논문 99-24-6T-17 한국통신학회논문지 '99-6 Vol.24 No.6T

HVPM에 의한 카오틱 신호 발생기와 카오틱 랜덤 시퀀스 특성

정회원 이 익 수*, 김 형 락*, 이 동 록*, 송 규 익**

The Properties of Chaotic Random Sequence and Chaotic Signal Generator by HVPM(Hyperchaos Volume Preserving Maps)

Ik-Soo Lee*, Hyung-Rag Kim*, Dong-Rok Lee*, Kyu-Ik Sohng** *Regular Members*

요 약

본 연구에서는 기존의 단순한 카오스 현상을 나타내는 수식을 기초로 하여 암호시스템이나 PN(pseudo-noise) 시퀀스에 적용하기 위한 카오스 발생수식을 제안한다. 단계별로 모듈러(modulus) 함수를 사용하여 다양한 카오틱 신호(chaotic signal)를 발생시키기 위하여 이산시간(discrete-time) 하이퍼카오스 VP 사상(HVPM, hyperchaos volume preserving maps)을 제안하여 아날로그 형태의 카오틱 시퀀스(CAS. chaotic analog sequence)와 이를 이진화한 카오틱 시퀀스(CBS, chaotic binary sequence)에 대한 특성들을 분석하였다.

일반적인 非線型(nonlinear) 신호처리 기법들을 이용한 수치해석에서 카오틱 신호가 갖는 비주기성(aperiodicity), 양(+)의 리아푸노프(positive Lyapunov), 전 위상공간(phase space)를 채우는 특이한 어트랙터(attractor) 등의 카오틱 신호가 갖는 특징들을 가지는 것을 확인할 수 있었다. 또한 발생된 카오틱 신호들을 아날로그 및 디지털 형태의 코드로 변환하여 구한 상관(correlation) 함수값이 기존의 PN 시퀀스와 같은 특징을 가지며, HVPM이 생성하는 카오틱 신호를 통계적으로 분석한 분포도는 균일(uniform)분포를 나타내었다.

ABSTRACT

In this paper, we have proposed a novel chaotic generation equation for generating chaotic signals such as pseudo-random sequences. We accomplish this by discrete time HVPM(hyperchaos volume preserving maps) which leads to CAS(chaotic analog sequence) and CBS(chaotic binary sequence) data.

The chaotic signals of HVPM which is used specific parameters space are analyzed by general nonlinear signal process methods. The chaos signals that are calculated numerical and statistical process with computer simulation have proved chaos properties; aperiodicity, positive Lyapunov, special chaos attractor etc. And the chaotic PN sequence(CPNS) of analog and binary types which is coded by the chaotic sequence, that can be extracted from a 3-dimensional discrete time chaotic generation equation(3D2CGE) for generating various chaotic signals. We have tested a correlation function and the degree of statistical independence of each CPNS that is evaluated in order to apply to spread spectrum communication. Experimental results show that the proposed CPNS codes are used for the spreading sequence and secure communication codes.

* 포항1대학 정보통신과
** 경북대학교 전자전기공학부
논문번호 : 99016-0412, 접수일자 : 1999년 4월 12일
※ 본 연구는 1998년 한국학술연구재단의 연구비 지원에 의해 수행되었음.

I. 서 론

최근 카오틱 신호는 안전통신(secure communication)에 적당하다고 연구되고 있다[3-6]. 카오스 시스템에서 변수들을 변화시킴으로서 다양한 카오스 동적(dynamic) 특성과 예측이 불가능한 신호를 발생시킬 수 있다[1]. 또한 카오틱 신호는 광대역 전력 스펙트럼(broad-band power spectrums) 특성과 초기상태에 민감한 특징을 보인다. 이러한 카오틱 신호는 랜덤(random) 신호의 성질과 비슷하며, 특정 신호처리의 분석공격에도 방어된다.

카오스 시스템(chaos systems)을 동기화시키는 구성들이 많이 제안되었고, 이것을 비화통신 및 암호통신에 적용하려는 시도가 활발히 진행되고 있다[4,8]. 대부분의 제안들(schemes)은 구동(drive) 또는 전송(transmit) 시스템에서 카오틱 캐리어(chaotic carrier) 또는 파라메터(parameter) 변조기법을 이용하여 정보신호를 마스킹(masking)하여 통신을 한다. 그러나 기존의 단순한 카오틱 신호는 안전한 시퀀스(secure sequence)로 직접 사용할 수 없다. 의도된 측정자(motivated observer)가 충분한 카오스 정보를 획득하면 쉽게 재구성(reconstruction)할 수 있다. Short, Pérez와 Cerderia 등은 이러한 카오스 암호 시스템의 구성들은 안전하지 않으며, 역마스킹(unmasking)의 예측기법(prediction techniques)을 이용하면 신호를 복호할 수 있다고 발표했다[14]. 또한 일반적인 카오스 시스템을 사용할 경우에는 위상공간에서 전형적인 패턴이나 어트랙터가 나타나므로 신호를 역마스킹하는데 도움을 주며, 상관함수가 매우 긴 시간에 낮은 값을 갖는 경우에는 전송된 신호를 예측하는데 유리하다고 알려져 있다. 그리고 기존의 카오스 시스템은 회로구현이 어려우며, 보통 한 개의 리아푸노프 지수를 갖는 단점이 있다. 따라서 카오틱 신호는 아직 고도의 안전성을 제공하지 못하므로, 다중 카오스 발생원(multiple chaos sources)을 사용해야 한다고 제안하였다[14].

