N형 비선형 매핑함수를 이용한 HVPM 회로의 구현

°이익수*, 여지환**
*포항1대학 정보통신과, **대구대학교 정보통신과

Implementation of HVPM circuit using N-type mapping function

°Ik-soo Lee*, Ji-hwan Ryeu**
*Dept. of Information Communication, Pohang College,
**Dept. of Electronics, Taegu University
E-mail: leeis@pohang.ac.kr

ABSTRACT

본 논문에서는 복잡한 카오스 신호를 발생시키는 HVPM(hyperchaotic volume preserving maps) 모델과 HVPM 모델의 구현회로를 제안한다. 랜덤한 카오스 신호를 발생시키기 위하여 3차원 이산시간(discrete-time) 연산과 비선형 사상(maps)으로 모듈러(modulus) 함수를 이용하여 하이퍼카오스 신호를 발생시킨다. 그리고 HVPM 모델은 여러 가지 시스템 파라미터들을 변화시키면 다양한 카오스 신호를 발생시킬 수 있으며, 출력되는 카오스 신호는 비주기성을 갖게 된다. 이러한 특징을 갖는 HVPM 모델의 회로 구현을 위하여 2단 N형의 함수를 CMOS와 선형 연산증폭기 및 비교기를 이용하여 보드상에서 구현하여, 다양한 하이퍼카오스 신호를 확인할 수 있었다.

I. 서 론

카오스 신호는 다양한 동적(dynamic) 특성을 보이며, 예측이 불가능한 랜덤신호를 발생시킨다. 특히, 초기상태에 민감한 특징을 가지며, 신호의 주파수를 분석하면 광대역 전력 스펙트럼(broadband power spectrum) 분포를 나타낸다. 이러한 특징을 이용하여 최근에는 카오스 시스템간의 동기화(synchronization) 알고리즘들이 많이 제안되었고, 이것을 비화통신 및 암호통신에 적용하려는 시도가 활발히 진행되고 있다.[1],[2]

종래의 제안들은 카오틱 캐리어(chaotic carrier) 또는 파라미터(parameters) 변조기법을 이용하여 정보신호를 카오스 신호와 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[3] 등은 카오스 암호시스템의 구성들은 안전하지 않으며, 역마스킹(unmasking)의 예측기법을 이용하면 신호를 복호할 수 있다고 하였다. 일반적으로 카오스 동적현상의 경우는 위상공간에서 전형적인 패턴이나 사상 또는 어트랙터(attractor)가 나타나므로 신호를 역마스킹하는데 도움을 주며, 카오스 신호의 상관(correlation) 함수 값이 긴 시간에 낮은 값을 갖는 경우는 신호를 예측

하는데 더욱 유리하다고 알려져 있다. 그리고 단순한 카오스 시스템은 양의 값을 갖는 한개의 리아푸노프 지수를 가지므로 두개 이상이 양의 값을 갖는 하이퍼카오스(hyperchaos) 시스템을 사용해야 신호의 안전성을 제공한다고 한다.[4]

한편, 주파수확산(SS; spread spectrum)[5] 통신기술은 확산 시퀀스(spreading sequence) 또는 PN(pseudo-noise) 시퀀스에 기인한다. 그러나 기존의 PN 시퀀스는 종류와 크기가 다양하지 않으며, 주기성이 있다는 것이 단점으로 암호화 시스템 응용될 때에는 문제가 된다. 또한 간섭을 줄이고, 통신성능을 향상하기 위해서는 PN 시퀀스가 좋은 상관특성을 가져야 하며, 빠른 PN 코드의 획득을 위하여 회로구현이 가능해야 하고 고도의 안전성(security) 등을 가져야 한다.

이러한 이유로 카오스 시스템은 기존의 주파수확산 시스템의 단점을 보안할 수 있다. 먼저 카오스 시스템은 다양한 PN 시퀀스의 발생이 쉬우며 비주기적인 신호의 특징으로 인하여 신호의 보안성을 높일 수 있다. 그리고 보안통신에서 비밀키(secret key)로 사용할 수 있는 시스템 파라미터들을 변화시켜 다양한 동적상태로 변화시킬 수 있다. 이렇게 함으로써 임의의 아날로그 시퀀스를 조합하여 사용하여 복잡하면서도 랜덤한 PN 시퀀스를 발생시킬 수 있다.

