퍼지 및 지능시스템학회 논문지 2003, Vol. 13, No. 6, pp. 698-703

자기피드백 마스킹 기법을 사용한 카오스 음성비화통신

Chaotic Speech Secure Communication Using Self-feedback Masking Techniques

이익수* · 여지환**
Ik-Soo Lee*, Ji-Hwan Ryeo**

* 포항1대학 컴퓨터정보통신과
** 대구대학교 정보통신학부

요 약

본 논문에서는 카오스 신호를 이용하여 음성신호의 보안전송을 위한 아날로그 비화통신 시스템을 제안하고 통신성능을 분석하였다. 기존의 카오스 동기화 및 카오스 변조통신 알고리즘을 개선하여 통신환경에서 발생하는 다양한 조건들을 적용하여 음성신호의 복원능력을 모의실험 하였다. 일반적인 PC(Pecora & Carroll) 제어기법과 제안한 SFB(Self-FeedBack) 마스킹 기법을 사용하여 송신단에서 음성신호를 카오스 신호로 마스킹하여 변조하고, 통신채널에 잡음신호를 추가하여 전송하였다. 수신단에서는 카오스 응답시스템을 이용하여 음성신호를 복조하고, 복원성능을 계산하기 위하여 아날로그 복원 에러신호의 평균전력을 제안하여 계산하였다. 실험결과 마스킹 정도, 파라미터들의 민감성, 채널잡음 등에 대하여 PC 제어기법보다 피드백 제어기법의 복원성능이 우수함을 정량적인 데이터로 확인할 수 있었다. 또한 로렌쯔 카오스 비화통신시스템에 사용할 경우 파라미터들의 조합으로 암호키를 구성해야 하므로 파라미터 변화율에 대응하는 복원에러율의 관계를 모의실험값으로 구하였다.

Abstract

This paper presents analog secure communication system about safe speech transmission using chaotic signals. We applied various conditions that happen in actuality communication environment modifying chaotic synchronization and chaotic communication schemes and analyzed restoration performance of speech signal to computer simulation. In transmitter, we made the chaotic masking signal which is added voice signal to chaotic signal using PC(Pecora & Carroll) and SFB(self-feedback) control techniques and transmitted encryption signal to noisy communication channel. And in order to calculate the degree of restoration performance, we proposed the definition of analog average power of recovered error signals in receiver chaotic system. The simulation results show that feedback control techniques can certify that restoration performance is superior to quantitative data than PC method about masking degree, susceptibility of parameters and channel noise. We experimentally computed the table of relation of parameter fluxion to restoration error rate which is applied the encryption key values to the chaotic secure communication.

Key words : 카오스동기제어, 아날로그 마스킹, 음성비화통신, PC, SFB, 복원에러율

1. 서 론

최근 정보보안의 동향을 보면 아날로그 음성전화의 경우는 도청 및 통화 내용 녹음 방지를 위한 제품이 있고, 디지털 데이터 보안의 경우는 네트워크 및 시스템 운영체제의 보안 및 소프트웨어 방화벽 제품들이 다양하게 출시되고 있다. 그러나 원하는 송·수신 단말기간의 보안에 관한 제품은 가격이 고가이며, 실시간 정보처리가 어려운 단점이 있다. 카오스 동력학(chaos dynamics)은 결정론적(deterministic) 시스템이지만 다양한 동적특성을 보이며, 신호예측이 불가능한 랜덤신호를 발생시킨다. 특히 초기상태에 민감한 특징을 가지며, 독립된 카오스 시스템의 장기간 예측이 불가능하므로 카오스 동기화는 불가능한 것으로 알려졌다. 1990년에 카오스 시스템간의 동기화(synchronization) 알고리즘이 제안된 이후, 카오스 시스템은 실시간 정보의 비화 및 정보의 암호화에 적당하다고 알려지면서 최근에는 주파수확산 비화통신 및 카오스 암호기술 등에 응용하려는 시도가 활발히 진행되고 있다.

1990년 PC(Pecora & Carroll)는 카오스 동기기법을 제안하여 회로상에서 카오스동기화를 실험적으로 증명하였다. 이후 많은 카오스 동기방법이 제안되었으며, 특히 아날로그 통신시스템에 카오스 마스킹(chaotic masking) 또는 카오스 변조(chaotic modulation) 방식들이 많이 제안되었다. PC는 동일한 카오스 시스템을 송신측의 구동시스템(drive system)과 수신측의 응답시스템(response system)으로 분리하여 구동시스템에서 카오스 신호로 구동하더라도 응답시스템의 카오

접수일자 : 2003년 2월 14일
완료일자 : 2003년 10월 28일
※ 본 연구는 한국과학재단 목적기초연구 (R01-1999-00019)의 지원으로 수행되었습니다.