한편, 주파수확산통신(spread spectrum communication) 기술은 확산 시퀀스(spreading sequence) 또는 PN(pseudo-noise) 시퀀스에 기인한다. 지금의 PN 시퀀스는 Gold 시퀀스 또는 Kasami 시퀀스와 같은 LFSR(linear feedback shift registers)를 이용하여 여러 가지 종류의 시퀀스를 발생시키고 있으며, 지난 수십 년간 통신, 항해 및 관계된 시스템에서 성공적으로 사용되어 왔다[7]. CDMA 시스템에서 코드를 인식하기 위해 다른 PN 시퀀스를 가지고 있는 사용자(users)는 동시에 같은 주파수 대역으로 SS(spread spectrum) 신호를 전송할 수 있고, 복조시에는 같은 PN 시퀀스를 사용하여 원하는 신호를 복호한다. 그러나 이러한 기존의 PN 시퀀스는 종류(families)와 크기(sizes)가 다양하지 않다는 것이 단점이며, 통신에서 정보보호나 암호화 시스템 응용될 때에는 문제가 된다. 또한 미래에 주파수 확산통신의 수많은 사용자(users)의 수요를 충족시킬 수 있는지에 대한 의문이 남는다. 실제 PN 시퀀스의 상호상관 값이 영이 아니므로, 채널간의 간섭(co-channel interference)이 발생하여 동시에 통신할 수 있는 사용자를 제한한다. 따라서 채널간의 상호간섭을 줄이고, CDMA의 통신성능(capacity)을 향상하기 위해서는 발생된 PN 시퀀스가 좋은 상관(correlation) 특성을 가져야 하며, 빠른 PN 코드의 획득(fast acquisition)과 고도의 안전성(high level security) 등을 가져야 한다[8,9].

카오틱 신호는 랜덤신호와 같은 특징으로 인하여 가상랜덤수 발생기(pseudo-random number generator)의 가능성을 부여해 주며, 안전통신에 적용이 가능할 것이다. 최근의 연구 논문에 의하면 카오스 비선형 사상(chaotic nonlinear mapping)에 기초한 PN 수열은 기존의 Gold 또는 Kasami 계열의 최대값과 비교하여 성능이 떨어진다고 알려져 있다[8]. 그럼에도 불구하고 카오스 시스템을 기반으로 한 랜덤수를 이용한 PN 시퀀스의 발생 방법에는 몇 가지 장점이 있다. 우선 다양한 PN 시퀀스의 발생이 쉽고, 암호통신에서 비밀키(secret key)로 사용할 수 있는 파라메터들을 변화시켜 다양한 형태의 동적응답을 만들 수 있다. 이렇게 함으로서 임의 수열(sequence, family)의 크기와 주기를 변화시켜 다양한 랜덤수나 PN 시퀀스를 발생시킬 수 있다[10-13].

본 연구에서는 이러한 기존의 카오스 시스템이 갖는 단점을 극복하고 단순한 카오스 현상을 나타내는 것을 기초로 하여 모듈러(modulus) 함수를 사용하여 다양한 카오틱 신호를 발생시키기는 하이퍼 카오스 수식을 제안한다. 아날로그 형태의 카오틱 신호와 이를 이진화한 카오틱 신호에 대한 통계적으로 다양한 특징들을 분석하였다. 본 논문의 구성을 보면, II절에서 HVPM에 대하여 설명하고, III절에서는 제안한 3D^{2}CGE를 이용하여 수치실험한 결과를, IV절에서는 CAS와 CBS에 대하여 상관특성을 분석하여 PN 시퀀스로의 사용이 가능함을 나타내었다.

Ⅱ. HVPM의 모델링

기하학적 관점에서 카오틱 사상(chaotic map)은 단순한 'n'차 비선형 함수를 선형사상(linear mapping)으로 하여 계속적인 순환 피드백(recursive feedback)으로 카오스 신호를 발생시킬 수 있다. 이때의 핵심 메커니즘은 팽창(stretching, expansion)과 축소(folding, contraction)의 계속적인 반복에 의한 것이다[1].

본 연구는 특히 암호통신(private and secure communication)에 적합하고, 동기화 구현이 가능한 카오스 동적시스템을 구축하기 위한 기반 연구로 카오틱 신호를 발생시키는 모델을 제안하는데 중점을 둔다. 따라서 추구할 카오스 시스템은 다음과 같은 바람직한 신호특성을 가져야 한다.

① 상태공간에서 일정한 패턴이나 어트랙터(attractor)를 가지지 않아야 한다.
② 매우 짧은 기간에 상관(correlation) 값이 '0'를 가져야 한다.
③ 스펙트럼이 전 주파수 대역에 걸쳐 확산분포해야 하며, 낮은 확률분포에 의해 신호 예측이 불가능해야 한다.
④ 두개 이상의 리아푸노프 지수(Lyapunov exponet)를 가지는 시스템, 즉 하이퍼카오스 (hyperchaos) 시스템이어야 한다.
⑤ 카오스 시스템이 전송된 신호에 동기화가 가능해야 한다.
⑥ 매우 빠른 시간에 동기화가 진행되어야 하며, 잡음신호에 민감하지 않아야 한다.
⑦ 비선형 형태로 정보신호가 카오스 캐리어(chaotic carrier)와 더해져야 한다.
⑧ 시스템 설계 및 구현이 용이하고, 분석이 가능해야 한다.

