論文 97-22-11-14

통신암호화에 응용된 로렌츠 기반 이산 카오스의 동기화에 관한 연구

正會員 박 철*, 김 영 태**, 고 형 화**

A Study on Synchronization of Lorenz-Based Discrete Chaotic with Application to Communication Encryption

Chul Park*, Young-Tae Kim**, Hyung Hwa Ko** *Regular Members*

요 약

본 논문에서는 카오스 현상을 발생시키는 이산 로렌츠 시스템의 컴퓨터 모의 실험에 대한 방법을 제시하였다. 모의 실험에서의 카오스적인 움직임은 수치해석에 의해 예측된 결과와 일치하였다. 동기화된 카오스 시스템의 원리를 사용함으로써, 비화통신을 위한 접근방법 로렌츠 방정식을 코딩한 송·수신기를 컴퓨터를 사용, 모의 실험함으로써 증명하였다. 송신기에서는 카오스 신호를 사용해서 보내고자 하는 메시지를 먼저 카오스 신호와 곱하고 다시 카오스 신호를 더해서 전송한다. 한편 수신기에서는 전송된 신호를 수신측 카오스 신호로 빼준 후에 다시 나누어서 전송된 메시지를 회복하는 방법을 사용하였다. 비선형 상태추정으로써 로렌츠 이산 카오스 동기 시스템의 견고성의 정도를 결정하기 위해서 샘플링 시간을 달리했으며, 이 때 동기 오차와 그에 따른 송신 신호와 수신 신호와의 오차 값을 비교하여 성능을 평가하였다.

ABSTRACT

In this paper, a computer simulation of the Lorenz discrete chaotic system is described. The chaotic behavior closely matches the results predicted by numerical simulations. Using the concept of discrete synchronized chaotic systems, the possibility of a secure communication is proved by simulating the Lorenz system in both the transmitter and receiver. In the proposed approach, at first, a chaotic modulating signal is multiplied with the message, and these are transmitted with adding a chaotic modulating signal, and then at the receiver, the chaotic modulating signal is regenerated and divided from the receiver signal. Varying a sampling time interval to calibrate the robustness of the Lorenz discrete synchronized chaotic system as a nonlinear state estimator, we measured the performance of the

*가산전자 연구원
**광운대학교 전자통신공학과
論文番號:96396-1220
接受日字:1996年 12月 20日

Lorenz discrete synchronized chaotic system by comparing the synchronization error and the error between transmitted signal and received signal.

Ⅰ. 서 론

자연현상의 대부분은 비선형적이며 쉽게 예측되지 않는다. 아주 세심하게 실행된 실험조차도 주위 환경으로부터 완전하게 차단될 수 없기에 라플라스가 제안했던 절대적인 수학적 측량의 정확성은 물리적으로 실현할 수 없다. 비선형적 시스템에서 본질적으로 존재하는 오차는 시스템이 전개해 감에 따라 점점 증폭되어 신호가 어느 정도 성장하면 그 시스템이 초기 정보를 모두 잃어버리게 되어 뜻밖의 결과를 불러일으킨다. 그때 예측은 불가능하게 되고 우리는 우연한 현상을 보게 된다. 이렇듯 비선형적 시스템에서는 초기 조건의 근소한 차이가 매우 다른 결과를 초래한다. 이것이 바로 결정론적 카오스이다.

카오스 운동은 초기 조건에 매우 민감한 특성을 가지고 있기 때문에 초기치의 작은 오차를 지수 함수적으로 빠르게 증폭시켜 버린다. 하지만 1989년 미국 해군 연구소와 페코라(Pecora)등에 의해 두 개의 동일한 계를 카오스 운동으로 동기화시킬 수 있는 방법이 고안되었다. 이러한 특별히 유용한 특성을 자체-동기라고 하며[1][2][3], 이 경우의 전제조건은 두 시스템이 안정 시스템이어야 한다. 카오스 시스템이 안정적이라는 것은 리아프노프 지수(Lyapunov exponent)가 모두 음수(−)일 때를 의미하며 이때 두 시스템이 동기화된다. 안정 시스템이 초기 조건에 약간의 변화가 있어도 종국에는 같은 상태의 운동으로 귀착되는 성질을 갖고 있기 때문에 두 개의 카오스 안정 시스템을 동시에 구동시킬 때, 양쪽 시스템의 상태가 약간 다르더라도 시스템의 안정성에 의해 같은 상태의 카오스 운동으로 동기화될 수 있게 된다. 카오스 시스템은 자체-동기시스템이다. 구동 시스템(송신기)과 안정적 응답 부시스템(수신기)은 공통신호로 결합될 때 동기화된다. 동기화된 카오스 시스템에서 그 동기화 능력은 견고하다. 예를 들어, 로렌츠 시스템에서 동기화는 구동 시스템의 교란에서도 매우 견고하다. 이러한 특성이 흥미있는 통신응용에 적용된다. Cuomo와 Oppenheim의 논문[4],[5]에 소개된 카오스 정보은닉 기술은 비화통신이 잠재적으로 가능한 것을 보여준다. 카오스 동기 시스템의 입력은 송신기의 상태 벡터 중 하나의 요소로 구성되어 있고 송신기의 전차원 벡터를 생성한다. 잡음이 없는 상태에서의 측정의 경우, 로렌츠 시스템은 지수적으로 빠르게 수렴함으로써 점근선적 상태추정은 정확하다.

