연접 혼돈 맵과 LSB 확장 기법이 적용된 의사 혼돈 수열의 특성 분석

최효정, *노홍준, 송홍엽

연세대학교, *LIG Nex1

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

Characteristic analysis of pseudo-chaotic sequences using cascade chaotic map and LSB extension method

Hyojeong Choi, *Hongjun Noh, Hong-Yeop Song

Yonsei Univ., *LIG Nex1.

요 약

본 논문은 연접 혼돈 맵(cascade chaotic map)에 LSB(Least Significant Bit) 확장 기법을 적용하여 출력된 의사 혼돈 수열의 랜덤 특성, 주기성 및 자기 상관 특성을 부동 소수점을 사용한 단일 혼돈 맵의 출력 수열과 비교하여 분석한다. 랜덤 특성의 분석은 근사 엔트로피(Approximate Entropy, ApEn), 순열 엔트로피(Permutation Entropy, PE), 샤논 엔트로피(Shannon Entropy, SE)를 계산하여 분석하였으며, 실험 결과 연접 혼돈 맵에 LSB 확장 기법을 적용한 수열은 좋은 랜덤 특성, 자기 상관 특성 및 긴 주기를 갖는다.

Ⅰ. 서 론

기존 직접 수열 대역 확산(Direct Sequence Spread Spectrum, DSSS) 시스템에서 사용하는 의사 난수 수열(PN code)은 수열 집합의 크기가 제한적이다. 반면, 혼돈 맵은 초기값에 민감한 특성을 가지고 있기 때문에 미세한 초기값의 차이 만으로도 일정한 주기 없이 무한한 수의 수열을 생성할 수 있어 의사 난수 수열을 사용하는 기존 DSSS 시스템에서 혼돈 수열의 사용이 연구되어 왔다[1].

디지털 시스템에서 혼돈 수열을 부동 소수점 산술로 구현하는 경우, 연산의 오차가 발생하여 혼돈 맵의 정의와 달리 짧은 주기성이 발생하거나 임의의 값으로 수렴하는 등 동적 저하(dynamical degradation)가 발생한다. 이러한 디지털 구현 문제를 해결하기 위해 단일 혼돈 맵을 연접한 연접 혼돈 맵[2]과 이진 시프트 혼돈맵(Binary Shift Chaotic Map, BSCM)에서 LSB를 확장하는 기법[3]이 제안되어 왔다.

디지털 혼돈 맵의 특성은 주로 랜덤 특성, 주기성, 상관 특성 등으로 분석된다. 여기서 랜덤 특성의 판단은 ApEn, PE, SE가 주로 사용된다[4][5]. ApEn과 PE는 SE만으로는 수열에 대한 복잡도 차이를 구분할 수 없다는 한계 때문에 제안된 분석기법이며, ApEn은 패턴의 일관성이 유지되는 가능성을 측정하는 파라미터이고, PE는 수열 내부 성분들의 순서를 고려한 측정 파라미터이다.

본 논문에서는 BSCM을 연접하고 LSB 확장 기법을 적용하여 생성된 의사 혼돈 수열의 랜덤 특성(ApEn, PE, SE), 주기성, 자기 상관 특성을 부동 소수점을 사용한 단일 혼돈 맵의 출력 수열과 비교하여 분석한다.

Ⅱ. 본론

A. 이진 시프트 혼돈 맵(BSCM)과 LSB 확장 기법

본 논문에서는 BSCM으로 베르누이 맵과 텐트 맵을 고려한다. 베르누이 맵 S는 다음 식 (1)로 정의되는 함수이다.

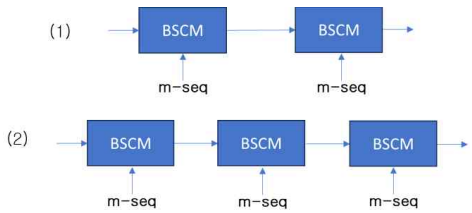

그림 1. 연접 혼돈 맵과 LSB 확장 기법의 결합

$$S(x) = 2x \pmod 1 = \begin{cases} 2x, & 0 \le x \le 1/2 \\ 2x-1, & 1/2 \le x < 1 \end{cases} \quad (1)$$

BSCM으로서 베르누이 맵의 연산은 최상위 비트(Most Significant Bit, MSB)를 버리고 단순히 왼쪽으로 한 비트 이동하는 연산으로 설명될 수 있다. 텐트 맵 T는 다음 식 (2)로 정의되는 함수이다.

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

텐트 맵의 구현은 베르누이 맵과 비슷하며, 유일한 차이점은 $(1-x)$가 곱해지므로 보수 연산을 취하는 연산이 추가 된다. 이들을 LSB 확장 기법에 적용할 때 모든 연산은 L비트 메모리 단위에서 수행되며, 2배를 취하는 연산으로 메모리 유닛의 MSB를 버리면서 왼쪽으로 한 비트 이동하고 이때의 LSB를 PRNG의 출력 비트로 대체한다. 이에 대한 자세한 구현 알고리즘은 [2]에 자세히 설명되어있다.