본 연구에서는 일정 방향으로 확장과 축소를 수행하여 지역적으로 'VP(volume preserving)'를 이루고, 접힘(folding) 함수는 모듈러 함수를 이용하여 방향성을 갖지 않는 사상으로 하이퍼카오틱(hyperchaotic) 신호를 발생시키는 시스템을 제안하려고 한다. 그리하여 위의 모든 특징들을 갖는 카오틱 신호를 발생시키기는 어렵지만 상당부분에 적합한 카오틱 신호를 발생시킬 수 있다.

선형변환(linear transformation) 'L'은 팽창함수(EF, Expansion Function)가 되며, 사상 'x(n+1)=Lx(n)'에 의해 카오스 신호를 발생시킨다. 그리고, 접힘함수(FF, Folding Function) 'F(x)=($x_1$mod$k$, $x_2$mod$k$, $x_3$mod$k$, ...,$x_n$mod$k$)'를 사용하면 위상공간(phase space) 'R_n'에서 영역 [$-m_i$, m_i]에 제한된 신호가 된다. 이러한 과정은 모듈러(modulus) 함수를 사용한 것으로 잘 알려진 'Bernoulli Shift Map'과 같은 기하학적 특성을 갖는다. 기존의 잘 알려진 카오스 신호를 발생시킬 수 있는 수식을 기초로 하여 복잡하면서도 다양한 카오스 현상을 발생시킬 수 있는 수식을 설계하였다. 제안한 식 (1)을 3차 이산시간 카오스 발생수식(3-dimensional discrete-time chaotic generation equation, 3D^{2}CGE)으로 모델을 정하였다. 이 수식은 카오틱 신호의 값들을 제한된 영역에서 계속적인 순환루프(recursive loop)를 수행하도록 모듈러(modulo) 함수를 사용하였으며, 3차원 카오틱 신호가 나타나도록 차분방정식으로 나타내었다.

$$\left.\begin{aligned} x(n+1) &= \alpha x(n)+\beta y(n)+\gamma z(n) \\ y(n+1) &= \varepsilon x(n)+\lambda y(n)+\mu z(n) \end{aligned}\right\}$$
$$z(n+1) = \rho x(n)+\sigma y(n)+\upsilon z(n)$$
$$(\zeta \pm a) \bmod b \mp c \qquad (1)$$

모듈러 함수는 'modulus shift'로 처리되며, 'tent map'이나 'Bernoulli map'에서 처럼 'folding' 함수를 응용하였다. 여기서 '(ζ+a) mod b - c'의 의미는 매번 x(n), y(n), z(n) 신호에 'a'를 더하고 'b'로 나눈 나머지를 'c'로 뺀 후에 x(n+1), y(n+1), z(n+1)의 신호를 발생시킨다. 이러한 모듈러 함수는 다음 그림 1과 같다.

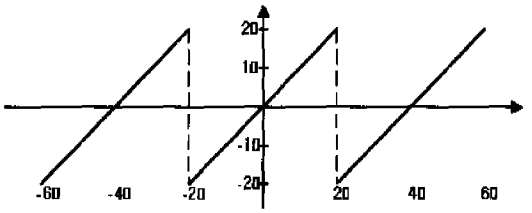


그림 1. 모듈러(modulo) 함수

제안한 식 (1), 즉 HVPM(Hyperchaos Volume Preserving Maps)을 이용한 카오스 발생수식에서 'x(n+1)', 'y(n+1)', 'z(n+1)'의 항은 'x(n)', 'y(n)'과 'z(n)' 값들의 선형조합으로 하여 구성할 수 있으며,

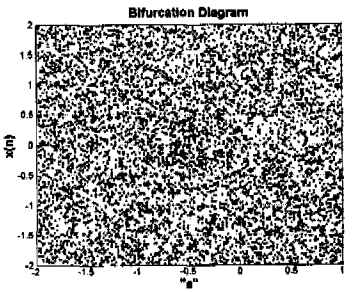
'α', 'β', 'γ', 'ε''λ', 'μ', 'ρ', 'σ', 'υ' 등은 카오스 상태를 변화시킬 수 있는 파라메터들로서 다양한 동적응답(dynamic response)를 보인다. 그리고, 각각의 'n' 시간, 즉 이산시간에는 순환루프(recursive loop) 형태로 카오틱 신호를 발생시킨다.

Ⅲ. 3D^{2}CGE의 수치해석

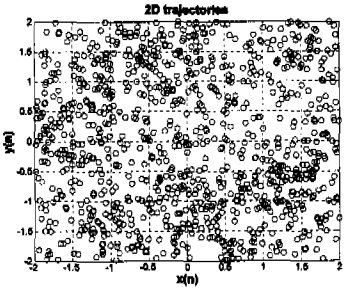
제안한 3차 이산시간 카오스 발생수식(3-dimensional discrete-time chaotic generation equation, 3D^{2}CGE)을 컴퓨터를 이용하여 비선형 동력학(nonlinear dynamics) 신호처리 기법을 바탕으로 카오스 상태의 동적응답을 수치해석(numerical analysis)으로 분석하였다.