본 논문은 Cuomo와 Oppenheim[6]이 제안한 카오스 발생기를 아날로그(analog) 회로구현 대신 이산적인 수치해석 방법을 통하여 컴퓨터 모의실험으로 시스템을 구현하였으며 이 이산적 카오스 발생기를 바탕으로 새로운 정보 은닉모델을 제안하였다. 제안된 정보 은닉모델은 송신기에서는 카오스 신호를 사용해서 보내고자 하는 메시지를 먼저 카오스 신호와 곱하고 다시 카오스 신호를 빼준 후에 다시 나누어서 전송된 메시지를 회복하는 방법을 사용하였다. 아날로그 회로구현 방법과 컴퓨터 모의 실험과의 차이점을 살펴보면 아날로그 회로는 증폭기를 이용한 시간의 변화량이 연속적인 아날로그 신호인 반면 컴퓨터 모의 실험은 시간의 변화량이 이산적인 디지털 시스템이다. 따라서 신호를 해석하는 방법이 회로구현과 모의 실험은 다르다. 특히 회로해석은 미분 방정식으로 로렌츠 어트렉터를 표현하나 이산 로렌츠 동기 시스템은 차분방정식이나 맵핑을 이용하여 해석한다. 그러므로 미분 방정식에서는 고려하지 않는 샘플링 간격도 동기를 결정하는 중요한 파라미터로 작용한다. 본 논문에서 제안한 이산 시스템을 로렌츠 이산 동기화 시스템이라고 한다. 본 논문의 구성은 다음과 같다. 2장에서 카오스 이론을 살펴보고 3장에서 제안한 로렌츠 기반 통신 암호화 모델을 살펴본다. 4장에서 컴퓨터 모의 실험에 대한 결과와 고찰을 다루고 5장에서 결론을 기술하였다.

Ⅱ. 카오스 이론

카오스 현상을 정의할 때 흔히 "nonlinear dynamical system"이라 하며 사전적인 의미는 다음과 같다. 「결정론적 역학계(deterministic dynamical system)에 나타나

는 유계(有界)한 비주기적인 거동의 총칭, 특히 안정성(리아프노프 지수 함수로 판정함)을 동반하여 나타나는 카오스를 스트레인지 어트랙터(strange attractor)라고 부른다. 그 특징으로는 초기값에 대한 예민성, 궤도 불안정성, 연속적인 주파수 성분으로 된 난잡한 거동 등이다[7].」 스트레인지 어트랙터의 여러 가지 모델 중에서 본 논문에서 사용한 로렌츠 어트랙터에 대하여 살펴본다. 최초의 스트레인지 어트랙터는 1963년에 발표된 "결정론적 비주기성 흐름(Deterministic Aperiodic Flow)"[10]이란 E. N. Lorenz의 논문에서 나타난다. 로렌츠는 난류현상을 세 개의 상미분 방정식으로 구성된 동역학계로 단순화한 후 아날로그 컴퓨터를 사용하여 모의 실험을 하였다. 모델의 출발점은 1916년 Rayleigh가 연구했던, 두께 h인 유체층의 밑면을 고온, 윗면을 저온으로 하여 두면의 온도차를 ΔT로 유지할 때(중력의 방향은 아랫방향이다), 유체층을 통한 에너지의 전송의 문제에 관한 것이다. 이때 ΔT를 증가시키면 열전도에 의한 에너지 전송은 불안정해지고 곧이어 레일리 대류(Rayleigh convection)가 일어난다. ΔT를 더 증가시키면 레일리 대류의 해 또한 불안정해져서 시간과 관계되는 동역학을 보인다. 이러한 현상이 로렌츠(Lorenz)가 고려했던 것이다. 이때 2차원 운동만을 고려한다면($\partial/\partial z \equiv 0$) 그러한 유체는 다음과 같은 미분 방정식을 만족한다.

$$\begin{aligned} x' &= \sigma(y-x) \\ y' &= \gamma x - y - xz \\ z' &= -bz + xy \end{aligned} \tag{1}$$

여기서 x는 대류운동의 진폭, y는 내려가는 것과 올라가는 흐름 사이의 온도차, z는 수직한 방향의 온도 분포에서 선형적인 것으로부터 변형정도 등을 나타낸다. 그리고 $\sigma = \nu/x$는 Prandtl 수, ν는 점성계수, x는 열전도율, $\gamma = \gamma_a/\gamma_c$는 정규화된 레일리수이다. 여기서 $\gamma_a = g\alpha h^3 \Delta T/\nu x$, $\gamma_c = \pi^4(1+a^2)^3/a2$, g는 중력가속도, α는 열팽창계수, a는 x방향의 파장을 결정하는 매개변수, $b = 4(1-a^2)^{-1}$이고, 미분은 정규화 시간($\pi^2 h^{-2}(1+a^2)xt$, t는 시간)에 관한 미분을 나타낸다.

Ⅲ. 이산 로렌츠 기반 통신 암호화 모델

1. 제안하는 정보 은닉 모델

통신에서 카오스의 응용 방법 중 하나는 카오스적 신호 은닉과 회복이다([4][5][6][16][17][18]). 본 논문은 이산 로렌츠 어트랙터를 이용하여 정보를 은닉하는 모델을 그림1과 같이 제안하였다.

송신측은 카오스 신호 $x(n)$을 사용해서 보내고자 하는 정보 신호 $m(n)$를 먼저 카오스 신호 $x(n)$와 곱하고 다시 카오스 신호 $x(n)$을 더해서 전송한다. 여기서 카오스 신호 $x(n)$을 한 번 더 더해 주는 것은 수신측에서 동기를 맞추기 위한 신호를 첨가하기 위해서다. 한편 수신측에서는 전송된 신호 $s(n)$를 수신측 카오스 신호 $x_r(n)$로 빼준 후에 다시 나누어서 전송된 신호를 회복한다. 이때 송·수신단이 동기상태가 되는 것이 중요한데, 전송된 신호 $s(n)$의 일부가 수신측 카오스 발생 신호 $y_r(n)$과 $z_r(n)$의 입력으로 들어가서 송신측 카오스 발생기 $x(n)$과 수신측 카오스 발생기 $x_r(n)$의 동기를 맞추는 역할을 한다.