스 신호들이 자기 동기화(self synchronization)를 보이는 중요한 알고리즘을 발표했다[1]. 그리하여 Cuomo와 Oppenheim은 3차원 아날로그 로렌쯔(Lorenz) 회로에서 PC의 카오스 동기화 기법을 적용하여 음성신호를 카오스 마스킹하여 송·수신간의 비화통신이 가능하다는 것을 증명하였다[2].

한편, Pyragas[3]와 Kocarev[4] 등은 단방향 결합된(unidirectionally coupled) 카오스 응용시스템에서 컴퓨터 수치계산을 수행하지 않고 연속적인 피드백 제어(successive feedback control)기법을 이용하여 카오스 시스템을 동기화시켰다. 또한 Zaghloul[5]은 전송측에서 마스킹된 변조신호를 다시 자기 피드백시켜 송·수신간에 완전한 카오스 동기화와 정보신호의 복원을 모의실험을 통해 증명하였다. 최근에는 카오스 동기화와 카오스 변조통신을 할 경우 발생하는 복원에러를 줄이기 위한 다양한 연구가 진행되고 있다. 특히 실제 통신시스템의 구현시에 문제가 되는 잡음환경이나 송·수신 시스템 파라미터의 불일치 또는 통신시스템 섭동의 변화에 효율이 좋은 출력을 발생시키기 위하여 적응필터(adaptive filer), EKF, Observer based, 임펄스 동기화 등에 관한 연구가 활발히 진행되고 있다[6]-[9].

카오스 신호를 이용하는 카오스 변조방식은 카오스 캐리어(chaotic carrier) 또는 카오스 파라미터(chaotic parameters)를 변화시켜 정보신호를 변·복조한다.[10] [14] 특히 카오스 신호는 잡음과 유사한 광대역 주파수 특성으로 인하여 주파수확산 통신시스템에 적용할 수 있다. Parlitz와 Zaghloul[11] 등은 카오스 시스템에서 발생시킨 카오스 시퀀스를 이진 PN 확산코드로 사용하여 주파수확산 통신에 적용하여 외부의 잡음과 채널잡음의 영향, 다중접속시의 성능 등을 디지털 신호 전송의 비트에러율(bit error rate; BER)를 구하는 모의실험을 하였다. 또한 Chua와 Kennedy[12] 등은 카오스 시스템의 파라미터를 스위칭하여 카오스 동기화 및 비동기화 상태를 디지털 형태로 변환하여 통신하는 변조기법을 제안하였다. 이러한 디지털 변조방식에서는 반송파로 정현파 신호를 사용하지 않고 카오스 신호를 사용함으로써 카오스 변조통신시스템이 구성되어 정보신호의 비화통신이 가능해진다. 이러한 주파수확산 시스템은 다중경로의 전파지연에 의한 낮은 신호대잡음비(SNR) 성능이 향상되고, 채널의 잡음과 간섭의 영향을 최소화할 수 있으며, 방해자에 의한 보안성을 높일 수 있는 장점을 갖는다. 그러나 기존의 카오스 동기현상을 이용하는 아날로그 비화시스템은 회로소자의 제한 및 아날로그 신호처리로 인한 사용주파수 대역이 문제점으로 지적되고 신호대잡음비의 선택도 매우 제한되어 비화시스템이 유연하지 못한 단점을 가진다. 또한 비화 및 보안정도가 낮으며, 전송된 신호의 완전한 복원이 어려운 단점도 가지고 있다.

음성신호를 일반 아날로그 유선선로를 사용하여 카오스 비화통신을 행할 경우 아날로그 비화통신 알고리즘을 적용해야 한다. 따라서 기존의 카오스 동기화 및 비화통신 방법의 경우 사용 주파수의 제한과 아날로그 보드상에서 발생하는 송·수신단의 소자값들의 불일치 현상 그리고 통신채널상의 잡음과 지연특성 등이 필연적으로 발생하므로 음성신호의 복원과정에서 에러가 필수적으로 발생하게 된다.

본 논문에서는 이러한 현상들을 기반으로 하여 아날로그 비화통신 시스템을 하드웨어로 구현할 경우 발생되는 문제점과 특성을 컴퓨터 시뮬레이션으로 실험하여 시스템 설계에 참조하고자 한다. 아날로그 비화통신 알고리즘 중에서 기존의 PC 제어기법과 제안한 SFB 제어기법을 비교하여 모의실험을 행하였다. 특히 복원성능의 경우는 전구간에서 아날로그 에러신호의 평균전력값을 제안하여 분석하였으며, 마스킹 정도, 신호대잡음비, 채널잡음, 카오스 시스템의 파라미터 변화 등에 관하여 모의실험을 행했다. 제안한 SFB 제어기법의 알고리즘이 음성신호의 비화통신에 적합함을 확인할 수 있었으며, 다양한 통신환경에서 음성신호의 복원성능을 계산하였다.

