HVPM의 카오스 신호와 치환동기

°이익수*, 여지환**

*포항1대학 정보통신과, **대구대학교 정보통신공학부

Replaced Synchronization and Chaos Signal by HVPM

°Ik-soo Lee*, Ji-hwan Ryeo**

*Dept. of Information Communication, Pohang College,

**Dept. of Electronics, Taegu University

Tel: (0562)245-1253, E-Mail: leeis@pohang.ac.kr

요 약

본 논문에서는 카오스 현상을 나타내는 수식을 변형하여 암호시스템이나 PN(pseudo-noise) 시퀀스에 적용하기 위하여 복잡한 카오스 신호를 발생시키는 하이퍼카오스 VP 사상(HVPM, Hyper chaos Volume Preserving Maps)과 이들간의 카오스 동기화를 제안한다. 단계별 모듈러(modulus) 함수를 이용하여 랜덤한 카오스 신호를 발생시키기 위하여 이산시간(discrete-time) HVPM 모델을 설정하고, 수치해석 실험으로 아날로그 카오틱 시퀀스(CAS. chaotic analog sequence)의 특징을 분석한다. 그리고 HVPM의 신호를 기존의 단순한 PC(Pecora, Carroll)방법을 응용한 치환동기화(synchronous substitution)를 이용하여 구동 및 응답시스템간의 카오스 동기화(chaos synchronization) 제어를 한다. 수치실험에서 카오스 신호가 갖는 특징들을 확인할 수 있었으며, 치환동기시스템에서 효과적인 카오스 동기화가 수행됨을 증명할 수 있었다.

I. 서 론

카오스 신호는 다양한 동적(dynamic) 특성과 예측이 불가능한 랜덤신호를 발생시킬 수 있으며, 광대역전력스펙트럼(broadband power spectrum) 특성과 초기상태에 민감한 특징을 보인다. 최근 카오스 시스템을 동기화시키는 구성들이 많이 제안되었고, 이것을 비화통신 및 암호통신에 적용하려는 시도가 활발히 진행되고 있다[1,2].

종래 제안들은 카오틱 캐리어(chaotic carrier) 또는 파라메터(parameters) 변조기법을 이용하여 정보신호를 마스킹(masking)하여 통신을 한다. 그러나 기존의 단순한 카오스 신호는 안전한 시퀀스(secure sequence)로 직접 사용할 수 없다. 의도된 측정자가 카오스 정보를 획득하면 쉽게 재구성(reconstruction)할 수 있다. Short, Pére 등은 카오스 암호시스템의 구성들은 안전하지 않으며, 역마스킹(unmasking)의 예측기법을 이용하면 신호를 복호할 수 있다고 발표했다[5]. 보통 카오스 현상의 경우에는 위상공간에서 전형적인 패턴이나 어트랙터가 나타나므로 신호를 역마스킹하는데 도움을 주며, 상관함수가 긴 시간에 낮은 값을 갖는 경우에는 신호를 예측하는데 유리하다고 알려져 있다. 그리고 한 개의 리아푸노프 지수를 갖는 단점이 있다. 따라서 카오스 신호는 아직 고도의 안전성을 제공하지 못하고 있다.

주파수확산통신[3] 기술은 확산 시퀀스(spreading sequence) 또는 PN(pseudo-noise) 시퀀스에 기인한다. 그러나 기존의 PN 시퀀스는 종류(families)와 크기(sizes)가 다양하지 않다는 것이 단점이며, 암호화 시스템 응용될 때에는 문제가 된다. 또한 미래에 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 간섭을 줄이고, 통신성능을 향상하기 위해서는 PN 시퀀스가 좋은 상관특성을 가져야 하며, 빠른 PN 코드의 획득(fast acquisition)과 고도의 안전성(high level security) 등을 가져야 한다. 그러나 카오스 신호는 랜덤신호와 같은 특징으로 인하여 가상랜덤수 발생기의 가능성을 부여해 준다. 우선 다양한 PN 시퀀스의 발생이 쉽고, 암호통신에서 비밀키(secret key)로 사용할 수 있는 파라메터들을 변화시켜 다양한 동적응답을 만들 수 있다. 이렇게 함으로서 임의 시퀀스의 크기와 주기를 변화시켜 랜덤한 PN 시퀀스를 발생시킬 수 있다[4].

