째로 준국소적인 피드백으로 임의의 뉴론을 동시동기화(simultaneous synchronization)를 행하는 실험을 행했다. 마지막으로 이러한 카오스 시스템의 동기화를 이용하여 음성신호의 비밀통화에 적용하여 신호의 변조 및 복조 등의 유용한 가능성에 대해 기술한다.

II. 카오스신경회로망

오징어 거대축색에 자극을 가한 후에 막전위를 측정한 결과를 보면, 외부적으로 자극을 가하지 않을 때는 자발적으로 주기적 응답을 일으키고, 자극을 가함에 따라 준주기(quasi-periodic) 또는 주기분배(bifurcation) 과정에 의한 복잡한 카오스 응답을 보인다. 이러한 뉴론의 카오스 응답특성을 나타내도록 모델링한 카오스 뉴론모델(chaotic neuron model)은 다음의 식 (1)과 (2)와 같이 차분방정식으로 나타내어진다[8].

$$x(t+1)=f\left[A(t)-\alpha\sum_{r=0}^{n}k^{r}g(x(t-r))-\theta\right] \quad (1)$$

$$f(y)=\frac{1}{1+\exp(-y/\varepsilon)} \quad (2)$$

여기서 각 변수는 다음과 같이 정의된다.

x(t+1) : 이산 시간 t+1에서의 뉴론의 출력
f(t) : 기울기 ε을 갖는 뉴론의 출력함수
A(t) : 이산 시간에의 외부 입력자극의 크기
g : 뉴론내부에서의 불응성 크기와 관계함수
k : 불응성 감쇠상수, $0 \le k \le 1$
α : 불응성 함수의 크기 상수, $\alpha > 0$
θ : 뉴론 내부의 역치값

식 (1)에서 뉴론의 내부상태를 y(t+1)라 정의하면 식 (3)과 같이되며, 't'의 상태와 k배한 후 't-1'의 상태를 대입한 후, 두식의 차를 구하여 차분방정식을 정리하면 식 (4)와 같이 된다.

$$x(t+1) = f[y(t+1)] \quad (3)$$

$$y(t+1) = k\,y(t)-\alpha f\{y(t)\}+a(t) \quad (4)$$

단, $a(t)=A(t)-kA(t-1)-\theta(1-k)$

결론적으로 식 (4)를 살펴보면 이산적인 카오스 뉴론모델의 내부특성 y(t+1)은 선형적인 항 ky(t), 비선형적인 항 αf{y(t)} 및 외부입력 a(t)의 합으로 이루어진다. 선형적인 항은 각 뉴론의 이전 카오스 뉴론의 내부상태 y(t)에 뉴론의 불응성적인 영향을 반영하는 k의 곱으로 이루어진다. 그리고 비선형적인 항은 불응성 함수의 크기를 결정하는 변수 α와 뉴론의 연속적인 출력함수(sigmoid output function)의 f{y(t)} 항의 곱으로 이루어진다. 외부입력 a(t)는 다른 뉴론의 출력으로부터 목표 뉴론으로의 외부 입력의 총합이 된다. 그림 1은 카오스 신경망에서 변수들을 k=0.8, α=1, ε=0.1의 값에서 내부적 상태를 도시한 것이다. 외부입력 a(t)의 변화에 따라 주기, 주기분배, 카오스 응답 등의 다양한 동적응답을 나타낸 것이다[9].

본 연구에서는 이산시간(discrete-time) 카오스신경망이 한방향으로 직렬로 연결된 형태의 결합을 구성한다. 그림 2에 보이는 것과 같이 카오스 뉴론은 3개로 정했으며, 신호의 흐름이 단일방향이며 동기화를 목적으로 제어입력 u(t)가 존재한다. 또한 뉴론간의 연결은 가중치 W를 두어 구성한다. 뉴론의 갯수를 N

이라고 하고, 시간 t에 있어서의 뉴론 i의 내부상태 $y_i(t)$는 아래의 방정식으로 기술된다.