2. SFB 마스킹 기법의 비화통신 시스템

Wu와 Chua[10]는 선형 자율시스템이 $dx/dt = Ax + f(x_P)$일 때, A의 모든 고유치(eignvalue)가 좌반평면에 존재하면 $dx/dt = Ax$ 시스템은 안정하다는 원리를 도입하였다. 구동-응답시스템(drive response system)을 구동시스템은 x, 응답시스템은 x'으로 구성한 후, 분리하면

$$\begin{aligned} \frac{dx}{dt} &= Ax + f(x_P) \\ \frac{dx'}{dt} &= Ax' + f(x_P) \end{aligned} \tag{1}$$

와 같이 되고, 식 (1)에서 두 시스템의 차분을 구하여 정리하면

$$\frac{d(x'-x)}{dt} = A(x'-x) \tag{2}$$

와 같이 된다. 여기서 A시스템의 고유값이 좌반평면에 존재할 경우 시간에 지남에 따라 전역적으로 카오스 동기화가 된다고 제안하였다.

본 논문에서 제안한 카오스 동기화 기법과 마스킹 기법을 이용한 카오스 음성 비화통신의 알고리즘은 다음과 같이 기술할 수 있다. 송신측에서

$$\frac{dv}{dt} = g(v,w) + s(t), \quad \frac{dw}{dt} = h(v,w) \tag{3}$$

와 같이 구동시스템을 구성할 경우 $s(t)$는 음성신호, $v(t)$는 송신측의 카오스 신호, h는 안정한 부시스템(sub-system)이 된다. 송신측에서는 음성정보의 인코딩 방법으로 카오스 구동신호와 마스킹한 $m(t)$를 카오스 변조신호로 하여 통신채널로 전송한다. 수신측에서는 안정한 응답 부시스템의 $v'(t)$ 신호를 $v(t)$로 대치하여 $dw'/dt = h(v,w')$와 같이 구성한다. 구동 $v(t)$신호에 의해 응답된 $h(v,w')$의 w' 부시스템의 리아푸노프 지수가 모두 음수이면, 시간이 지남에 따라 $|w-w'| \to 0$이 진행되어 카오스 시스템간에는 동기화가 이루어진다. 따라서 수신측에서 복호된 음성신호 $s'(t)$는 전송된 마스킹 신호와 동기화된 카오스 신호를 이용하여 다음의 식 (4)와 같이 디코딩 과정을 거쳐 복원된다.

$$s'(t) = \frac{dv}{dt} - g(v,w') \to \frac{dv}{dt} - g(v,w) \cong s(t) \tag{4}$$

일반적으로 기존의 아날로그 신호의 카오스 비화통신은 PC가 제안한 구동-응답시스템을 사용한다. 그림 1에서의 구성도와 같이 구동되는 카오스 신호에 정보신호를 마스킹하여 전송하면, 응답 부시스템에서는 전송된 마스킹 신호를 외부입력으로 하여 결합된 응답시스템에서 카오스 신호를 발생시키고, 디코딩 과정을 거쳐 정보신호를 복원하게 된다. 그러나 이러한 PC방식의 비화시스템 복원성능이 카오스 신호와 정보신호의 크기에 종속적이고, 인코딩할 경우 비선형 인코딩

이 불가능해 보안정도가 낮다는 단점을 가진다. 그러나 그림 1에서와 같이 자기피드백(self-feedback)을 이용한 SFB 제어기법으로 비화시스템을 구성하면 마스킹신호의 정도에 관계없이 정보신호의 복원이 가능한 독립적인 비화시스템을 구현할 수 있다.