본 연구에서는 기존의 암호통신이나 PN 시퀀스가 갖는 단점을 극복하고 모듈러(modulus) 함수를 도입하여 랜덤한 카오스 신호를 발생시키는 HVPM을 제안한다. 그리고 HVPM이 결합된 카오스 시스템을 구성하여 기존의 PC 동기제어를 변형한 치환동기법으로 동기화가 가능함을 보인다. 본 논문의 구성을 보면, II절에서 카오스 신호를 발생시키는 HVPM의 모델과 다양한 수치실험한 결과를 보이고, III절에서는 구동 및 응답시스템으로 구성한 카오스 시스템간의 치환동기화 수치실험을 행한다.

II. HVPM의 모델링

카오틱 사상(chaotic map)은 'n'차 비선형 함수를 선형사상으로 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. 본 연구에서는 지역적으로 'VP(volume preserving)'를 이루고, 점힘함수는 모듈러함수를 이용하여 방향성을 갖지 않는 하이퍼카오스신호를 발생시키는 수식을 제안한다.

선형변환 'L'은 팽창함수(EF, expansion function)가 되며, 'x(n+1)=Lx(n)'에 의해 카오스 신호를 발생시킨다. 접힘함수(FF, Folding Function) 'F(x)={$x_1$mod$k$, $x_2$mod$k$, $x_3$mod$k$, ...,$x_n$mod$k$}'를 사용하면 위상공간에서 영역 [$-k_i$, k_i]에 제한된 신호가 된다. 식 (1)을 3차 이산시간 카오스 발생수식을 HVPM(Hyperchaos Volume Preserving Maps)으로 정의하였으며 모듈러(modulo) 함수와 차분방정식으로 나타내었다.

$$\begin{aligned} x(n+1) &= \alpha x(n) + \beta z(n) \\ y(n+1) &= \gamma y(n) + \delta z(n) \quad (\zeta \pm A)\mathrm{Mod}(B) \mp C \quad (1) \\ z(n+1) &= \rho x(n) + \sigma y(n) \end{aligned}$$

여기서 모듈러함수의 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. 제안한 식 (1)을 이용한 카오스 발생수식에서 'x, y, z' 값의 선형조합으로 하여 구성할 수 있으며, 'α , β , γ , δ , ρ , σ ' 등은 카오스 상태를 변화시킬 수 있는 변수들로서 다양한 동적응답을 구할 수 있다. 그리고, 각각의 'n' 시간, 즉 이산시간에는 순환루프(recursive loop) 형태로 카오스 신호를 발생시킨다. 모듈러 함수는 다음 그림 1과 같이된다.

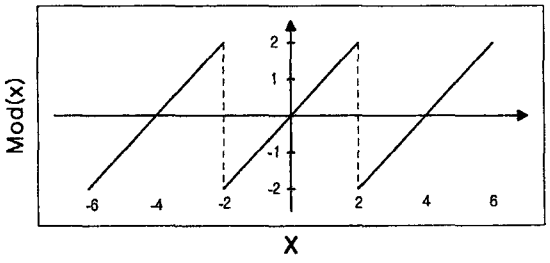

그림 1. 모듈러(modulo) 함수

3차 이산시간 HVPM 수식을 컴퓨터를 이용하여 비선형 동력학 신호처리 기법을 바탕으로 카오스 상태를 수치해석(numerical analysis)으로 분석하였다. 식 (1)에서 제어 파라메터 - α =-4/3, β =1.0, γ =1/3, δ =1.0, ρ =1.0, σ =1.0 - 값에

대하여 'x(n)', 'y(n)', 'z(n)' 등의 상태가 카오스 상태가 된다.