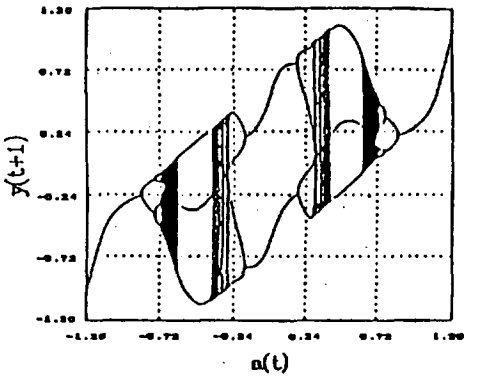

그림 1. 내부상태 분기도

Fig. 1. The bifurcation diagram of internal state.

$$y_1(t+1) = k y_1(t) - a x_1(t) + a(t) + u_1(t) \quad (5)$$

$$y_i(t+1) = k y_i(t) - (a+W) x_i(t) + W x_{i-1}(t) + a(t) + u_i(t) \quad (6)$$

where i = 2, 3, 4, • • •, N

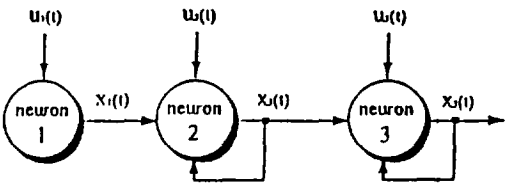

그림 2. 카오스 뉴론의 연결

Fig. 2. The connection of chaotic neurons.

Ⅲ. 카오스 동기화 현상

1. 축차동기화 제어법칙

축차동기화(逐次同期化)[7] 제어는 뉴론 p에서 q까지의 상태를 연속적으로 카오스 동기화 시키도록 하는 제어법칙을 말한다. 여기서, $1 \le p < q \le N$ 이다. 다음에 피드백 제어입력 $u_i(t)$는 다음과 같다[10].

$$u_i(t) = \begin{cases} (W+a)\{x_i(t) - x_{i-1}(t)\}, & \text{if } 1 < p < i < q \\ W\{x_i(t) - x_{i-1}(t)\}, & \text{if } 1 < p = i \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

식 (7)을 이용하여 제어입력을 가하면 뉴론 p에서 연속적으로 축차동기화가 이루어지고 최후의 뉴론 q가 p에 대하여 카오스 동기화가 된다. 이러한 제어법칙을 축차동기화 제어법칙이라 부르기로 한다. 그림 3은 뉴론 1, 뉴론 2, 뉴론 3을 축차 동기화 제어를 했을 때의 상태를 도시한 것이다. 과도기적 비동기 상태를 보이나 결국에는 y_1의 신호에 y_2, y_3가 따라가게 되며, 이것은 카오스 동기화가 되었다는 것을 알 수 있다. 또한 축차 동기화 제어법칙은 동기화시키는 뉴론에 대해 그 뉴론과 그 전의 뉴론의 출력만으로 구성되므로 완전히 局所 피드백(local feedback)이 된다. 그러나 동기화시키는 뉴론의 갯수가 많을 때에는 동기화가 달성될 때까지 지연시간이 걸린다.

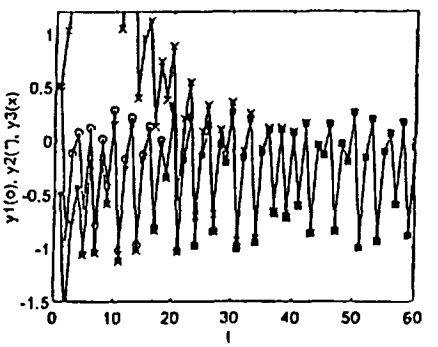

그림 3. 축차동기화

Fig. 3. The successive synchronization.