본 논문에서는 기존의 보안통신이나 주파수확산 시스템에 사용되는 PN 시퀀스의 단점을 극복하기 위하여 복잡한 하이퍼카오스 신호를 도입하였다. 또한 기존의 카오스 시스템이 위상공간에서 나타내는 전형적인 어트랙터를 개선하기 위하여 모듈러 함수를 도입하여 랜덤한 어트랙터 패턴을 갖는 3차원 이산시간 HVPM 모델을 제안하였다. 그리고 HVPM 모델을 N형 비선형 회로의 조합으로 모듈러 회로를 구현하고, 연산증폭기를 사용하여 아날로그 회로로 보드상에 구현하여 하이퍼카오스 신호의 발생을 확인하였다.

Ⅱ. HVPM 모델

이산시간의 카오틱 사상(chaotic map)은 n차 비선형 함수를 선형사상으로 하여 계속적인 순환 피드백(recursive feedback)으로 카오스 신호를 발생시킬 수 있다. 이때 핵심 메커니즘은 팽창(stretching)과 축소(folding) 변환의 계속적인 반복에 의한 것이다. 본 논문에서는 기존의 카오스 시스템이 갖는 전형적인 카오스 어트랙터를 변형한 랜덤한 어트랙터 패턴을 형성하기 위하여 위상공간에서는 VP(volume preserving)를 이루고, 계속적인 변환함수로는 모듈러 함수를 이용하여 출력신호간의 방향성을 갖지 않는 하이퍼카오스 신호를 발생시키는 차분방정식을 제안한다.

선형변환 L은 팽창함수(EF; expansion function)가 되며, e(n+1)=Le(n)에 의해 이산시간 카오스 신호를 발생시킨다. 또한 접힘함수(FF; folding function)는 f(e)={$e_1 \bmod k$, $e_2 \bmod k$, ..., $e_n \bmod k$)를 사용하면 위상공간에서 영역 [$-k_1$, k_1]에 제한된 신호가 된다. 다음의 식 (1), (2) 및 (3)을 3차원 이산시간 카오스 신호를 발생시키는 차분방정식을 HVPM(hyperchaotic volume preserving maps)으로 정의하였으며, 3차연립 차분방정식과 모듈러(modulus) 함수를 나타내었다.

$$\begin{aligned} x(n+1) &= f[\alpha x(n) + \beta z(n)] \\ y(n+1) &= f[\gamma y(n) + \delta z(n)] \\ z(n+1) &= f[\rho x(n) + \sigma y(n)] \end{aligned} \tag{1}$$

$$Y = f(X) = \begin{cases} h(X+p) & \text{for } X < 0 \\ h(X-p) & \text{for } X \geq 0 \end{cases} \tag{2}$$

$$\begin{aligned} a(t+1) &= h\{a(t)\} \\ &= k_1 a(t) - k_2 \left\{ \frac{2}{1+e^{-a(t)/\varepsilon}} - 1 \right\} \end{aligned} \tag{3}$$

여기서 모듈러 함수 f의 변환은 X의 신호에 $\pm p$를 더한 후, h함수의 출력값을 Y로 한다. 식 (1)에서의 연립방정식은 $x(n)$, $y(n)$, $z(n)$ 값의 선형조합으로 하여 구성할 수 있으며, α, β, γ, δ, ρ, σ 등과 k_1, k_2, ε, p 등은 카오스 상태를 변화시킬 수 있는 변수들로서 다양한 동적응답을 구할 수 있다. 그리고,

각각의 입력 n시간, 즉 이산시간에는 순환루프의 출력으로 $n+1$시간의 카오스 신호를 발생시킨다. 모듈러 함수 f는 다음의 그림 1에서와 같다.