식 (1)에서 제어 파라메터 -'α'는 -4/3, 'β'는 1.0, 'γ'는 0.0, 'ε'는 0.0, 'λ'는 1.0, 'μ'는 1.0, 'ρ'는 1.0, 'σ'는 1.0, 'υ'는 0.0- 값에 대하여 'x(n)', 'y(n)', 'z(n)' 등의 상태가 카오스 상태가 된다. 동력학 시스템에서 상태의 안정성을 판별하는데 리아푸노프 지수(Lyapunov exponent)가 자주 사용된다. 리아푸노프 지수는 초기값(initial values)들이 정상상태에서 어떠한 영향을 미치는가 하는 정도를 측정하는 것으로, 보통 지수의 값이 '0'이하일 때에는 안정한 주기상태가 된다. 리아푸노프 지수값이 양(positive)의 값일 때에 카오스 상태로 간주할 수 있다. 제안한 카오스 사상에서 발생된 카오스 시간파형을 분석하여 Lyapunov 지수값을 구하면 (0.6829, 0.3023, -0.9852)가 되고, 여기서 보면 두 개의 지수값이 양(+)이므로 하이퍼카오스(hyperchaos) 시스템이 된다. 그리고 지수값을 모두 더하면 '0'이 된다는 것은 지역적으로 제한된 영역에서 동작한다는 VP(volume preserving) 사상을 나타낸다는 것을 가르킨다.

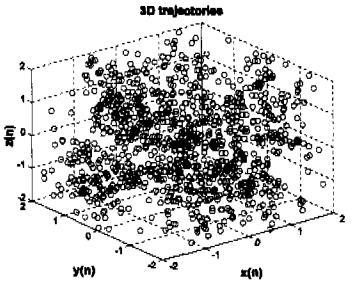
그림 2의 (a)는 파라메터 'α'의 변화에 대하여 카오스 상태의 출력 'x(n)'을 나타낸 것으로 전형적인 분기(bifurcation)구조는 보이지 않고 불규칙한 카오스 구조가 내재 되어있는 형태와 구조가 보인다. 또한 그림 2의 (b)와 (c)는 위상공간에서 '1000'개의 상태를 '2D'와 '3D'로 표현한 것으로 전형적인 카오스 어트랙터(chaotic attractor) 구조와는 다른 위상공간 전지역에 걸쳐 흩어져 균일한(uniform) 분포를 보인다. 이것은 기존의 'Logistic map', 'Lorenz attractor' 등의 카오스 어트랙터와는 달리 일정한 패턴을 형성하지 않아 카오스 상태를 예측하기가 어렵게 된다는 것을 나타낸다.



(a) 분기구조



(b) 2D 어트렉터



(c) 3D 어트랙터

그림 2. 3D2CGE의 카오스 시간파형과 어트랙터

카오스 신호의 중요한 특징은 초기값에 매우 민감한 특성을 보이며, 긴 시간(long-term)에 대해서는 예측이 불가능하게 된다. 즉 처음에 매우 근접한 초기값을 갖는다고 할지라도 몇번의 순환(iteration) 후에는 완전히 다른 특성을 갖는 신호가 발생된다는 것이다.

그림 3은 동일한 파라메터 변수들을 가진 3D^{2}CGE에서 'x(n)', 'y(n)', 'z(n)' 등이 모두 '0.0001=10^{-4}'의 차이로 할당한 2개의 신호가 반복계산 후에 나타나는 'x(n)'의 두 신호의 형태를 보여주고 있다. 대략 '15'번의 반복 후에 차이를 보이기 시작함을 알 수 있다. 카오스 시스템에서 이러한 급속한 초기값의 민감성은 무수한 초기값의 선택과 더불어 제안한 3D^{2}CGE의 제어 파라메터들은 랜덤수(random number) 발생시의 랜덤시드(random seed)로 간주하여 각각의 값들을 변화시켜 무수히 많은 랜덤신호를 얻을 수 있다.

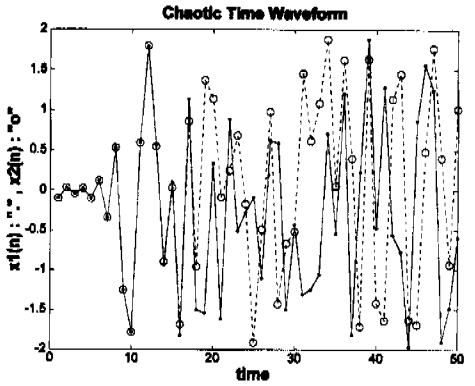


그림 3. 두 초기값의 변화에 대한 카오틱 신호

이렇게 발생된 카오스 상태의 시간파형(time waveform)을 주파수(frequency) 스펙트럼으로 분석하면 신호의 주파수는 넓은 대역에 전력이 분포하며 균일(white)한 광대역 스펙트럼(broad-band spectrum) 형태를 가진다. 그림 4는 위의 파라메터로 설정하고 시간파형을 '4096' DFT(Discrete Fourier Transform)로 진폭 스펙트럼을 나타낸 것이다. 이러한 광대역 신호, 즉 카오틱 신호가 통신에서 반송파(carrior)로 사용될 경우에 신호의 주파수 분포를 전송대역에 확산시키는 주파수확산(spread spectrum) 통신에 사용이 가능할 것이며, 통신 사용자들에게 확산부호(spreading code)로 할당하여 사용이 가능해질 것이다.