2. 동시동기화 제어법칙

동시동기화(同時同期化)[7] 제어는 n개의 특정뉴론 p1, p2, • • • , pn을 동기화시키는 제어법칙을 말한다. 단, $0 \le pj \le N$, $j \ne m$

이라면 pj ≠ pm 이다. 여기서 S={p1, p2 , … , pn}라고 두면 동기화시키는 뉴론은 연속적으로 연결되어 있을 필요는 전혀 없다. 이러한 형태는 축차동기화 제어방법과는 다르다. 피드백 $u_i(t)$의 제어입력은 다음과 같이 정의된다[10].

$$u_i(t)=\begin{cases}(W+\alpha)\{y_i(t)-y_{i-1}(t)\}+\\ \alpha\{y_{i-1}(t)-y_{pl}(t)\}, & \text{if } i\neq 1 \text{ and } i\in S\\ \alpha\{y_1(t)-y_{pl}(t)\}, & \text{if } i=1\in S\\ 0 & \text{otherwise}\end{cases} \quad (8)$$

식 (8)을 적용하여 일차원카오스 신경회로망에서 임의의 pj, pm ∈ S 에 대한 뉴론의 동기화가 행해진다. 따라서 이 제어법칙을 사용하면 동기화가 동시에 일어난다. 이러한 제어법칙을 동시동기화라 한다. 그림 4는 p1이 1이라 하고 뉴론 1에서 뉴론 3까지를 동기화 했을 때의 y_1, y_2, y_3의 시간 변화를 보인 것이다. 축차동기화 제어의 경우와 달리 동기되는 뉴론이 단시간 내에 동기화되는 것을 알 수 있다. 동시동기화 제어는 임의의 뉴론의 조합에 대해 단시간에 동기화가 달성되지만, 뉴론 p1의 출력을 필요로 하는 단점이 있다. 동기화시키고 싶은 뉴론으로 특정 뉴론을 선택할 수 있으나 준국소적인 피드백을 사용하므로 축차동기 제어에 비해 복잡하게 된다.

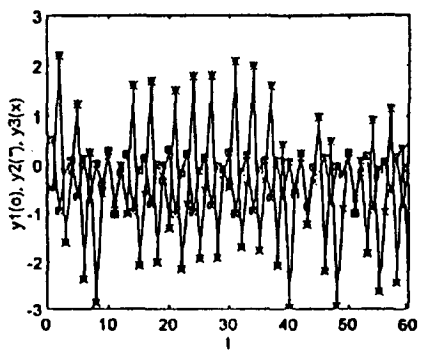

그림 4. 동시동기화
Fig. 4. The simultaneous synchronization.

IV. 음성비화 전송시스템에 응용

카오스 신호는 위상공간에서 장기간 예측이 불가능한 신호이므로 신호의 합성과 발생 등에 많은 유용성을 보여주고 있으며, 특히 카오스 동기화를 이용한 통신시스템에 응용이 될 수 있다는 것이 보고되고 있다. 카오스 변조(chaotic modulation)를 이용한 통신은 잡음억제능력, 광대역통신, 암호 및 비화통신 등의 응용성이 다양하다[11-13]. 본 연구에서는 앞절에서 실험한 카오스 동기화 현상을 기반으로 송·수신간의 비화통신시스템을 구성하여 음성신호를 재생하는 실험을 행했다.

위에서 살펴본 카오스 동기화를 이용하여 음성신호의 비화전송법을 살펴본다. 먼저 3개의 뉴론으로 이루어진 시스템을 생각한다. 카오스 동기화의 구성은 송신단, 교환기, 수신단의 세개의 블럭으로 나누어지며, 통신을 위한 각각의 블럭은 그림 5와 같으며 각 블럭의 카오스 동기화를 위한 수식은 다음과 같이된다.

$$\begin{aligned}y_1(t+1)=&\ ky_1(t)-ax_1(t)+a(t)\\ &+u_1(t)+s(t)\\ y_2(t+1)=&\ ky_2(t)-(W+\alpha)x_2(t)\\ &+Wx_1(t)+a(t)+u_2(t)\\ y_3(t+1)=&\ ky_3(t)-(W+\alpha)x_3(t)\\ &+Wx_2(t)+a(t)+u_3(t)\end{aligned} \quad (9)$$

여기서 s(t)는 송신측의 음성신호원이며 송신측에서의 카오스 신경망의 카오스 내부상태에 음성신호를 더하면 전송신호는 카오스적 잡음과 같이 된다. 송신측의 카오스 변조신호의 주파수 특성은 넓은 대역을 차지하므로 음성신호는 카오스 신호속에 묻혀 외부적으로 비화통신이 이루어진다.