카오스 신호의 특징은 초기값에 민감한 특성을 보이며, 예측이 불가능하게 된다. 그림 2는 'x(n)', 'y(n)', 'z(n)' 의 각각에 '10^{-4}'의 차이로 신호가 반복 계산 후에 나타나는 'x(n)'의 두 신호의 형태를 보여주고 있다. 카오스 시스템에서는 무수한 초기값의 선택과 더불어 파라메터들은 랜덤수 발생시의 랜덤시드(random seed)로 간주하여 많은 랜덤신호를 얻을 수 있다. 그림 3은 위상공간에서 '2000' 개의 상태를 표현한 것으로 위상공간 전지역에 걸쳐 흩어져 균일한 분포를 보인다. 이것은 기존의 전형적인 어트랙터와는 다른 일정한 패턴을 형성하지 않아 카오스 상태를 예측하기가 어렵게 된다는 것을 나타낸다.

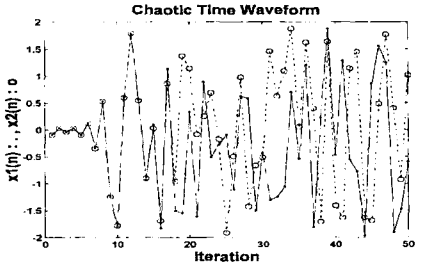

그림 2. 초기값이 다른 카오스 신호

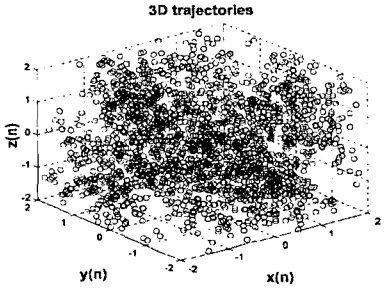

그림 3. 3차원 카오스 어트랙터

발생된 카오스 상태의 시간파형을 주파수(frequency) 스펙트럼으로 분석하면 신호의 주파수는 넓은 대역에 전력이 분포하며 균일(white)한 광대역 스펙트럼(broad-band spectrum) 형태를 가진다. 그림 4는 파형을 '4096' DFT(Discrete Fourier Transform)로 진폭 스펙트럼을 나타낸 것이다. 이러한 신호는 반송파(carrior)로 사용될 경우에 신호의 주파수 분포를 전송대역에 확산시키는 주파수확산통신에 사용할 경우 확산부호(spreading code)로 할당할 수 있다. 또한, 주파수 확산 시스템에서 확산 PN 코드는 자기상관(Autocorrelation) 함수값이 영지연(zero-delay)일 때 높으며, 그 이외의 지연시간에서는 거의 '0'에 가까운 특성을 가진다. 그림 5에 결과를 나타내었다.

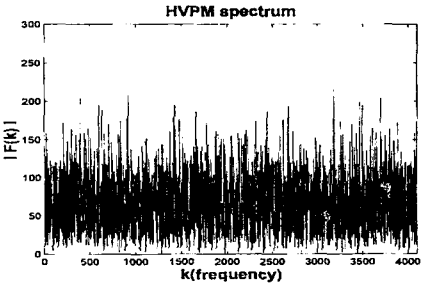

그림 4. HVPM 신호의 스펙트럼

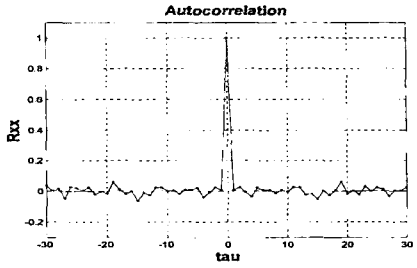

그림 5. CAS의 자기상관 함수값

III. HVPM의 카오스 동기화

카오스 시스템은 복잡한 비주기운동으로 자체적으로 동기화를 이탈한다. 독립된 카오스 시스템은 지수함수적으로 변화를 일으키며, 완전히 상관관계를 갖지 않는 동작상태를 보인다. 본 연구에서는 PC(Pecora와 Carroll)[4]의 카오스 동기화 개념을 도입하고 응용했다. PC의 방법은 하나의 카오스 시스템을 두 시스템으로 분리한 후, 응답시스템의 리아푸노프 지수(Lyapunov exponent)가 음수인 경우에 구동시스템에서 카오스 신호를 구동하여 응답시스템으로 인가했을 경우 두 시스템

간에는 카오스 동기화가 이루어진다는 것을 증명했다.