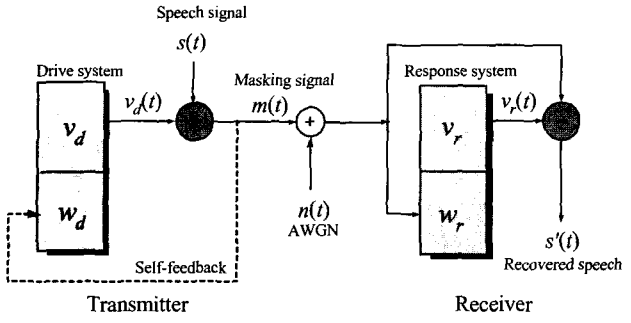


그림 1. 자기피드백 마스킹 제어기법의 비화통신시스템

본 논문에서는 로렌쯔 회로시스템[2]을 적용하여 기존의 PC 제어기법을 개선한 피드백 마스킹 제어기법을 제안하여 카오스 비화시스템을 구성하여 실험하였다. PC 방법은 단순하게 일방향으로 구동 및 응답시스템을 구성된 반면, SFB 마스킹 제어기법에서는 식 (5)과 (6)에서와 같이 구동 부시스템에 마스킹신호를 자기 피드백시켜 송신시스템을 구동하게 한다. 여기서 전송되는 카오스 변조신호는 카오스 신호와 음성신호를 마스킹한 신호는 $m(t)=x_1(t)+s(t)$와 같이 부호화 된다. 다음의 식 (5)는 송신 구동시스템이 되고, 식 (6)은 수신 응답시스템이 된다. 특히 3개의 로렌쯔 회로시스템 파라미터값 $\sigma=16.0$, $\gamma=45.6$, $b=4.0$ 등은 송·수신간에는 이상적으로 동일해야 신호의 정확한 복원이 가능하다.

$$\begin{aligned}\frac{dx_1}{dt} &= \sigma(x_2-x_1)\\ \frac{dx_2}{dt} &= \gamma m(t)-x_2-20\,m(t)x_3\\ \frac{dx_3}{dt} &= 5m(t)x_2-bx_3\end{aligned} \tag{5}$$

$$\begin{aligned}\frac{dy_1}{dt} &= \sigma(y_2-y_1)\\ \frac{dy_2}{dt} &= \gamma m(t)-y_2-20\,m(t)y_3\\ \frac{dy_3}{dt} &= 5m(t)y_2-by_3\end{aligned} \tag{6}$$

그림 2에서는 로렌쯔 회로시스템에서 PC 카오스 동기화 방법을 이용하여 초기값이 각각 +2와 -2 값으로 카오스 동기제어를 행할 경우 시간이 지남에 따라 카오스 동기화 과정을 나타낸 것이다. 그러나 비화시스템에 적용할 경우 음성신호가 추가되면 시간에 따라 신호변화가 급격히 심하므로 동기화가 실패할 경우도 생길 수 있다. 따라서 복원에러 $e(t)$를 줄이려면 급속한 동기화가 수행되어야 하며, 음성신호의 샘플링 시간보다 카오스 신호의 샘플링 속도가 빨라야 한다. 실험에서는 출력을 ±5V로 정규화한 로렌쯔 회로에서 40%의 급격한 변화를 갖는 초기값에 대하여 Runge-Kutta 수치해석 방법으로 샘플시간을 0.01로 하여 실험한 결과이며, 약 100번의 이산 계산 후에 동기화가 마무리됨을 확인할 수 있다.

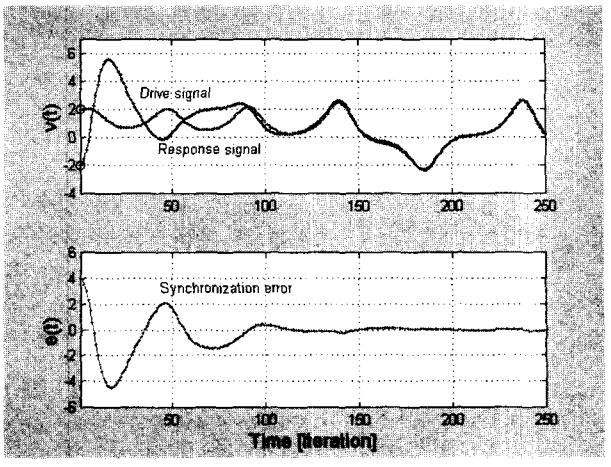
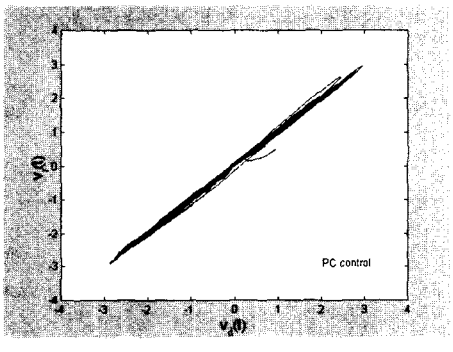
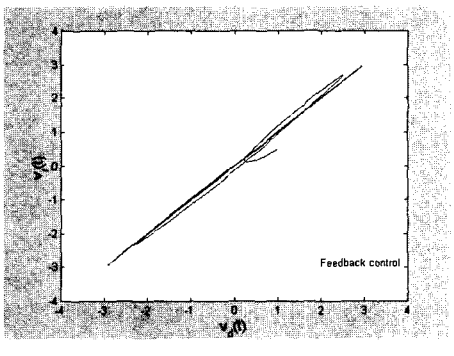