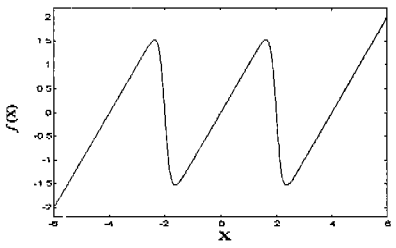

그림 1. 모듈러 함수

제안한 HVPM 모델을 컴퓨터를 이용하여 비선형 동력학 신호처리 기법을 바탕으로 카오스의 동적상태를 수치해석으로 분석하였다. 식 (1)에서 식 (3)에 적용한 시스템 파라미터로는 α=-4/3, β=1.0, γ=1/3, δ=1.0, ρ=1.0, σ=1.0, p=2.0, k_1=1.0, k_2=2.0, ε=0.1 등의 값에 대하여 $x(n)$, $y(n)$, $z(n)$ 등의 출력신호는 카오스 신호가 된다. 카오스 신호의 특징은 초기값에 민감한 특성을 보이며, 예측이 불가능하게 된다. 모의실험에서 각 상태의 값을 10^{-4}의 차이로 신호가 반복 계산 후에 출력되는 두 카오스 신호는 즉각적으로 다른 파형을 보여주었다. 따라서 카오스 시스템에서는 무수한 초기값의 선택과 더불어 시스템 파라미터들은 랜덤한 시퀀스 발생의 랜덤 시드(seed)로 처리하여 수많은 비주기의 랜덤신호를 얻을 수 있다. 그림 2는 3차원 위상공간에서 1000개의 카오스 출력상태를 표현한 것으로 체적의 위상공간에 걸쳐 흩어진 랜덤한 어트랙터의 패턴을 보인다. 이것은 기존의 전형적인 어트랙터와는 다른 일정한 패턴을 형성하지 않으며, 복잡한 카오스 상태로 신호를 예측하기가 어렵게 된다는 것을 나타낸다.

발생된 카오스 상태의 시간파형을 주파수 스펙트럼으로 분석하면 신호의 주파수는 넓은 대역에 전력이 분포하며 균일한 광대역 스펙트럼 형태를 가진다. 이러한 신호는 반송파(carrior)로 사용될 경우에 신호의 주파수 분포를 전송대역에 확산시키는 주파수확산통신에 사용할 경우 확산부호로 할당할 수 있다. 또한, 주파수확산 시스템에서 확산 PN 코드는 자기상관(autocorrelation) 함수값이 영지연(zero-delay)일 때 높으며, 그 외에는 적은 값을 가진다.

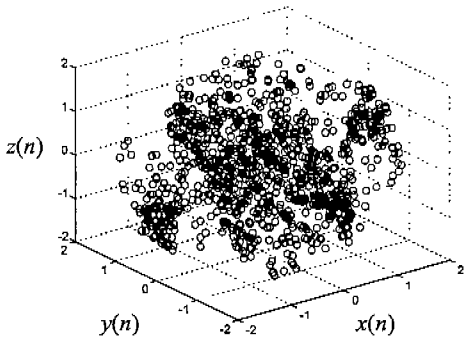

그림 2. 3차원 카오스 어트랙터

III. HVPM 모델의 회로구현

카오스 신호를 발생시키는 회로는 카오스 방정식에 따라 다양하게 구현이 가능하며, 비선형 전달함수 소자, 수동소자 및 능동소자 등을 사용하여 구성할 수 있다. 또한 출력신호의 종류로는 이산시간(discrete time) 및 연속시간 (continuous time)의 형태 또는 전압 및 전류의 형태 등에 따라 다양하게 제안되었고, 최근에는 고차원의 카오스 발생회로가 활발히 연구되고 있다.