본 실험에서 치환동기를 제안하여 카오스 동기화를 검증했다. 구동시스템(transmitter)에서 기본적인 구동신호와 다른 카오스 신호들을 혼합하고 변형하여 새로운 스칼라 구동신호를 만들어 응답시스템(receiver)에서 이것을 이용하여 카오스 동기화를 수행한다. 이것은 기존의 PC 방법에서는 응답시스템에서 CLE(conditional Lyapunov exponents)를 체크하여 값이 '-' 값이 되면 부시스템(subsystem)이 안정하므로 구동 및 응답시스템을 구성하였지만, 치환동기에서는 불안정한 부시스템조차도 카오스 동기화를 가능하게 한다. 이렇게 구동신호를 변형시키면 다양한 카오스 구동신호를 만들 수 있을 뿐만 아니라 수신단에서 구동신호를 원하지 않은 측정자가 신호를 해석하기가 어렵게 되어 암호화통신에 효과적인 방법이 된다. 또한 안정한 부시스템을 구성한다는 것은 쉬운 것이 아니기 때문에 치환동기를 이용하면 불안정한 부시스템을 적당하게 설계하면 불안정한 응답시스템에서도 즉각적인 카오스 동기화를 이룩하는 장점을 가진다. 다음의 식 (2)은 치환동기화를 위한 응답시스템의 구성을 나타낸 것이다.

$$\begin{aligned} w(n) &= z(n) + Tx(n) \\ \tilde{z}(n) &= w(n) - Tx'(n) \\ x'(n+1) &= \alpha x'(n) + \beta\tilde{z}(n) \\ y'(n+1) &= \gamma y'(n) + \delta\tilde{z}(n) \\ z'(n+1) &= \rho x'(n) + \sigma y'(n) \end{aligned} \qquad (2)$$

동기화 상태에서 안정성(stability)를 결정하는 데는 응답시스템의 CLE가 사용된다. sub-Jacobian의 고유치(eignvalues)가 's-plane'의 경우는 좌반평면(left-half plane)에 존재해야 한다. 다음의 그림 6은 T가 '-2/3' 일때 Jacobian의 고유치가 '2/3', '1/3'이 되므로 안정한 시스템이 되어 시간이 지남에 따라 즉각적인 동기화가 수행됨을 보인다.

IV. 결 론

본 연구에서는 모듈러(modulus) 함수를 사용하여 다양한 카오스 신호를 발생시키는 HVPM을 제안하여 카오스 신호가 위상공간을 채우는 것을 볼 수 있었다.

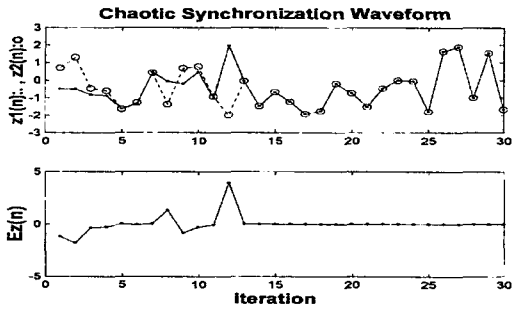

그림 6. 치환동기화

이러한 복잡한 카오스 신호는 광대역 전력스펙트럼(broad-band power spectrum)을 가지며, 자기상관함수 값도 빠른 시간에 '0'로 되었다. 그리고 카오스 동기화를 위하여 HVPM의 치환동기 방법으로 즉각적이며, 효과적인 동기제어를 구성할 수 있었다. 앞으로 제안한 수식과 카오스 시스템을 디지털 카오스회로로 구현하는데 연구가 진행되어야 한다.

참 고 문 헌

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

[2] 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.

[3] 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.

[4] 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.

[5] Kevin M. Short, "Steops toward unmasking secure communications," International journal of Bifurcation and Chaos, Vol.4, No.4 pp.959-977, 1994.
[6] T. L. Carrol, J. F. Heagy and L. M. Pecora, "Transforming signals with chaotic synchronization," Phys. Rev. E. *Vol.* 54, No. 5. pp.4676-4680, 1996.