그림 2. 카오스 동기화의 예

그림 3에서는 기존의 단순한 PC 마스킹 방법과 제안한 SFB 마스킹 방법을 사용한 컴퓨터 시뮬레이션 결과를 나타낸 것이다. 음성정보신호의 레벨을 카오스 캐리어 신호에 비하여 20% 마스킹하여 전송했을 경우의 동기 실험결과이다. 그림에서 45^0의 기울기는 카오스 동기화가 이루어짐을 의미하며, PC 제어기법을 사용한 동기화 현상과 SFB 제어기법을 사용한 동기화 현상을 비교했을 경우 자기피드백 제어기법을 도입한 시스템에서의 동기성능이 우수함을 확인할 수 있다.



(가) PC 제어



(나) SFB 제어

그림 3. PC 및 SFB 제어기법의 카오스 동기화

3. 카오스 비화통신시스템의 성능분석

음성통신에서 일반 아날로그 유선선로를 사용하여 카오스 비화통신을 행할 경우 사용 주파수의 제한과 아날로그 보드상에서 발생하는 송·수신단 소자값들의 불일치현상, 통신채널상의 잡음과 지연특성 등이 존재하므로 음성신호의 복원에러는 필수 불가결하게 발생한다. 본 논문에서는 이러한 현상을 기반으로 하여 아날로그 비화통신 시스템을 하드웨어로 구현할 경우 발생되는 문제점과 특성을 모의실험을 통하여 분석하고 하드웨어 시스템 설계할 경우 참조하고자 한다. 우선 아날로그 비화통신 알고리즘 중에서 기존의 PC 제어기법과 SFB 제어기법을 비교하여 모의실험과 성능분석을 행하였다.

그림 4에서는 음성신호 $s_1(t)$에 카오스 신호 $v_1(t)$를 마스킹하여 잡음이 존재하는 통신채널에서 전송하고, 다시 복원하는 과정을 보인 실험결과이다. 그림 4에서의 세번째 신호 $m(t)$는 구동 카오스 신호에 비하여 20% 정도의 음성신호를 약 -14dB 값으로 마스킹하여 실제 전송되는 마스킹 신호이다. 통신채널에서 마스킹신호에 대하여 백색잡음신호(AWGN) $n(t)$를 추가하여 전송하고, PC 제어방법을 이용한 비화통신 알고리즘을 통하여 송·수신단의 시스템 파라미터들이 동일할 경우를 가정하여 복원한 음성신호가 다섯번째 $s_2(t)$신호이다. 그리고 여섯번째 신호 $e(t)$는 복원에러를 나타낸 것으로, 처음상태에는 초기값이 다르므로 초기에러가 발생하지만 점차적으로 카오스 동기화가 진행되어 복원에러신호가 작아지고, 음성신호가 존재하는 구간에서는 적은 값의 복원에러가 생기게 된다. 일반적으로 비화통신 시스템에서 $m(t)$신호로부터 정보신호 $s(t)$를 예측할 수 없어야 안전한 시스템(secure system)이라 할 수 있고, 이상적으로는 송·수신단에 동일한 카오스 시스템의 전자소자들이 완전히 매칭되고 통신채널에서 잡음이 없어야 신호의 완전한 복원이 가능하다.

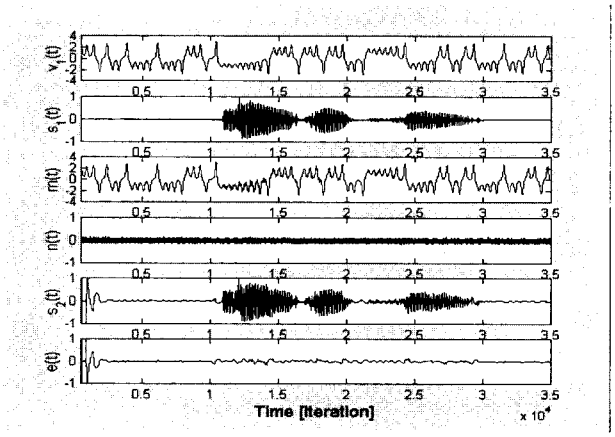


그림 4. SFB 마스킹 제어기법의 카오스 비화통신 예

한편, 디지털통신시스템의 성능을 분석하기 위해서는 신호대잡음비를 변화시키면서 비트에러율을 계산한다. 그러나 카오스 비화통신시스템과 같이 복원에러가 발생하는 아날로그 시스템에서는 복원성능을 측정하기 위하여 본 논문에서는 복원 에러신호의 평균전력을 구하는 방법을 제안하였다. 식 (7)에서와 같이 카오스신호 대 음성신호비(chaos to speech ratio; CSR)와 카오스신호 대 잡음신호비(chaos to noise ratio; CNR)를 새롭게 정의하였다. 그리고 식 (8)은 수신단에서의 아날로그 복원성능을 측정하기 위하여 아날로그 전구간의 복원에러값의 평균전력 P_e를 계산한 것으로 실험에서 예를들면 그림 4의 여섯번째 복원 에러신호의 평균전력은 0.001449가 되었다.