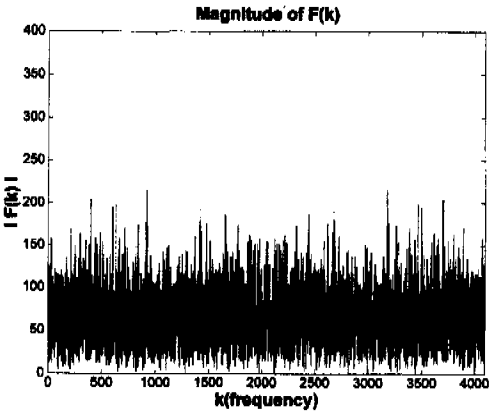


그림 4. 카오틱 신호의 주파수 스펙트럼

그리고 3D^{2}CGE에 의해 발생시킨 '40,000' 이산값에 대하여 'x(n)' 데이터의 분포도(distribution degree)를 그림 5에 나타내었다. 통계적으로 분석한 결과, 평균값(M)은 '(0.005, 0.0035, 0.0042)'이며 표준편차(σ)의 값은 '(1.1700. 1.1492, 1.1569)'로 되었다. 특정값의 분포정도가 높은 부분이 있으나, 확대한 특정 구간에서도 균일한 분포(uniform distribution)를 나타낸다. 그리고 이러한 균일 분포도는 카오스 시스템의 파라메터 값을 변화시킴으로서 쉽게 바꿀 수 있다.

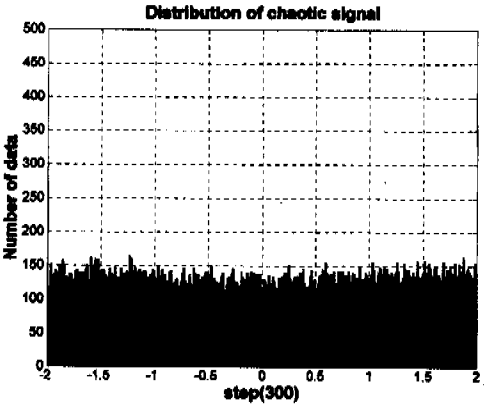


그림 5. 아날로그 카오틱 신호의 분포도

Ⅳ. CAS와 CBS의 분석

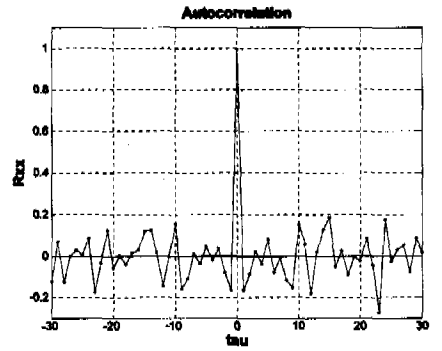
본 연구에서 제안한 3D^{2}CGE에서 발생된 카오스 시퀀스를 확산부호로서의 사용이 가능한지, 또는 PN 시퀀스의 보편적인 특징들을 만족하는지에 대한 수치실험을 행했다. 먼저, 카오스 비선형 사상(chaotic nonlinear maps)에 기초로 하여 임의의 시드(seeds)로 다양한 형태의 비주기적인 아날로그 카오스 PN 수열을 적당한 주기 'T'로 구간을 나누어 발생시킨다. 그리고 발생한 CAS(chaotic analog sequence) 쌍(pair)들을 자기상관(autocorrelation) 및 상호상관(crosscorrelation)의 함수값을 구하여, 확산코드로서 사용할 수 있는지에 대하여 성능을 계산하였다. 수치실험에서 먼저 아날로그 카오스 신호 형태 자체로 상관관계를 분석한다. 기존의 암호(cryptography) 시스템은 유한필드(finite fields) 또는 모듈(modules)에 의한 정수연산을 디지털시스템으로 구현하여 사용하였다. 그러나 카오스 시스템의 파라메터나 상태값들이 아날로그 형태로 표현되므로 카오스 시퀀스 자체를 응용한 시스템의 기초 연구를 위하여 상관관계를 분석하였다. 아날로그 신호 자체를 이용할 경우는 정보의 정확한 복호(recovery)가 필요치 않는 시스템에 적용될 수 있을 것이다. 그 이유는 아날로그 시스템의 구현시에 발생하는 시스템 파라메터 또는 온도 등의 작은 편차

(deviation)가 불가피하므로 정확한 정보의 암호화(encoder) 및 복호화(decoder)가 불가능하기 때문이다.

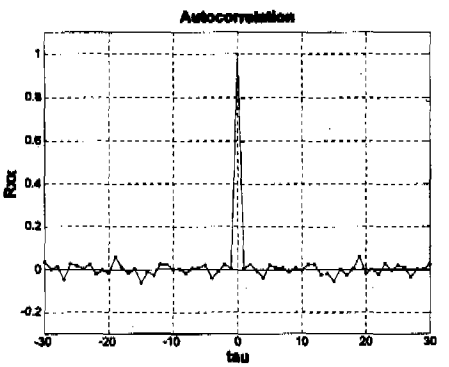
주파수확산 시스템에서 PN 시퀀스는 신호의 전송 대역폭(transmission bandwidth)을 넓히며, 같은 전송 대역폭에 다른 많은 가입자(user) 신호를 분리하기 위한 다중접속(multiple-access)을 위하여 이용되고 있다. 이때 사용하는 확산 PN 코드는 자기상관(auto-correlation) 함수값이 영지연(zero-delay)일 때 높으며, 그 이외의 지연시간에서는 거의 '0'에 가까운 특성을 가진다. 또한 상호상관(cross-correlation) 함수값은 모든 지연시간에 대하여 낮은 상관값을 가져야 채널간의 간섭이 적어진다.

3D^{2}CGE에서 다양한 주기로 카오스 시퀀스를 발생시킬 수 있으며, 주기가 다른 이산시간 카오스 신호는 'n' 시간에 계속적인 비선형 계산으로 발생이 가능하며, 상관함수 값 '$R_{xx}(h)$'은 다음의 식 (2)로 구할 수 있다.