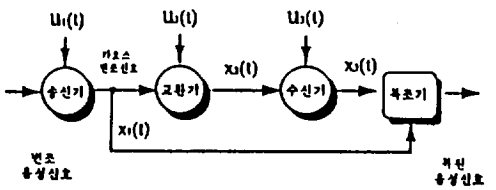

그림 5. 비화 통신시스템의 구성
Fig. 5. The block of secure communication.

축차동기화의 제어는 수신단과 교환기가 먼저 동기화를 이루며, 교환기가 동기화 되면 송신단을 동기시켜 송·수신단을 전체적으로 비화통신을 이룬다. 축차동기화 경우의 제어 입력은 다음과 같다.

$$\begin{aligned} u_1(t) &= 0 \\ u_2(t) &= (W+\alpha)\{x_2(t) - x_1(t)\} \\ u_3(t) &= (W+\alpha)\{x_3(t) - x_2(t)\} \end{aligned} \quad (10)$$

또한, 동시동기화 제어 경우의 구성을 보면 송신단과 교환기 또는 송신단과 수신단간의 동기화는 축차동기화와 같은 제어를 행하면 된다. 그러나 교환기를 거치지 않고 송신단과 원하는 수신단과의 비화통신을 위해서는 동시 동기화 제어가 필요하다. 송신단과 교환기는 비화통신이 이루어지지 않는다. 이러한 동시 동기화를 위한 제어입력은 다음과 같다.

$$\begin{aligned} u_1(t) &= 0 \\ u_2(t) &= 0 \\ u_3(t) &= (W+\alpha)\{x_3(t)-x_2(t)\} \\ &\quad +\alpha\{x_2 - x_{p1}\} \end{aligned} \quad (11)$$

그리고 송신측에서는 카오스 변조된 상태의 y(t)의 신호를 송신단에서 f{y1(t)}을 통하여 교환기 및 수신단의 입력으로 주어야 한다. 수신단에서 송신단의 신호를 다음의 수식과 같이 복조하면 s'(t) = s(t) 즉, 송.수신단간의 동기화가 되어 음성비화가 이루어 진다.

$$\begin{aligned} s(t) &= k\{y_2(t)-y_1(t)\} \\ &\quad -\{y_2(t+1)-y_1(t+1)\} \end{aligned} \quad (12)$$

s'(t)의 계산에 y1(t+1), y2(t+1)가 필요하게 되므로 이 값이 구해지는 것은 시각 t+1일 때이므로 복조는 한 클럭 후에 복조해 낸다. 그림 6은 동시동기화 제어의 경우에 s(t)가 음성신호일때의 송.수신간의 시간응답을 나타내었다. 전송신호 y1(t)는 카오스 및 음성신호가 섞여 있으므로 예측이 불가능한 카오스 상태이지만, 카오스 동기화를 구성하여 복호화한 신호를 보면 완전히 음성신호가 재생되고 있다는 것을 알 수 있다. 또한 송신측에서 구동하는 암호화된 신호(encoded masking signal)는 수신측에서 정확히 복구하려면 이산시간의 속도와 정보신호의 크기에 매우 독립적이므로 잘 선택하여야 한다. 본 실험결과를 보면 카오스 동기화 현상은 잡음신호에 매우 둔감하며, 주어진 제어입력을 가하면 특정한 수신단이 카오스 동기화를 이루어 음성비화 통신시스템을 구성할 수 있다.