송신측과 수신측이 동기 상태가 되게 하는 동기 능력은 샘플링 시간 Δt에 따라 오차가 달라진다. 즉 샘플

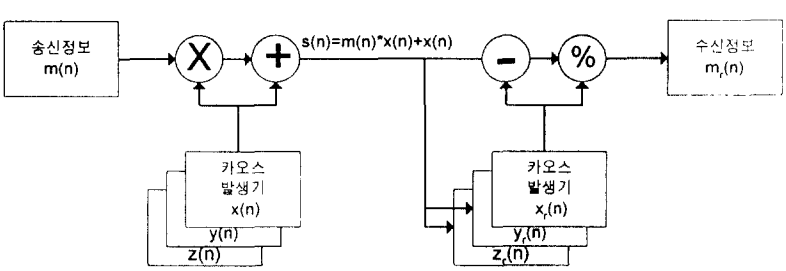


그림 1. 정보 은닉 모델
Fig. 1 Chaotic signal hiding model

링 간격 Δt가 좁을수록 동기능력은 구동 신호에서의 혼란에 민감하지 않다. 그러므로 동기는 은닉된 신호와 함께 행해 진다. 이러한 구상은 단지 로렌츠 어트렉터에 국한되지 않고 다른 어트랙터를 사용하여 은닉 시스템을 구현하는 것도 충분히 가능하다. 예를들어 Kocarev 등[19]은 Chua의 회로를 사용하여 신호은닉 개념을 밝혔다[4][5].

본 논문에서는 전송신호를 $s(n)=x(n)\times m(n)+x(n)$ 형태로 전송되는 신호로 생각한다. 카오스 신호를 메시지와 곱한 것은 신호를 변조하기 위해서이고, 카오스 신호를 더한 것은 수신측에서 동기를 맞추기 위해서다. 은닉을 위해 $m(n)$의 전력 레벨은 $x(n)$의 전력 레벨보다 훨씬 더 작아야 동기능력이 우수하다. 수신기가 $s(n)$와 동기가 되었다면, $x_r(n)\simeq x(n)$이다. 그리고 결국 $m(n)$는 $m_r(n)=\{s(n)-x_r(n)\}/x_r$로 회복되어진다.

2. 송신기

파라미터 $\sigma=16$, $\gamma=45.6$과 b=4로 정했을 때 송신기의 동적 시스템은 다음과 같다.

$$\begin{aligned} x' &= 16(y-x) \\ y' &= 45.6x-y-20xz \\ z' &= 5xy-4z \end{aligned} \tag{2}$$

식(2)를 그대로 C-언어로 구현하기에는 오차가 커서 오차를 지수 함수적으로 증가시키는 카오스 방정식에 그대로 사용할 수 없다. 오차를 줄이기 위해서는 오차가 적은 수치 해석법인 Runge-Kutta 4차법[12]을 사용하였다.

3. 수신기

식(2)에서 카오스 신호에 동기된 전차원 응답 시스템은 다음과 같이 주어진다.

$$\begin{aligned} x_{rn}' &= 16(y_{rn}-x_{rn}) \\ y_{rn}' &= 45.6x_{rn}-y_{rn}-20x_{rn}z_{rn} \\ z_{rn}' &= 5x_{rn}y_{rn}-4z_{rn} \end{aligned} \tag{3}$$

이 시스템은 변수(x_n, y_n, z_n)를 (x_{rn}, y_{rn}, z_{rn})로 다시 이름을 붙이고 두번째와 세번째 방정식에서 x_n를 x_{rn}로 대치한 송신기 방정식으로부터 얻을 수 있으며, 이 시스템을 수신기로 부른다. 송신기 상태변수를 백터 $d=(x_n, y_n, z_n)$로 집합적으로 표시하고 수신기 변수를 $r=(x_{rn}, y_{rn}, z_{rn})$로 표시한다.

그림 1의 정보은닉 모델의 수신기를 구현한 동적 시스템은 다음과 같다.

$$\begin{aligned} x_{rn}' &= 16(y_{rn}-z_{rn}) \\ y_{rn}' &= 45.6s(n)-y_{rn}-20s(n)z_{rn} \\ z_{rn}' &= 5s(n)y_{rn}-4z_{rn} \end{aligned} \tag{4}$$

식(4)에서 두번째와 세번째 방정식에 x_{rn}대신에 송신기로부터 전송된 신호 $s(n)$을 쓴 것은 동기를 맞추기 위해서 임을 주의하여야 한다. 동기화 시스템의 수학적 증명[13]은 카오스 동기화의 특성인 부시스템의 신호가 주시스템의 신호의 초기 조건에 관계없이 동기화를 이룬다는 것을 증명한다[6].

Ⅳ. 실험 및 고찰

1. 실험환경

본 논문에서는 여러 가지 조건 하에서 평균 동기 오차 및 평균 신호 오차를 측정하여 카오스 통신모델의 성능을 측정하였는데 평균 동기 오차 및 평균 신호 오차를 구하는 식은 다음과 같다. 모의 실험은 채널상에서 나타나는 오류나 잡음은 고려하지 않았다. 먼저 평균 동기 오차 값을 구하는 경우를 살펴보면 송신측 카오스 신호 x_n에서 수신측 카오스 신호 x_{nr}를 뺀 값을 제곱하여 시간 n=1에서 n=k 까지 합한 값 $SU\ M_{ex}$는 다음과 같다.

$$SU\ M_{ex}=\sum_{n=0}^{k} e_{x_n}^2 \tag{5}$$

여기서, $e_{x_n}=x_n-x_{nr}$이다. 송신측 카오스 신호 x_n와 수신측 카오스 x_{nr}사이의 평균 동기 오차 RMS_{ex}를 구하기 위해서는 $SU\ M_{ex}$에 제곱근을 취한 다음 k로 나누면 된다.

$$RMS_{ex}=\frac{\sqrt{SU\,M_{ex}}}{k} \tag{6}$$

평균 동기 오차 RMS_{ex}를 dB로 계산하면 다음과 같다.