B. 실험 환경 및 의사 혼돈 수열의 특성 분석

본 논문은 그림 1과 같이 II-A에서 설명한 단일 BSCM들을 연접하고 LSB 확장 기법을 적용하는 경우를 고려한다. 본 논문의 모든 실험은 길이 50000과 초기값 0.7을 사용하여 실험하였으며, LSB 확장을 위한 PRNG로서 m-수열을 사용하였다. 표 1은 단일 맵을 부동 소수점 산술 및 LSB 확

		type	Quantization	ApEn	PE	SE	주기
베르누이	부동 소수점	single 32 bit	2^{23}	0.567	2.531	12.863	6532
	LSB 확장기법	메모리 유닛 수: 16 LFSR 유닛 수 : 16	2^{16}	0.693	2.461	15.609	65535
		메모리 유닛 수: 16 LFSR 유닛 수 : 32		0.693	2.460	14.952	$2^{32}-1$
텐트	부동 소수점	single 32 bit	2^{23}	0.642	2.158	12.437	4949
	LSB 확장기법	메모리 유닛 수: 16 LFSR 유닛 수 : 16	2^{16}	0.651	2.150	14.957	41556
		메모리 유닛 수: 16 LFSR 유닛 수 : 32		0.653	2.151	14.951	$\approx 10^{11}$
베르누이 + 텐트	LSB 확장기법	메모리 유닛 수: 16 LFSR 유닛 수 : 16	2^{16}	1.263	2.571	14.958	524280
		메모리 유닛 수: 16 LFSR 유닛 수 : 32		1.266	2.573	14.946	$\approx 10^{11}$
베르누이+ 텐트 + 베르누이	LSB 확장기법	메모리 유닛 수: 16 LFSR 유닛 수 : 16	2^{16}	1.957	2.582	14.958	131070
		메모리 유닛 수: 16 LFSR 유닛 수 : 32		1.959	2.582	14.954	$\approx 10^{11}$

표 1. 단일 혼돈 맵과 연접 혼돈 맵에 LSB 확장 기법을 적용한 출력 수열의 랜덤 특성과 주기

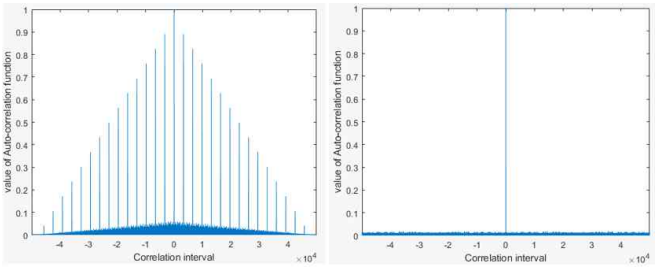

그림 2 . 부동소수점 연산을 사용한 베르누이 맵과 LSB 확장기법을 사용한 베르누이+텐트+베르누이 맵의 자기 상관 특성

장 기법을 사용하여 출력한 수열과, 그림 1과 같이 연접 혼돈 맵에 LSB 확장 기법을 결합하여 사용한 출력 수열의 랜덤 특성과 주기를 보여준다. 32 비트 부동 소수점 연산을 사용한 경우, 소수점 이하 자릿수를 표현하는 비트 수가 23비트이므로 0과 1사이의 2^{23}개의 실수로 표현된 수열이 출력되며, 본 논문에서 고려한 LSB 확장 기법에서는 16개의 메모리 유닛을 사용하였으므로 2^{16}개의 실수로 표현된 수열이 출력된다. 표 1에서 LFSR의 유닛 수는 m-수열을 생성하는데 필요한 레지스터 수를 의미하며, LFSR 유닛 수 16은 주기가 $2^{16}-1$인 m-수열을 사용하여 LSB를 확장한 것을 의미한다.

먼저, 표 1에서 단일 맵을 사용한 경우에 대해 비교해보면, LSB 확장 기법을 사용한 경우가 부동 소수점 32비트를 사용한 경우에 비해 훨씬 더 낮은 정밀도를 갖지만 ApEn와 SE가 증가하고 PE는 비슷하게 유지되면서 주기가 훨씬 길어진다. 베르누이 맵에 LSB 확장 기법을 사용한 경우의 출력 수열은 사용된 "m-수열의 주기"와 동일한 주기가 발생하며, 텐트 맵의 경우에는 "메모리 유닛 수×m-수열의 주기"와 동일한 크기의 주기가 발생하는 것을 확인했다.

연접 맵(베르누이+텐트)에 LSB 확장 기법을 결합하여 사용한 경우에는 동일한 정밀도에서 단일 맵에 LSB 확장 기법을 적용한 경우보다 랜덤 특성(ApEn, PE, SE)이 개선되며 주기는 "(메모리 유닛 수/2)×m-수열의 주기"가 되는 것을 확인했다. 또한, 베르누이+텐트+베르누이를 연접하여 LSB 확장 기법을 적용한 경우에는 가장 좋은 랜덤 특성을 가지며, 주기의 경향성은 파악되지 않았지만 m-수열과 메모리 유닛의 적절한 선택으로 매우 긴 주기를 갖는 출력 수열을 충분히 생성할 수 있음을 확인했다.

그림 2는 부동 소수점 연산을 사용한 단일 베르누이 맵과 LSB 확장 기법을 사용한 베르누이+텐트+베르누이 맵의 자기 상관 특성을 보여준다. 다른 경우에 대한 자기 상관 특성을 실험한 결과는 본 논문에서 생략하였지만 연접 혼돈 맵에 LSB 확장 기법을 적용한 경우 그림 2의 오른쪽 그림과 같이 좋은 자기 상관 특성을 갖는 것을 확인하였다.

따라서 본 논문에서 실험한 결과에 따라 향후 직접 수열 대역 확산 시스템에서 집합의 크기가 유한한 기존 PN 코드 대신, 본 논문에서 제안하는 연접 혼돈 맵과 LSB 확장 기법을 결합하여 출력된 수열을 고려할 수 있을 것으로 기대한다.

ACKNOWLEDGMENT

이 논문은 2023년도 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).

참 고 문 헌

[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] 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.

[3] 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.

[4] S. M. Pincus, "Approximate entropy as a measure of system complexity," Proc. *Nat. Acad. Sci. USA*, vol. 88, Mar. 1991.

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