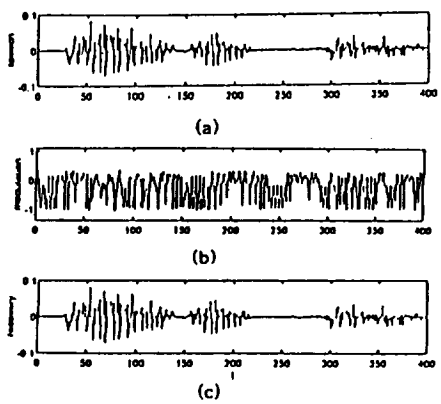

그림 6. (a) 음성신호, (b) 변조신호, (c) 복원신호
Fig. 6. (a) speech signal, (b) modulation signal, and (c) recovery signal.

V. 결 론

본 연구에서는 카오스 시스템을 동기화하기 위하여 일차원 단방향 연결을 갖는 카오스 신경망에서 세개의 뉴론을 구성하여 카오스 동기화를 축차 및 동시동기화 구성하였다. 또한 뉴론간의 카오스 동기화를 이용하여 간단한 음성비화를 행했다. 축차동기화는 출력과 연결하고 있는 뉴론의 출력에만 의존하는 피드백이고, 동기화는 축차적으로 가능하다. 동시동기화는 동기시킬 특정 출력을 이용하는 방법으로, 임의의 지점에 동시에 동기화가 이루어진다. 본실험에서 두 가지 제어방법을 이용하여 뉴론간에 카오스 동기화로 음성비화 시스템에 적용시켜 음성신호를 전송 및 복호하는 시스템에 응용하는 실험을 행했다. 실험결과에서 송신단의 음성신호는 수신단에서 정확히 복구해 내며, 동시동기화의 적용으로 임의의 수신단에 비화통신 시스템을 구성할 수 있었다.

앞으로 실제 카오스 동기화 현상을 비화시스템에 적용하기 위해서는 통신채널의 잡음, 왜곡, 간섭, 지연시간, 제한된 대역폭 등의 다양한 영향에 대하여 실험을 행해야 한다. 그리고 고속도 및 정확성을 위하여 카오스 회로의 IC 칩화가 필수적이라 할 것이다.

참 고 문 헌

1. T.S.Parker and L.O.Chua, "Choas: a tutorial for engineers," *Proc. of IEEE*, vol.75, no. 8, pp. 982-1008, 1987.
2. Hao Bai-lin, Chaos II, *World Scientific*, 1990.
3. Thomas L. Carroll and Louis M. Pecora, " Synchronizing chaotic circuits, " *IEEE Trans. Circuits Syst.*, Vol. 38. no. 4. pp.453-456, 1991.
4. Y.C. Lai and C. Grebogi, *Physical Review E*, vol.47, no.4, pp.2357-2360, 1993.
5. E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.* vol. 64, no. 11. pp. 1196-1199, 1990.
6. K. Pyragas, "Continuous control of chaos by self-controlling feedback," *Phys. Rev. A170*, pp. 421-428, 1992.
7. Toshimitsu Ushio, "Chaotic synchronization in one-dimensional chaotic neural networks with uni-directional connections," *通信學報(in Japan) Technical Report of IEICE*, 1993.
8. K. Aihara, T. Takabe and M. Toyoda, "Chaotic neural networks," *Phys. Lett. A*, vol. 144, no. 6-7, pp. 333-339, 1990.
9. 이익수, 정호선, "카오스 뉴론회로를 이용한 CNN의 하드웨어 구현에 관한 연구," *The 3th Proceeding of JCEANF 93*, pp. 407-411, 1993.
10. Y. C. Doh, I. S. Lee, and H. S. Chung, "Ciphering system using chaotic synchronization," *The 11th Korea, Japan, and China Joint Seminar*, pp. 83-91, 1994.
11. A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signal process ing in the context of chaotic signals," *Proc. of ICASSP*, vol. 4. pp. 117-120, 1992.
12. K. M. Cuomo and A. V. Oppenheim, "Circuits implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* vol. 71, no. 1. pp. 65-68, 1993.
13. L. O. Chua, L Kocarev, K. Eckert, "Experimental chaos synchronization in chua's circuit," *Int. J. Bifurcation and Chaos*, vol. 2, no. 3, pp. 705-708, 1992.