$$RMS_{ex.dB} = 20 \log_{10} RMS_{ex} \quad (7)$$

다음으로 평균 동기 오차를 구하는 방법과 동일한 순서대로 평균 신호 오차 RMS_{em}를 유도하면 다음과 같다. 송신측 신호 m_n에서 수신측 신호 m_{nr}를 뺀 값을 제곱하여 시간 n=1에서 n=k 까지 합한 값 $SU\ M_{em}$는 다음과 같다.

$$SUM_{em} = \sum_{n=1}^{k} e^2_{m_n} \quad (8)$$

여기서, $e_{m_n} = m_n - m_{nr}$이다. 송신측 카오스 신호 m_n와 수신측 카오스 m_{nr}사이의 평균 신호오차 RMS_{em}을 구하기 위해서는 $SU\ M_{em}$에 제곱근을 취한 다음 k로 나누면 된다.

$$RMS_{em} = \frac{\sqrt{SUM_{em}}}{k} \quad (9)$$

평균 신호오차 RMS_{em}를 dB로 계산하면 다음과 같다.

$$RMS_{em.dB} = 20 \log_{10} RMS_{em} \quad (10)$$

2. 카오스 신호와 메시지의 비에 따른 동기 오차 및 신호 오차 측정

본절에서는 카오스 신호 x(n)과 메시지 m(n)의 비에 따른 동기 오차 및 신호 오차를 측정하였다. 표 1에서와 같이 동기 오차 및 신호차는 카오스 신호 x(n)과 메시지 m(n)의 비를 dB로 계산하여 신호 및 동기 오차를 계산하였다. 먼저 샘플링시간 Δt가 5×10^{-6}일 때에 신호 오차 및 동기 오차를 구하였다. 이를 위한 실험 조건은 샘플 n을 카운트하여 1000번째 마다 하나씩 추출한 샘플 100개를 가지고 $RMS_{ex.db}$와 $RMS_{em.db}$를 계산한 후 그림 2에 계산한 결과를 m(n)/x(n)의 dB로 하여 나타냈다.

$$\left(\frac{m}{x}\right)_{dB} = 20 \log \frac{m(n)}{x(n)} \quad (11)$$

측정결과 로렌츠 통신 모델에 있어서 송신된 메시지를 수신하기 위한 카오스 신호 x(n)과 메시지 m(n)의 비가 작아지면 즉, 송신 메시지 m(n)의 크기가 커질수록 그에 비례하여 동기 오차가 증가함을 알았고

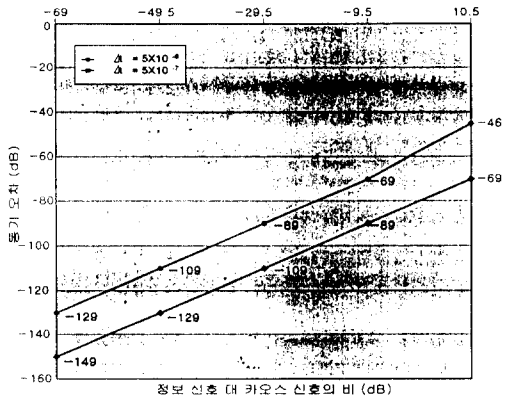


그림 2. m(n)/x(n)에 따른 동기 오차 값
Fig. 2 Synchronization error versus m(n)/x(n)

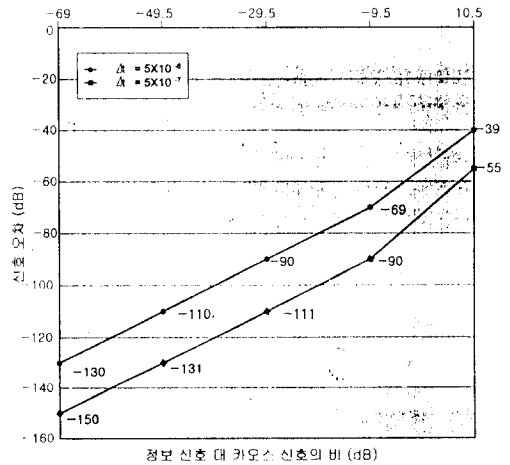


그림 3. m(n)/x(n)에 따른 신호 오차
Fig. 3 Signal error versus m(n)/x(n)

샘플링 시간의 간격이 좁아질 수록 이에 비례하여 동기 오차 및 신호 오차가 감소한다. 측정결과를 살펴보면 m(n)/x(n)가 20dB로 줄 때마다 동기 오차 및 신호 오차가 20dB씩 감소함을 알았다.

3. 수신 카오스 신호의 송신 카오스 신호 추적과정

송신 카오스신호의 초기 조건을 (-0.74075, 0.911909, 1.70688)으로 주고 수신 카오스 신호의 초기 조건을 (-0.911909, 0, 0)으로 주었을 때 샘플링 시간 Δt에 따른 동기화를 위한 추적 시간 n을 살펴보았다.

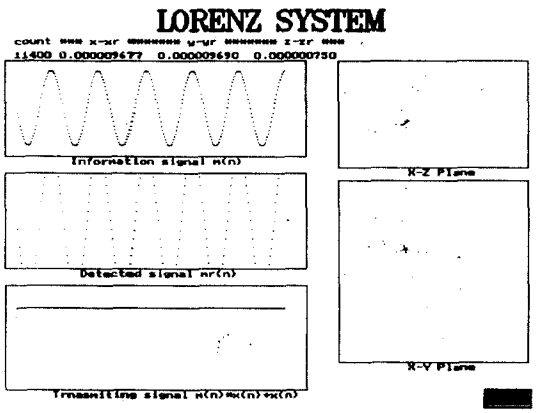
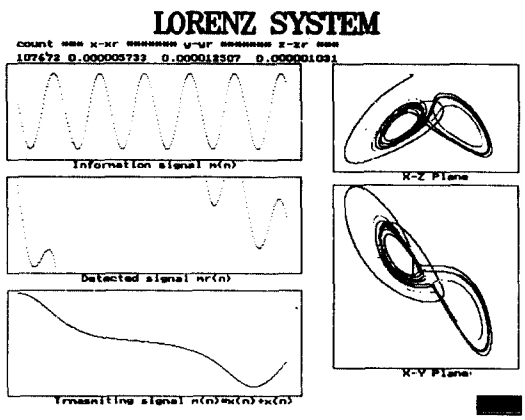