$$\mathrm{CSR} = 10\log\frac{v(t)^2}{s(t)^2},\quad \mathrm{CNR} = 10\log\frac{v(t)^2}{n(t)^2} \tag{7}$$

$$P_e = \frac{1}{N}\sum_{t=0}^{N} e(t)^2,\quad e(t) = s(t) - s'(t) \tag{8}$$

표 1에서는 기존의 PC 방법과 제안한 SFB 방법으로 모의실험한 결과를 나타낸 것이다. 마스킹율은 음성신호 대 카오스 신호의 비율을 구한 것으로 PC방법에서는 마스킹율이 높아질수록 즉, CSR이 낮을수록 P_e 값이 줄어듬을 알 수 있다. 이것은 음성신호가 카오스 신호에 비하여 신호레벨이 점차적으로 증가함에 따라 지수함수적으로 복원신호의 평균에러가 감소함을 의미하는 것이다. 그러나 제안한 피드백 제어방법인 SFB에서는 통신시스템에서 채널잡음이 없을 경우 음성신호의 레벨이 줄어들더라도 복원에러를 전혀 발생시키지 않은 완전한 음성복원이 됨을 모의실험으로 확인할 수 있었다.

표 1. PC와 SFB 비화시스템의 복원에러 평균전력값

마스킹율 (%)		1	2	5	10	20	30	50
CSR (dB)		44.7	38.7	30.7	24.7	18.6	15.1	10.7
P_e	PC	0.01264	0.00420	0.00180	0.00145	0.00136	0.00134	0.00132
	SFB	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000

일반적인 카오스 시스템에서는 초기값에 민감하며, 시스템 파라미터의 변화에 따라 다양한 동적현상을 보인다. 따라서 카오스 시스템에서 파라미터값의 설정은 중요한 역할을 한다. 또한 아날로그 하드웨어 시스템으로 구현할 경우 전자소자들을 완전히 동일하게 제작하기는 불가능하며, 외부 환경의 변화에 소자값들이 약간의 변화를 일으킨다. 이것은 카오스 회로시스템의 파라미터가 변동값을 갖는다는 것을 의미한다.

본 논문에서는 동일한 송·수신단의 카오스 시스템 파라미터를 설정한 경우와 각 소자값들의 변화를 파라미터 변화율로 다르게 설정했을 경우 비화시스템에서 나타나는 복원에러의 성능을 분석하였다. 표2와 그림 5는 파라미터 변화에 대한 카오스 비화시스템의 복원성능을 모의실험한 것이다.

표 2. 파라미터 변화의 비화시스템 복원성능값

변화율 / 파라미터			1%	2%	5%	10%
P_e	σ	PC	0.001359	0.001450	0.002739	0.007924
		SFB	0.000083	0.000328	0.001976	0.007449
	γ	PC	0.002033	0.003899	0.017179	0.064926
		SFB	0.000650	0.002602	0.016262	0.065048
	b	PC	0.001997	0.003612	0.014840	0.054702
		SFB	0.000555	0.002219	0.013842	0.055206
	σ, γ, b	PC	0.003779	0.011303	0.066288	0.273591
		SPB	0.002572	0.010374	0.094289	0.276683

식 (5)과 (6)에서와 같이 로렌쯔 회로시스템은 3개의 시스템 파라미터 σ, γ, b가 있다. 따라서 표 2는 3개의 파라미터 변화율(Variation)에 대한 PC 비화시스템과 SFB 비화시스템의 복원성능값을 정리한 것이다. 전체적으로 고찰하면, 그림 5에서와 같이 SFB 제어를 사용한 알고리즘이 단순한 PC 제어방법보다 파라미터의 변화에 둔감한 것을 확인할 수 있다. σ의 1% 변화에 대한 복원에러의 평균전력 P_e를 기준으로 했을 경우 PC방식이 SFB방식보다 약16.4배 높고, 5%의 경우는 1.4배 높음을 알 수 있다. 또한 PC방식을 기준으로 5% 파라미터 변화를 설정했을 경우 σ의 1% 변화에 대한 P_e는 약 2배, γ와 b의 경우는 각각 약 8.5배와 7.4배가 됨을 계산할 수 있었다.