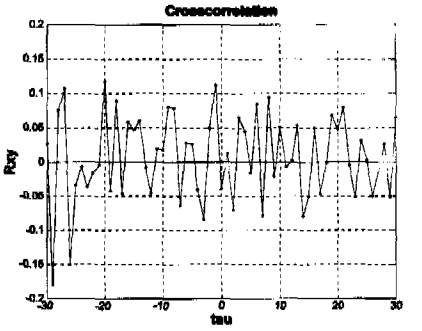
$$R_{xx}(h) = \frac{1}{N}\frac{\sum_{i=0}^{N}[x(i)-M][x(i+h)-M]}{\sigma^2} \qquad (2)$$



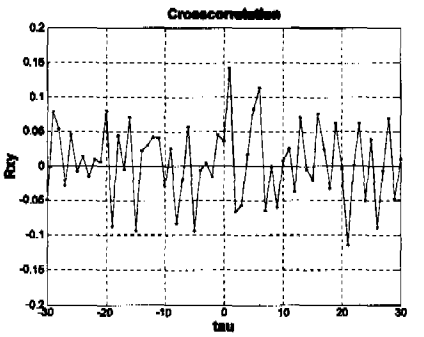
(a)



(b)



(c)



(d)

그림 6. 카오틱 아날로그 시퀀스(CAS)의 상관함수 값

그림 6의 (a)와 (b)는 동일한 파라메터와 초기값으로 발생된 자기상관 함수를 표현한 것이다. (a)는 '100', (b)는 '1000'의 카오스 시퀀스 길이(sequence length)로 자른 신호를 나타낸 것으로 상관함수에 기여하는 신호의 길이 또는 점(point)가 증가함으로서 자기상관의 특성이 양호하다는 것을 알 수 있다. 그림 6의 (c)는 동일한 파라메터값에 초기값을 달리한 신호에 대하여 그리고 (d)는 파라메터값을 달리한 신호간의 상호상관 함수값을 도시한 것이다. 종래의 랜덤신호의 상관값(correlation value)과 유사한 특성을 보인다. 즉, 근접한 초기값의 변화에 의한 신호들 상호간에 상관되지 않고 PN 코드 계열의 상관특성과 유사함을 알 수 있다. 이것은 'VP' 시스템의 특징으로 초기값의 팽창과 축소함수에 의해 급속하게 서로의 연관성을 상실한다는 것을 나타낸다. 그리고 실제 통신시스템 구현시에 상호상관 값이 적을수록 신호간 간섭의 정도가 작아 다중접속에 유리하다.

3D^{2}CGE을 정확한 계속적인 소수 계산과정을 거치면, 무한한 주기를 가진 랜덤한 아날로그 카오스 신호로 변환된 값이 된다. 이러한 형태의 신호를 디

지털 통신에 확산부호로 사용하기 위해서는 아날로그 신호를 이진값(binary value)으로 변환하는 과정이 필요하다. 그리고 실제 시스템에 적용될 때에는 유한 소수점 계산과 주기 'T'로 제한하여 사용하며, CDMA과 같은 주파수확산 통신시스템에서는 이진(binary) 코드 형태로 사용된다.

그림 7은 카오틱 아날로그 시퀀스(CAS)와 이진화를 수행한 카오틱 이진 시퀀스(CBS, chaotic binary sequence) 결과를 나타내었다. 아날로그 형태의 '40,000' 카오스 시퀀스를 분석하여 평균(Average, M)을 먼저 구하고, 'M'값을 문턱값(threshold)으로 하였다. 출력은 '±1'로 이진화(binarization)를 행한 과정은 다음의 식 (3)과 같다.

$$b_n = \begin{bmatrix} -1 & \text{for } x(n) \le M \\ +1 & \text{for } x(n) > M \end{bmatrix} \qquad (3)$$