그림 4. $\Delta t = 5\times10^{-2}$인 경우의 실험
Fig. 4 Simulation in case of $\Delta t = 5\times10^{-2}$



(a)

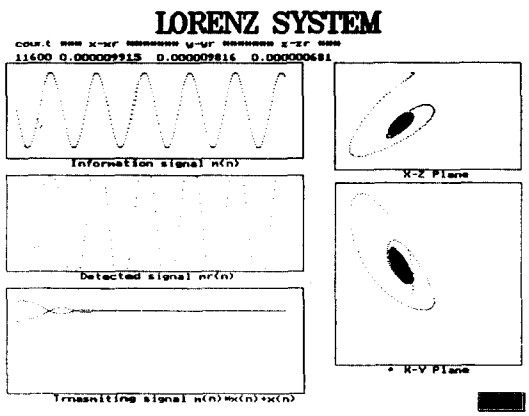
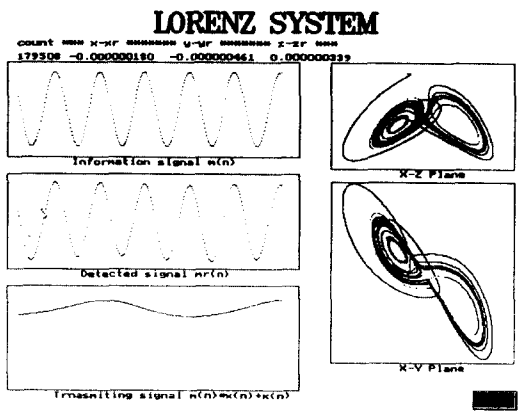


그림 5. $\Delta t = 5\times10^{-3}$인 경우의 실험
Fig. 5 Simulation in case of $\Delta t = 5\times10^{-3}$



(b)

그림 7. $\Delta t = 5\times10^{-5}$인 경우의 실험
(a) n = 107,672 (b) n = 172,500
Fig. 7 Simulation in case of $\Delta t = 5\times10^{-5}$
(a) n = 107,672 (b) n = 172,500

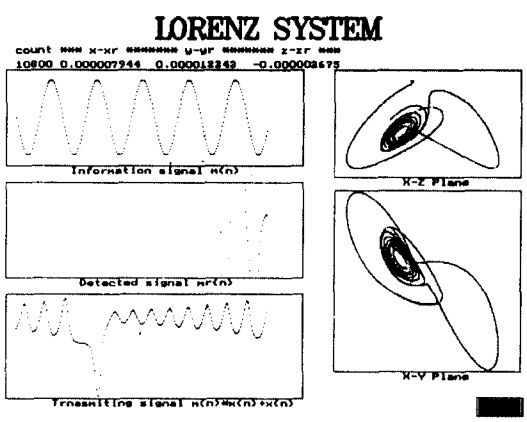
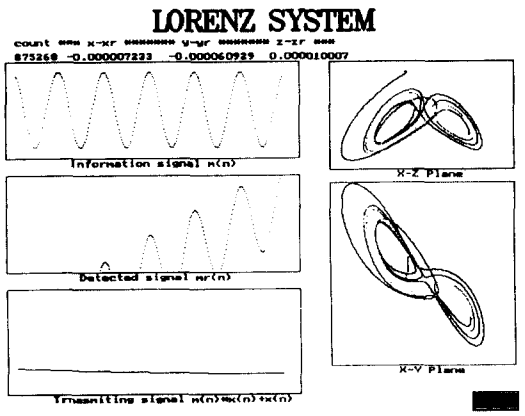
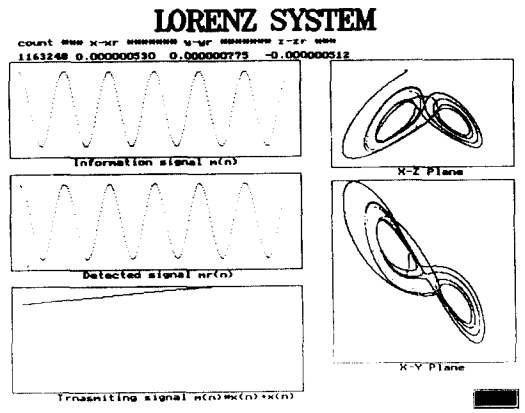


그림 6. $\Delta t = 5\times10^{-4}$인 경우의 실험
Fig. 6 Simulation in case of $\Delta t = 5\times10^{-4}$

위에서 보는 바와 같이 샘플링 시간 $\Delta t = 5\times10^{-2}$인 경우는 분석을 할 수 없을 정도로 난잡한 신호의 형태를 보인다. 샘플링 시간 $\Delta t = 5\times10^{-3}$인 n = 3400회 쯤에서 평형점으로 수렴함으로써 카오스가 발생되지 않음을 보였다. 샘플링 시간 $\Delta t = 5\times10^{-4}$인 경우는 n = 10,000회 쯤에서 동기가 이루어지지만 동기 오차가 커서 정확하게 데이터는 복원되지 않는다. 이때 동기 오차는 약 -1×10^{-4}~1×10^{-4} 사이이다. 샘플링 시간 $\Delta t = 5\times10^{-5}$인 경우에는 n = 89,000회 쯤에서 동기가



(a)



(b)