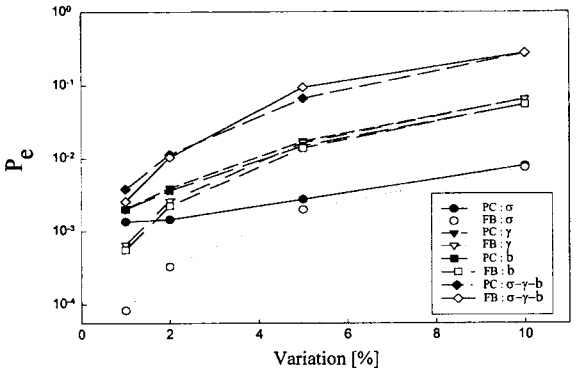


그림 5. 파라미터 변화에 대한 복원에러율

그림 6은 피드백 제어기법을 이용하여 각각 1%, 5%, 10%의 σ 파라미터의 변화에 대한 복원에러 신호를 정량적인 파형신호로 나타낸 것으로 파라미터의 변화율이 심할수록 복원에러가 증가함을 알 수 있고, P_e 값은 그림 6의 위에서부터 0.000083, 0.001976, 0.007449 등의 값을 계산할 수 있다.

결론적으로 로렌쯔회로를 이용한 카오스 비화시스템에서는 σ의 파라미터에 둔감하며, γ 파라미터에 민감함을 분석할 수 있었다. 또한 피드백 제어방법을 이용한 데이터를 분석하여 보면 PC 제어방법보다 파라미터의 변화율에 따라 P_e가 훨씬 증가하는 단점을 모의실험에서 확인할 수 있었다. 이러한 파라미터의 변화에 대한 복원에러율의 비교·분석한 결과는 추후 카오스 시스템 파라미터를 조합하여 암호키를 만들 경우 유용한 데이터로서 활용할 수 있을 것이다.

마지막으로 그림 7은 통신채널에서 잡음이 존재할 경우의 PC 비화시스템과 SFB 비화시스템의 성능을 분석한 것이다. 그래프에서 보면 채널의 잡음이 줄어짐에 따라 PC 방법과 피드백 제어방법에 의한 복원에러가 현저하게 낮아짐을 알 수 있다. 특히 SFB 제어를 행한 알고리즘이 PC방법보다 복원성능이 우수하다는 것을 확인할 수 있었고, 채널잡음이 적을 경우에도 피드백 제어를 행한 시스템의 복원에러율이 현저히 낮아짐을 알 수 있다. 예를들면 그림 7에서와 같이 신호대 잡음비 CNR이 25dB의 경우 피드백 제어방식의 복원능력이 PC 제어방식보다 약 4.3배 정도 우수함을 확인할 수 있다.