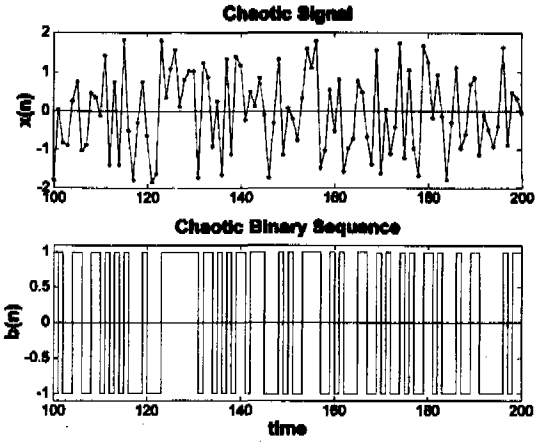


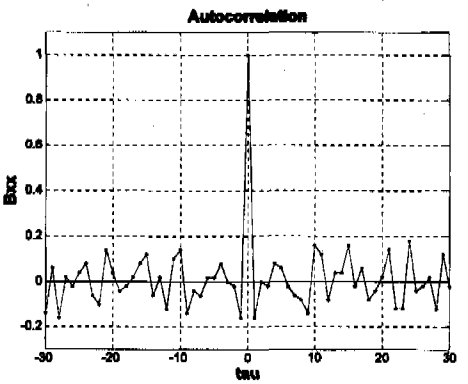
그림 7. 카오틱 신호와 CBS 파형

주파수확산시스템(spread-spectrum system)에 사용되는 PN 시퀀스는 실제 랜덤이 아니며, 결정적이고 주기적인 시퀀스이다. 그러나 이상적인 PN 시퀀스는 이진화('1', '0')된 신호의 상대적인 빈도수가 같아야 하며, '11'과 '00'와 같이 길이가 '2'로 연속된 비율이 '25[%]', '111' 또는 '000'의 연속된 비율이 '12.5[%]' 정도로 분포해야 한다고 한다. 따라서 본 실험에서 '40,000' 시간에 이진화를 행한 카오스 이진 시퀀스 데이터를 분석한 결과를 표 1에 나타내었다. 이러한 상대적인 데이터의 분포도와 CBS의 상대적 코드 비율은 확산코드로 사용될 때 신호의 성질을 나타낸다. 또한 초기값과 카오스 시스템의 이득을 변화시킴으로 인하여 다양한 형태의 시퀀스 비율로 변화시킬 수 있다.

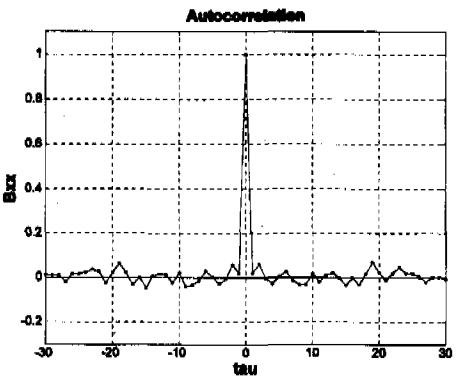
표 1. 카오틱 이진 시퀀스의 코드 비율

연속 bit 종류		개수 [비율 (%)]	
1	0	20,003 [50.0]	19,997 [50.0]
11	00	4790 [11.96]	4760 [11.90]
111	000	2554 [6.39]	2563 [6.41]
1111	0000	1417 [3.54]	1420 [3.55]

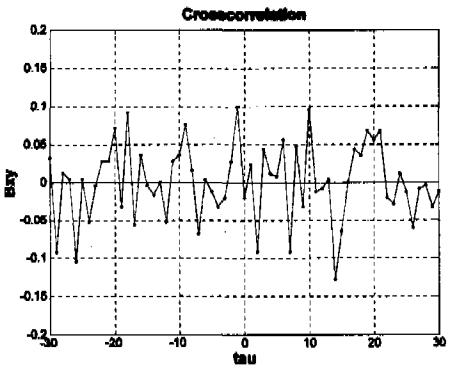
다음 그림 8은 카오스 이진 시퀀스로 자기상관 및 상호상관값을 구한 것이다. 전체적으로 보면 상관함수에 기여하는 시퀀스의 길이(sequence length) 또는 점(point)가 증가함으로서 상대적으로 영 지연 시간에서의 자기상관의 값이 큼을 알 수 있다. 그리고 파라메터값과 초기값을 달리한 신호에 대하여 상호상관(cross-correlation) 함수값이 작다는 것을 나타낸 것이다. 전절의 아날로그 카오틱 시퀀스의 상관값(correlation value)과 유사한 특성을 보이는 것을 것을 알 수 있다.



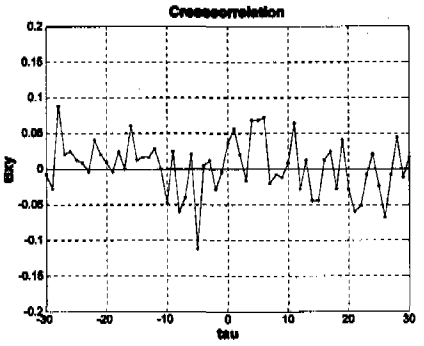
(a)



(b)



(c)



(d)

그림 8. 카오틱 이진 시퀀스(CBS)의 상관함수 값

따라서, 본 연구에서 제안한 카오스 수식을 이용하면 다양한 카오스 신호를 얻을 수 있으며, 이러한 카오스 신호를 이진화하여 PN 코드로 사용할 경우에 주기가 무한대이므로 임의의 주기 길이로 선택할 수 있으며, 빠른 시간에 확산코드를 만들 수 있다. 위와 같은 특징들을 주파수확산 통신에 응용될 경우 확산코드로 다양한 PN 코드를 얻을 수 있으며, 카오스 신호를 이용함으로 인하여 정보보호를 할 수 있는 장점을 가지는 시스템으로의 응용이 가능할 것이다.

V. 결 론

본 연구에서는 모듈러(modulus) 함수를 사용하여 다양한 카오틱 신호를 발생시키기 위하여 HVPM을 제안하여 아날로그 및 디지털 형태의 카오틱 시퀀스에 대한 특징들을 분석하였다. HVPM에서 발생된 카오스 신호를 위상공간에 표현하면 일정한 어트랙터 패턴이 나타나는 것이 아니라, 어떤 집단점(clustering points)에 모이지 않고 랜덤 데이터와 같이 위상공간에 흩어져 위상공간을 채우는 것을 볼 수 있었다. 이러한 모듈러 함수에 의해 발생된 신호는 광대역 전력스펙트럼(broad-band power spectrum)을 가지며, 자기상관함수 값도 빠른 시간에 '0'로 되었다. 또한 통계적으로 분석한 분포도는 균일(uniform)분포를 나타내었다.