그림 8. $\Delta t = 5\times10^{-6}$인 경우의 실험
(a) n = 875,268 (b) n = 1,163,248
Fig. 8 Simulation in case of $\Delta t = 5\times10^{-6}$
(a) n = 875,268 (b) n = 1,163,248

이루어지기 시작해서 n = 123,000회 쯤에서 동기가 완전히 이루어진다. 이때 동기 오차 -1×10^{-5}~1×10^{-5} 사이로써 비교적 정확한 정보를 수신 할 수 있다. 샘플링 시간 $\Delta t = 5\times10^{-6}$인 경우에는 n = 830,000회 쯤에서 동기가 이루어지기 시작해서 n = 1,130,000회 쯤에서 동기가 완전히 이루어지며 이때 동기 오차는 -1×10^{-7}~1×10^{-7}사이에서 발생한다. $\Delta t = 5\times10^{-7}$인 경우에는 가장 적은 동기 오차를 가진 정보를 수신한다. 이때의 n은 약 9,500,000회 정도이다. 결국 샘플링 시간이 짧아지면 그와 반비례하여 동기를 이루어야 하는 시간이 길어지는 것을 알 수 있다. 상태공간상에서 관찰했을 때 동기가 이루어지는 순간의 위치는 거의 비슷하다. 그러므로 샘플링 시간 간격에 따라 일정한 위치에 도달하는 속도차이 때문에 추적시간이 시간 간격 Δt에 반비례하여 길어짐을 알 수 있다.

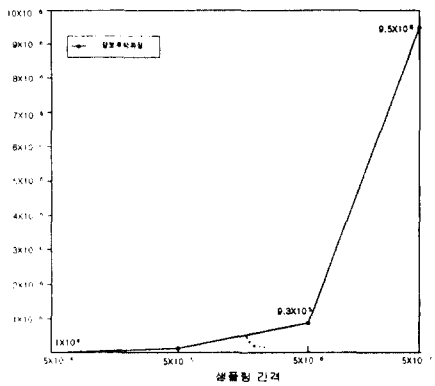


그림 9. Δt에 따른 정보 추적시간
Fig. 9 Tracing time versus Δt

4. 샘플링 시간에 따른 동기 오차 및 신호 오차 측정

아날로그 회로로 구현한 로렌츠 기반 카오스 통신 모델은 미분 방정식을 사용하기 때문에 연속적인 시간의 변화율 dt를 가지고 어트랙터의 궤도를 진화시키지만 디지털 컴퓨터를 사용한 로렌츠 기반 어트랙터는 이산적인 시간 Δt를 사용하기 때문에 수치해석에서 발생하는 오차가 발생한다. 그래서 이산 로렌츠 어트랙터는 샘플링 시간에 따라 민감하게 동기오차가 변한다. 그러므로 샘플링 시간 Δt도 비화통신의 중요한 파라미터로 작용한다. 이것을 측정하기 위해 샘플링 시간 Δt를 5×10^{-2}~5×10^{-7}까지 변화시켜 가면서 발생하는 동기 오차 및 신호오차를 측정하여 보았다. 그림 4와 그림 5에서 알 수 있듯이 샘플링 시간 Δt가 5×10^{-2}과 5×10^{-3}일 경우는 카오스가 발생하지 않거나 안정 평형점에 수렴한다. 5×10^{-3}이하인 경우는 카오스가 발생하며 동기 오차도 샘플링 간격이 좁아지면 줄어들어서 수신 메시지에 오차가 줄어든다는 것을 알 수 있다. 표 1에는 측정한 내용을 기술하였으며 그림 10에는 샘플링 시간 Δt에 따른 동기 오차 및 신호 오차를 도표로 나타내었다.

표 1. 샘플링 시간 Δt에 따른 동기 오차 및 신호 오차 측정치
Table 1. Value of synchronization error and signal error according to sampling time Δt

Δt	동기오차 (dB)	신호오차 (dB)	비 고
5×10^{-2}			카오스가 발생하지 않음
5×10^{-3}			안정 평형점에 수렴함
5×10^{-4}	−115	−93	카오스는 발생하나 동기오차가 커서 메시지를 검출 할 수 없다.
5×10^{-5}	−139	−126	카오스가 발생하며 동기오차가 작다. 신호에는 가끔 임펄스 성분이 나타남
5×10^{-6}	−187	−186	동기오차와 신호오차가 매우 적다
5×10^{-7}	−196	−196	동기오차와 신호오차가 매우 적다

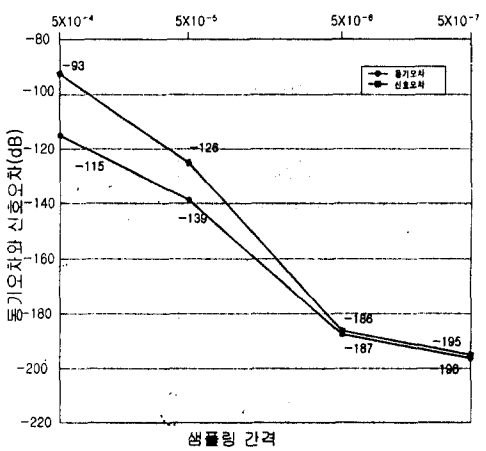


그림 10. 샘플링 시간 Δt에 따른 동기 오차 및 신호 오차 측정치
Fig. 10 Value of synchoronization error and signal error versus to sampling time Δt