본 논문에서는 제안한 HVPM 모델은 3차 이산시간 연립 차분방정식으로 표현되므로 그림 3에서와 같은 회로 블록을 3개로 구현할 수 있다. 우선 이산시간의 동작을 위하여 앞뒤에 샘플 및 홀드회로를 추가하고, 매핑회로 블럭은 다시 연산회로와 모듈러회로 블럭으로 나누어 구현할 수 있다. 연산회로 블럭에서는 HVPM 모델의 연립방정식 부분을 계산을 위하여 LF353 연산증폭기를 사용하였다. 그리고 그림 4에서와 같이 모듈러회로 블럭 구현하기 위하여 N형의 비선형함수 구현을 위하여 4007 내부의 CMOS 전달특성과 피드백 저항의 선형조합으로 구현하였다. 구현한 N형 특성함수를 비교기를 사용하여 2단계로 앞뒤로 이동하고, 조합하여 HVPM 모델의 모듈러 회로를 구현하였다. 또한 HVPM 모델을 전자회로로 구현하는데 있

어, 여러가지 파라미터들의 독립적인 가변이 가능하고, IC 칩으로 구현을 쉽게하기 위하여 아날로그 회로로 설계 및 구현했다. 그리고 HVPM의 동적특성은 $h(t)$ 함수의 기울기 ε에 의해 민감한 특성을 나타내므로 피드백 저항 R_f을 조정하여 급격한 기울기에서 완만한 기울기까지의 가변이 가능하도록 하였다.

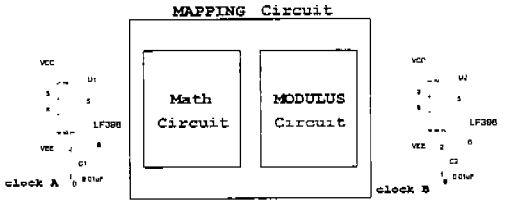

그림 3. HVPM 모델의 1차원 회로 블럭도

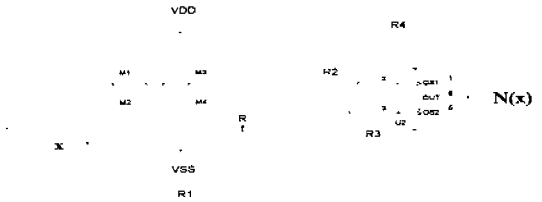

그림 4. N형 비선형 함수의 회로도

구현한 회로를 보드상에서 각종 시스템 파라미터는 가변저항으로 조정한 후, 실험을 행하였다. 그림 5는 오실로스코프를 사용하여 $z(n)$의 시간파형을 측정한 사진이다. 그림에서와 같이 구현한 카오스 회로의 이산시간 출력은 제한된 영역에서 비주기적인 랜덤한 파형을 발생시키는 것을 알 수 있다.

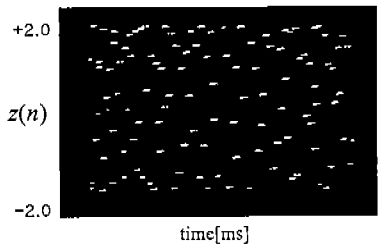

그림 5. HVPM 모델 회로의 출력파형

IV. 결 론

본 연구에서는 랜덤한 어트랙터 패턴을 형성하는 HVPM 모델을 제안하고, HVPM 모델을 아날로그 전자회로로 구현하여 보드상에서 하이퍼카오스 출력을 실험하였다. N형의 모듈러 함수를 사용하여 3차 이산시간의 다양한 하이퍼카오스 신호를 발생시켰으며, 구현한 회로에서도 다양한 시스템 파라미터를 가변저항을 사용하여 하이퍼카오스 신호의 출력을 증명하였다. 앞으로 제안한 HVPM 모델의 구현회로의 카오스 동기화 및 비화통신 시스템의 구현에 연구가 진행되어야 할 것이다.

※ 본 연구는 한국과학재단 목적기초연구 (1999-2-112-002-2)의 지원으로 수행되었음.

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] K. M. Short, "Steops toward unmasking secure communications," International journal of Bifurcation and Chaos, Vol.4, No.4 pp.959-977, 1994.

[4] T. Kapitanoak and L. O. Chua, "Hyperchaotic attractors of unidirectionally coupled Chua's circuits," Int. J. Bifurcation and Chaos, vol. 4, no. 2, pp. 477-482, 1994.

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