디지털 혼돈 맵의 동적 저하 개선을 위한 비트 확장 기법

최효정°, 김강산°, 노홍준°°, 송홍엽°

연세대학교 전기전자공학과° LIG 넥스원 C4I 연구소°°

Bit extension method for improving dynamic degradation of digital chaotic maps

Hyojeong Choi°, Gangsan Kim°, Hongjun Noh°°, Hong-Yoep Song°

Dept. of Electrical and Electronic Engineering° C4I R&D Center°°

Yonsei University LIG Nex1

{hjchoi3022, gs.kim, hysong}@yonsei.ac.kr hongjun.noh@lignex1.com

요 약

본 논문은 혼돈 맵(Chaotic map)을 디지털 시스템에서 구현할 때 발생하는 동적 저하(dynamic degradation)를 개선하기 위한 비트 확장(Bit extension) 기법을 소개한다. 본 기법으로 생성된 의사 혼돈 수열과 동일 정밀도의 고정 소수점 연산으로 생성된 의사 혼돈 수열의 랜덤 특성, 자기 상관특성 및 주기성을 비교하고, 연접 혼돈 맵(Cascade chaotic map)에 본 기법을 적용하여 출력된 수열의 랜덤 특성 및 주기성을 단일 혼돈 맵으로 출력된 수열과 비교한다.

1. 서론

혼돈 맵은 초기값에 민감한 특성을 가지고 있어 미세한 초기값의 차이 만으로도 완전히 다른 수열이 생성되는 비선형 함수이다. 이러한 특성으로 인해 서로 다른 무한한 수열을 쉽게 생성할 수 있어 기존 직접 수열 대역 확산 (Direct Sequence Spread Spectrum) 시스템에서 혼돈 수열의 사용이 연구되어 왔다[1,2,5].

무한한 실수 영역에서 정의되는 혼돈 맵을 유한 정밀도인 디지털 시스템에서 구현하는 경우, 연산의 오차로 인해 혼돈 맵의 정의와 달리 짧은 주기성이 발생하거나 임의의 값으로 수렴하는 등 동적 저하 현상이 나타난다[3,4]. 이러한 동적 저하 문제를 해결하기 위해 여러 혼돈 맵을 연접하거나[3], 이진 시프트 혼돈 맵(Binary shift chaotic map)의 LSB 를 확장하는 기법[4]이 제안되어 왔다. [4]에서 제안된 기법은 단순히 2 를 곱하거나 보수를 취하는 연산만을 사용하는 이진 시프트 혼돈 맵에서 마지막 비트를 확장하는 기법으로, 적용할 수 있는 맵과 파라미터가 한정적이다.

이러한 한계를 극복하고자 본 논문에서는 [4]의 기법을 변형하여 다양한 맵과 다양한 파라미터를 적용할 수 있는 비트 확장 기법을 소개하고 여러 특성들을 분석한다. 디지털 혼돈 맵은 주로 랜덤 특성, 주기성, 상관 특성 등으로 분석되며, 여기서 랜덤 특성의 판단은 ApEn, PE, SE 가 주로 사용된다[5].

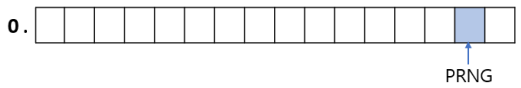

그림 1. 고정소수점 연산에서의 비트 확장

따라서 본 논문에서는 먼저 동일한 정밀도를 갖는 고정소수점 연산을 통해 생성된 의사 혼돈 수열과 본 기법을 적용한 의사 혼돈 수열의 랜덤 특성과 주기성을 비교하고, 더 나아가 두개의 맵을 연접한 연접 혼돈 맵에 여러 비트 확장을 통해 생성된 출력 수열의 랜덤 특성, 주기성, 상관특성을 분석한다.

2. 본론

본 논문에서는 혼돈 맵으로 Logistic 맵과 Tent 맵을 고려한다. Logistic 맵은 다음 식 (1)로 정의되는 함수이다.

$$L(x) = \mu x_n(1 - x_n) \quad (1)$$

여기서 $0 < \mu \leq 4$이고 $x_n \in [1,0]$이다. Tent 맵은 다음 식 (2)로 정의되는 함수이다.

$$T(x) = \begin{cases} ux, & 0 \leq x \leq 1/2 \\ u(1-x), & \frac{1}{2} \leq x < 1 \end{cases} \quad (2)$$

여기서 $1 \leq u \leq 2$이고 $x_n \in [1,0)$이다.

본 논문에서 제안하는 비트 확장 기법은 [4]에서 제안한 기법을 변형하여, 혼돈 맵을 구현할 비트 정밀도를 선택하고 그림 1 의 예시와 같이 고정소수점 연산에서 특정 비트를 의사 랜덤 수열로 확장시키는 기법이다. 본 논문에서는 16 비트 정밀도를 고려

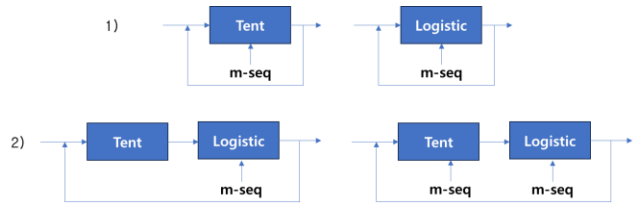

그림 2. 혼돈 맵의 비트 확장 기법

표 1. 고정소수점 연산에서 혼돈 맵의 특성

		Tent	Logistic
고정 소수점 16 비트	주기	595	79
	ApEn	0.5355	0.5284
	PE	2.0508	2.1445
	SE	6.3309	9.2764

하였으며, 모든 수열은 길이 50000 을 고려하였고, 의사 랜덤 수열로 주기가 $2^{16}-1$인 m-수열을 고려했다. 먼저 비트 확장 기법이 적용되지 않은 경우, 16 비트 고정소수점 연산을 적용한 Tent 맵과 Logistic 맵의 주기성과 랜덤 특성을 표 1 에서 보여준다. 이때 두 맵으로 출력된 수열은 혼돈 맵의 동적 저하로 인해 주기성이 매우 짧은 것을 확인할 수 있다.