5. 동기가 이루어지기 위한 파라미터 σ, γ, b의 범위 측정

본 절에서는 σ, γ, b를 변화시켰을 때 동기 오차 및 신호 오차를 측정하여 실험적으로 σ, γ, b 각각의 동기 가능한 범위를 측정해 보았다. 실험 방법은 Δt가 5×10^{-5}일 때의 파라미터 σ, γ, b중 하나를 송신측과 수신측 양쪽을 똑같은 값으로 변화시켜가면서 동기 오차가 −140 dB 이하일 경우의 파라미터 σ, γ, b의 범위를 측정하였다. 컴퓨터 모의 실험을 통해 송·수신측의 파라미터 σ를 동시에 같은 값으로 변화시킬 때의 동기여부를 측정해 본 결과 동기가 유지되면서 신호가 정확히 검출될 수 있는 파라미터 σ의 영역은 $7<\sigma<30$임을 알 수 있었다. $\sigma<7$인 경우는 안정 평형점으로 수렴, $\sigma>30$인 경우는 동기는 유지되었으나 신호오차가 큼을 알 수 있었다. 동일한 방법으로 파라미터 γ도 실험해 본 결과 $33<\gamma<70$의 사이에서 동기가 이루어짐을 알 수 있었다. $\gamma<33$은 평형점으로 수렴, $\gamma>70$은 동기는 유지되나 신호 오차가 너무 커 신호를 검출할 수 없었다. 또한 샘플링 간격을 5×10^{-5}에서 5×10^{-6}로 줄였을 경우에는 $\gamma>70$인 영역에서도 오차 없이 정확하게 수신할 수 있었다. 파라미터 b가 변할 때 b영역은 $1<b<6$ 사이에서 동기가 이루어짐을 알 수 있었다.

표 2. 파라미터 σ, γ, b와 샘플링 시간에 따른 동기 범위
Table 2. Range of synchronization according tp parameter σ, γ, b and sampling time Δt

동기 오차	Δt	파라미터	동기유지범위
−140dB 이하	5×10^{-5}일때	σ	$7<\sigma<30$
		γ	$33<\gamma<70$
		b	$1<b<6$

6. 송·수신기의 샘플링 시간과 파라미터의 차이에 따른 동기 오차 및 신호 오차 측정

본 절에서는 기본적으로 $\sigma=16$, $\gamma=45.6$, $b=4$와 샘플링 간격 $\Delta t=5\times10^{-5}$로 하고 송·수신 모델에서 한가지 파라미터만을 달리했을 때 동기오차가 −140 dB내에 있을 수 있는 송·수신기의 파라미터 σ, γ, b 및 Δt을 측정하였다. 먼저 송·수신 모델의 시간 간격 Δt를 송신 모델의 샘플링 시간 $\Delta t=5\times10^{-5}$로 고정시키고 수신 모델의 샘플링 시간 Δt_r을 5×10^{-5}~5.000000005×10^{-5}까지 달리했을 때까지를 측정하였다. 이때 오차의 정도를 나타내기 위해서 송신모델의 시간 간격 Δt를 수신 모델의 시간 간격 Δt_r로 뺀 후 Δt로 나누어준 것을 상대오차라고 하였으며 다음과 같이 나타낼 수 있다.

$$\text{오차비 } \Delta t = \frac{\Delta t - \Delta t_r}{\Delta t} \tag{12}$$

측정 결과 동기 오차가 −140dB이하 일 때 샘플링 시간 상대오차는 10^{-8}임을 알 수 있었다. 같은 방법으로 각각의 파라미터의 상대오차를 측정해 본 결과

$$\text{상대오차 } \sigma = \frac{\sigma - \sigma_r}{\sigma} = 10^{-4} \tag{13}$$

$$\text{상대오차 } \gamma = \frac{\gamma - \gamma_r}{\gamma} = 10^{-4} \tag{14}$$

$$\text{상대오차 } b = \frac{b - b_r}{b} = 10^{-4} \tag{15}$$

이었다. 표 3에 결과를 나타내었다. 본절의 실험 결과만을 고려해 볼 때 송·수신 당사자 외에 이산 카오스 모델의 비화통신의 견고성은 $10^{-8}\times10^{-4}\times10^{-4}\times10^{-4}=10^{-20}$의 전체 상대오차를 가지고 있음을 알 수 있다.

표 3. 파라미터 σ, γ, b와 샘플링 시간에 따른 상대오차
Table 3. Rate of error versus parameter σ, γ, b and sampling time Δt

동기 오차	파라미터 및 샘플링 시간	상대 오차
−140 dB 이하	Δt	10^{-8}
	σ	10^{-4}
	γ	10^{-4}
	b	10^{-4}
	total	10^{-20}

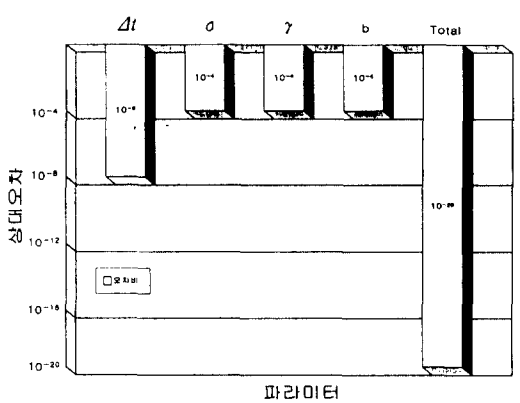


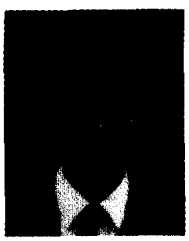
그림 11. 파라미터 σ, β, b와 샘플링 시간에 따른 상대오차
Fig. 11 Rate of error versus parameter σ, β, b and sampling time Δt