제안한 수식과 카오스 시스템을 전자회로로 구현이 가능하며, 구현된 회로상에서 동기화가 앞으로 수행되어야 한다. 아날로그 카오스 회로는 모든 시간에 대하여 속도가 빠르고, 특정 비주기적인 상태에서는 간단히 회로로 구현이 가능하지만, 파라메터의 매칭(matching)에 문제가 있고 특정 파라메터값은 디지털 회로 구현이 불가능하며, 데이터 재현성(reproducibility)에 어려움이 있다. 따라서 'n'차 비선형 사상은 아날로그 블록으로 만들고, 모듈러 함수는 디지털 타입으로 만들어 디지털 회로와 연결이 가능하도록 하고 외부 클럭에 동작하도록 하여 전체적으로 디지털 카오스회로를 구현하도록 연구가 진행되어야 한다.

참 고 문 헌

[1] Aihara, Chaos 이론의 기초와 응용, Science, 1990.

[2] 한국통신학회, 정보통신 : CDMA특집, 한국통신학회지, 제13권, 4호, 1996.

[3] U. Parlitz, S. Ergezinger, "Robust communication based on chaotic spreading sequences," Physics Letters A 188, pp.146-150, 1994.

[4] Tao Yang and Leon O. Chua, "Secure Communication via Chaotic Parameter Modulation," IEEE Trans. Circuits Syst., Vol.43, No.9, Sept. 1996

[5] K. M. Cuomo and A. V. Oppenheim, "Circuits implementation of synchronized chaos with applications to communcations," Phys. Rev. Lett. *Vol.* 71, No. 1. pp.65-68, 1993.

[6] U. parlitz and S. Ergezinger, "Robust communication based on chaotic spreading sequences," Phys. Rev. *A188*, 146-150, 1994.

[7] R. L. Pickholtz, D. L. Schilling and L. B. Milstein, "Theory of spread-spectrum communications-A tutorial," IEEE Trans. Comm., Vol. COM-30, No.5, pp. 855-884, May 1982.

[8] T. Kohda and A. Tsuneda, "Pseudonoise

sequence by chaotic nonlinear maps and their correlation properties," IEICE Trans. Commun., Vol. E76-B, No. 8, pp. 855-861, Aug. 1993.

[9] R. Kohno, "Pseudo-noise sequences and interference cancellation techniques for spread spectrum systems," IEICE Trans., Vol. E74, No. 5, pp. 1083-1991, May 1991.

[10] L. O. Chua, Y. Yao and Q. Yang, "Generating randomness from chaos and construction chaos with desired randomness," Int. J. Circuit and Applications, vol. 18, pp. 215-240, 1990.

[11] 김남선, 한영렬, "직접 확산 스펙트럼통신을 위한 Chaotic Sequence의 상관특성," 韓國通信學會論文誌 '95-1 Vol.20 No.1, pp. 45-54, 1995.

[12] G. M. Bernstein and M. A. Lieberman, "Secure random number generation using chaotic circuits," IEEE Trans. Circuits Syst., vol. 37, No. 9, pp. 1157-1164, Sept. 1990.

[13] Z. Hong and L. Xieting, "Generating chaotic secure sequences with desired statistical properties and high security," Int. J. Bifurcation and Chaos, Vol. 7, No. 1, pp. 205-213, 1997.

[14] Kevin M. Short, "STEPS TOWARD UNMASKING SECURE COMMUNICATIONS," International Journal of Bifurcation and Chaos, Vol.4, No.4 pp.959-977, 1994.

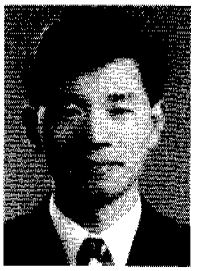
이 익 수(Ik-Soo Lee) 정회원

1968년 9월 24일생
1991년 : 경북대학교 전자공학과 졸업(공학사)
1994년 : 경북대학교 대학원 전자공학과 졸업(공학석사)
1996년 : 경북대학교 대학원 전자공학과 회로계통전공 박사과정 수료
1996년~현재 : 포항1대학 정보통신과 조교수
<주관심 분야> 회로설계 및 제어시스템, 신경회로망 퍼지이론, 카오스 이론 및 하드웨어

이 동 록(Dong-Rok Lee) 정회원

1961년 7월 5일생
1986년 : 경북대학교 공대 전자공학과 졸업(공학사)
1991년 : 경북대학교 산업대학원 졸업(공학석사)
1986년~1993년 : 한국전자(주) 종합연구소 선임연구원
1993년 ~ 현재 : 포항1대학 정보통신과 조교수
<주관심 분야> 반도체소자 설계 및 공정, 소자 모델링 및 시뮬레이션

김 형 락(Hyun-Rag Kim) 정회원



1967년 3월 14일생
1992년 : 경북대학교 전자공학과 (학사)
1994년 : 경북대학교 대학원 전자공학과(석사)
1997년 : 경북대학교 전자공학과 정보통신공학 전공 (박사과정)
1994년 : LG전자기술원 영상미디어 연구소 연구원
1995년 : (주)문화방송 기술연구팀 연구원
현재 : 포항1대학 정보통신과 조교수
<주관심 분야> 채널 코팅, 암호화

송 규 익(Kuy-Ik Sohng) 정회원

1952년 8월 15일생
1975년 : 경북대학교 전자공학과 졸업(공학사)
1977년 : 경북대학교 대학원 전자공학과 졸업 (공학석사)
1977년~1982년 : 국방과학연구소 연구원
1990년 : 일본 동북대학교 대학원 전자공학과 졸업 (공학박사)
1983년~현재 : 경북대학교 전자전기공학부 교수
<주관심 분야> 비디오 공학, 음향공학, 자동차 전기공학