비트 확장 기법의 실험 방법은 그림 2 와 같다. 그림 2 의 1)과 같이 Tent 맵과 Logistic 맵 각각에 대해 여러 위치에서 비트를 확장해보면서 가장 좋은 랜덤 특성과 상관 특성을 갖는 비트 확장 위치를 선택했다. 두 맵 모두 초기값은 0.7 을 사용하였으며, Tent 맵은 $u = 1.96875$로 설정하여 21 번째 비트를 확장시켰고, Logistic 맵은 $\mu = 4$로 설정하여 14 번째 비트를 확장시켰다. 이에 대한 결과 수열의 주기성, 랜덤특성, 자기상관 특성들은 표 2 에 나타내었다. 또한, 출력된 수열은 0 과 1 사이의 실수 수열이므로 0.5 를 임계값으로 설정한 후 이진으로 맵핑한 수열의 자기상관 특성도 함께 나타내었다.

표 2. 비트 확장기법이 적용된 단일 혼돈 맵의 특성

	Tent (21 번째 비트 확장)	Logistic (14 번째 비트 확장)
주기	196,605	65,535
ApEn	1.0927	0.6604
PE	2.3430	2.1565
SE	14.4386	13.8914
자기 상관	sidelobe max : 0.0180 sidelobe mean : 0.0036	sidelobe max : 0.0175 sidelobe mean : 0.0035
(이진) 자기 상관	sidelobe max : 0.0180 sidelobe mean : 0.0036	sidelobe max : 0.0184 sidelobe mean : 0.0036

그림 2 의 2)는 Tent 맵과 Logistic 맵을 연접하여 단일 비트 확장과 이중 비트 확장을 적용한 경우이다. 왼쪽 그림과 같이 연접 혼돈 맵에 단일 비트 확장을 적용한 경우 Logistic 맵의 14 번째 비트에만 확장을 적용하였고, 오른쪽 그림과 같이 이중 비트 확장을 적용한 경우에는 Tent 맵의 3 번째비트, Logistic 맵의 14 번째 비트를 확장시켰다.

표 3. 비트 확장기법이 적용된 연접 혼돈 맵의 특성

	Tent + Logistic (단일 비트 확장)	Tent + Logistic (이중 비트 확장)
주기	65,535	65,535
ApEn	1.1460	1.5520
PE	2.4434	2.5028
SE	14.3755	14.1917
자기 상관	sidelobe max : 0.0813 sidelobe mean : 0.0335	sidelobe max : 0.1010 sidelobe mean : 0.0844
(이진) 자기 상관	sidelobe max : 0.0473 sidelobe mean : 0.0052	sidelobe max : 0.0564 sidelobe mean : 0.0044

표 1-3 의 실험 결과를 살펴보면 표 2 와 같이 본 논문에서 제안하는 비트 확장 기법을 적용한 경우, Tent 맵은 사용된 m-수열의 주기×3 인 196,605 가되고 Logistic 맵은 사용된 m-수열의 주기가 되는 것을 확인했다. 즉, 비트 확장 기법을 적용하면 동일한 정밀도에서 주기를 크게 증가시킬 수 있으며 좋은 랜덤 특성, 자기상관 특성을 갖는 것을 알 수 있다. 표 3 과같이 연접 혼돈 맵에 비트 확장을 적용한 경우에는 표 2 의 단일 혼돈 맵에 비트 확장을 적용한 경우보다 더 좋은 랜덤 특성을 갖는 것을 확인하였다. 이때 Tent + Logistic 의 이중 비트 확장의 경우에는 출력된 실수 수열의 평균 값이 0.5953 이되어 자기 상관 사이드로브가 약 0.1 정도로 큰 값이 나오지만, 평균 값인 0.5953 을 임계값으로 설정한 후 이진 수열을 출력하면 우수한 자기 상관 특성을 갖는 것을 확인할 수 있다.

ACKNOWLEDGMENT

이 논문은 2023 년도 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임 (No. 11-202-205-010 (KRIT-CT-22-086), 비주기·비예측 임의성·연속성·신호형 초저피탐 은닉통신 과제).

3. 참고 문헌

[1] G. Heidari-Bateni, C.D. McGillem, “A chaotic direct sequence spread-spectrum communication system,” IEEE Trans. Commun. vol. 42, pp.1524–1527, 1994.

[2] 최효정, 노홍준, 송홍엽, "카오스 맵 기반으로 생성된 이진 수열의 상관특성과 균형특성," 2022 년 한국통신학회 추계종합학술발표회, 2022 년 11 월.

[3] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, “Cascade chaotic system with applications,” IEEE Trans. Cybern., vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[4] I. Öztürk and R. Kilic, “Digitally generating true orbits of binary shift chaotic maps and their conjugates,” Communications in Nonlinear Science and Numerical Simulation, vol. 62, pp. 395–408, Sep. 2018.

[5] C. Bandtand B. Pompe, “Permutation entropy a natural measure of complexity,” Physical Review Letters, pp. 174102(1-4), 2002.