V. 결 론

본 논문에서는 카오스 현상을 통신 암호화에 적용시킨 이산 로렌츠 어트랙터를 기반으로한 카오스 모델을 제시하였다. 여러 가지 어트랙터의 특성 중에서 통신에 적용될 수 있는 특성으로는 우선 어트랙터의 안정성을 평가하는 것이고 그 다음이 송신측의 카오스 신호를 수신측이 발생시키는 카오스 동기에 관한 것이다. 이를 로렌츠 어트랙터를 이용한 통신 암호화 모델을 컴퓨터 모의 실험을 통하여 실험 고찰하여 암호화 능력을 평가하였다. 미분 방정식을 대신하여 카오스를 발생시키기 위해 사용한 수치 해석 방법은 테일러 급수를 토대로 4차 미분항까지만 계산하는 Runge-Kutta 4차법이며, 5차 이상의 미분값은 생략하였다. 실험결과 카오스가 발생하기 위해서는 샘플링 간격 Δt가 5×10^{-14} 이하면 가능하지만 송·수신 모델 간에 동기를 맞추기에는 매우 불안정하다. 두 시스템이 동기가 맞기 위해서는 샘플링 간격이 5×10^{-5}보다는 작아야 함을 실험을 통해서 알 수 있었다. 결국 송신측에서 보낸 메시지를 수신측에서 수신하기 위해서는 동기 오차가 적어도 −140 dB이어야 송신된 메시지를 수신측에서 검출 할 수 있다. 실험 결과를 통해 카오스의 여러 가지 특성을 살펴보면 카오스 신호가 송신하고자 하는 메시지의 크기보다 클수록 동기능력이 우수함을 알 수 있었고, 수신기의 송신기의 추적 과정은 샘플링 시간과 반비례 한다. 특히 본 논문에서 가장 핵심적인 사항으로서 송·수신 시스템의 동기 여부는 샘플링 시간과 밀접한 관계를 가지고 있다. 왜냐하면 오차에 민감한 카오스 신호는 결국 샘플링 간격이 작을수록 좋다. 동기가 이루어지기 위한 파라미터 범위는 각 $7<\sigma<30$, $33<\gamma<70$과 $1<b<6$ 임을 알 수 있었다. 송·수신 시스템의 파라미터 및 σ, γ, b는 각각 10^{-4}이였으며, 결론적으로 제안된 모델이 비화통신을 이룰 수 있는 전체 상대오차는 10^{-20}임을 알 수 있었다.

참 고 문 헌

1. L. M Pecora and T.L Carroll, "Synchoronization in Chaotic Systems," *Phy. Rev. Lett.* vol. 64, pp. 821-824, Feb. 1990.
2. —, "Driving System with Chaotic Signals," *Phys. rev.*, vol. 44, pp. 2374-2383, Aug. 1991.
3. T. L. Carroll and L. M. Carroll and Pecora, "Synchronizing Chaotic Circuits," *IEEE Trans. Circuits and Syst.*, vol. 38, pp. 453-456, Apr. 1991.
4. K. M Cuomo, A.V. Oppenheim and S. H. Isabelle, "Spread Spectrum Modulation and Signal Masking Using Synchronized Chaotic Systems," *MIT Res. Lab. Electron.*, TRn 570, Feb. 1992.
5. A. V Oppenheim, G.W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signal Processing in the Context of Chaotic Signals," in *Proc. IEEE ICASSP*, Mar. 1992.
6. K. M. Cuomo, A.V. Oppenheim and Steven H. Strogatz, "Synchronization of Lorens-Based Chaotic Circuit with Application to Communication," *IEEE Transactions on Circuit and Systems*, vol. 40, No. 10, pp. 626-633, Oct. 1993.
7. 合原一幸 , 德永蜂治, "카오스응용 전략," 성안당, pp. 198, 1995.
8. Stephen H. Kellert, "카오스란 무엇인가," (주) 범양사출판부, pp. 26-31, 1995.
9. Peter Grassberger and Itamar Procaccia, *Physica* D 9, pp. 189-208, 1983.
10. E. N. Lorenz, "Deterministic Nonperiodic Flow," *J. Atmospheric Science*, vol. 20, pp. 130-141, Mar. 1963.
11. S. H. Strogatz, *Nonlinear Dynamics and Chaos.* Addison-Wesley, pp. 366-369, 1994.
12. 지영준, 김화준, 허정권, "C로 구현한 수치해석," 높이깊이, pp. 285-291, 1993.
13. W. L. Ditto and M. Louis, "Mastering of Chaos," *Sci. Am*, pp. 62-68, Aug. 1993.
14. D. W. Jordon and P. Smith, *Nonlinear Ordinary Differential Equations.* New York:Oxford University Press, 1987, 2nd ed.
15. R. He and P. Vaidya, "Analysis and Synthesis of Synchronous Periodic and Chaotic Systems," *Phys. Rev A.*, vol 46, pp. 7387-7392, Dec. 1992.
16. K.M Cuomo and A.V. Oppenheim, "Synchronized Chaotic Circuits and Systemas for Communications," *MIT Res. Lab. Electron.* TR 575, Nov. 1992.
17. K.M Cuomo and A.V. Oppenheim, "Chaotic Signals and Systems for Communications," *Proc. IEEE ICASSP*, Mar. 1993.
18. K.M Cuomo and A. V Oppenheim, "Circuit Implementation of Synchronized Chaos with Applications to Communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65-68, July. 1993.
19. L. Kocarev, K. Halle, K. Eckert, and L. Chua, "Experimental Demonstration of Secure Communication via Chaotic Synchronization," *Int. J. Bifucation Chaos*, vol. 2, pp. 709-713, Sept. 1992.



박 철(Chul Park) 정회원

1993년 2월:광운대학교 전자통신공학과 졸업(공학사)
1996년 2월:광운대학교 대학원 전자통신공학과 졸업(공학석사)
1994년 1월~1996년 8월:호서전문학교 전임강사
1997년 1월~현재:가산전자 연구원
※주관심분야:영상통신, 데이터 압축, 패턴인식.

김 영 태(Young Tae Kim) 정회원

1991년 2월:광운대학교 전자통신공학과 졸업(공학사)
1993년 2월:광운대학교 대학원 전자통신공학과 졸업(공학석사)
1993년 3월~현재:광운대학교 대학원 전자통신공학과 박사과정
※주관심분야:영상통신, 데이터 압축, 패턴인식.

고 형 화(Hyung Hwa Ko) 정회원

광운대학교 전자통신공학과 교수
한국통신학회 논문지 제22권 제4호 참조