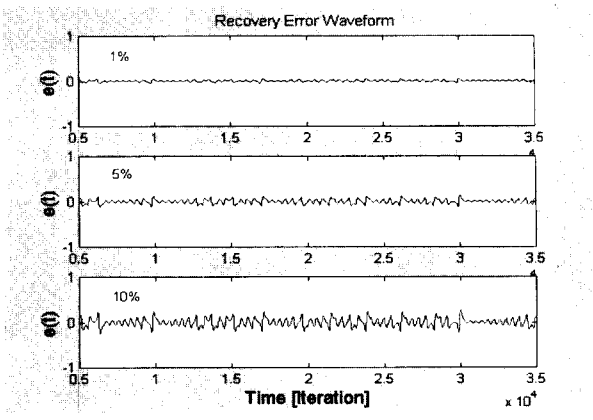


그림 6. SFB을 이용한 σ의 변화에 대한 복원에러 신호

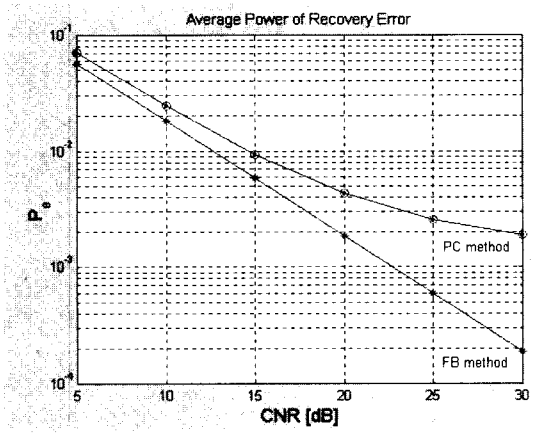


그림 7. 채널잡음이 있을 경우의 복원성능 비교

4. 결 론

본 논문에서는 PC 제어방법과 SFB 제어방법을 이용하여 음성신호에 대한 카오스 비화통신 시스템의 성능을 분석하였다. 실제 하드웨어로 제작하기에 앞서 컴퓨터를 이용하여 컴퓨터 시뮬레이션을 행하여 복원성능을 확인하고, 여러 가지 문제점과 하드웨어 설계에 고려해야 하는 사항들에 대하여 실험을 하였다. 결론적으로 PC 제어방법보다는 SFB 제어를 행한 비화시스템이 복원성능에서 훨씬 우수하다는 것을 확인할 수 있었다. 특히, 카오스 신호와 음성신호를 마스킹할 경우는 마스킹 신호의 크기에 관계없이 완전한 복원을 수행함을 증명하였다. 그리고 파라미터의 변화와 채널잡음이 존재하는 상황에서도 SFB 제어를 한 비화시스템의 복원능력이 우수함을 모의실험으로 증명할 수 있었다.

앞으로 카오스 신호와 정보신호를 마스킹할 경우 비화도를 높이기 위한 비선형적인 인코딩과 디코딩 방법을 고안해야 하며, 추가적으로 보안시스템의 성능을 향상시키기 위하여 암호화 블록을 두어 좀더 안전한 신호의 전송이 이루어지도록 연구해야 할 것이다. 또한 카오스 비화시스템을 하드웨어로 제작할 경우에 적합한 카오스 신호발생기에 관한 연구도 진행되어야 할 것으로 사료된다.

참 고 문 헌

[1] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, Vol.64, No.8, pp.821 824, 1990.

[2] 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.

[3] K. Pyragas, "Continuous control of chaos by self controlling feedback," *Phys. Rev. A170*, pp. 421 428, 1992.

[4] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.*, Vol.74, No.25, pp.5028 5031, 1995.

[5] V. Milanovic and M.E. Zaghloul, "Improved masking algorithm for chaotic communications systems," *Electron. Lett.*, Vol.32, pp.11 12, Oct., 1996.

[6] J.H. Peng, E.J. Ding, M. Ding and W. Yang, "Synchronizing hyperchaos with a scalar transmitted signal," *Phys. Rev. Lett.*, Vol.76, No.1. pp.904 907, 1996.

[7] T.L. Liao and N.S. Huang, "An observer based approach for chaotic synchronization with applications to secure communications," *IEEE Trans. Circuits Syst. I.*, Vol.46, No.9, pp. 1144 1150, Sept., 1999.

[8] Y. Zhang, G.H. Du and J.J. Jiang, "Synchronization chaos by impulsive feedback method," *Int. J. Bif. and Chaos*, Vol.11, No.8, pp.2233 2243, 2000.

[9] H. Leung and Z. Zhu, "Performance evaluation of EKF based chaotic synchronization," *IEEE Trans. Circuits Syst. I.*, Vol.48, No.9, pp. 1118 1125, Sept., 2001.

[10] C.W. Wu and L.O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication," *Int. J. Bif. and Chaos*, Vol.3, No.6, pp.1619 1627, 1993.

[11] U. Parlitz and S. Ergezinger, "Robust communication based on chaotic spreading sequences," *Phys. Lett. A188*, pp.146 150, 1994.

[12] G. Kolumbán, M.P. Kennedy, and L.O. Chua, "The role of synchronization in digital communications using chaos Part I: Fundamentals of digital communications," *IEEE Trans. Circuits System.*, Vol.44, No.10, pp. 927 936, Oct., 1997.

[13] J. Kraus, J.A. Nossek, T. Yang and L.O. Chua, "Evaluation of a continuous valued chaotic spreader used in a chaotic digital code division multiple access ((CD)2MA) system," *Int. J. Bif. and Chaos*, Vol.10, No86, pp.1933 1950, 2000.

[14] G. Jakimiski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits System.*, vol. 48, no. 2, pp. 163-169, Feb. 2001.

저 자 소 개

이익수(Ik-Soo Lee)

1991년 : 경북대학교 전자공학과 졸업(학사)
1994년 : 경북대학교 대학원 전자공학과 졸업(석사)
2000년 : 경북대학교 대학원 전자공학과 졸업(박사)
1996년~현재 : 포항1대학 정보통신과 조교수

관심분야 : 시스템설계, 카오스제어 등

Phone : +82-54-245-1253
Fax : +82-54-252-3400
E mail : leeis@pohang.ac.kr

여지환(Ji-Hwan Ryeo)

1975년 : 경북대학교 전자공학과 졸업(학사)
1977년 : 경북대학교 대학원 전자공학과 졸업(석사)
1992년 : 경북대학교 대학원 전자공학과 졸업(박사)
1982년 ~ 현재 : 대구대학교 정보통신공학부 교수

관심분야 : 반도체회로, 퍼지회로 등

Phone : +82-53-850-6612
Fax : +82-53-850-6612
E-mail : jhryeo@biho.taegu.ac.kr