

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

최효정, *노홍준, 송홍엽

연세대학교, *LIG Nex1



목 차



I. 서론

II. 혼돈 맵과 LSB 확장 기법

- 이진 시프트 혼돈 맵 (Binary Shift Chaotic Maps, BSCM)
- LSB 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 랜덤 특성, 주기성, 자기 상관 특성 분석 파라미터
- 실험 결과

IV. 결론

- 혼돈 맵은 미세한 초기값의 차이만으로 완전히 다른 실수 값이 도출되는 비선형 함수로 초기값의 변화만으로 주기가 없는 서로 다른 무한한 수열 생성 가능
 - DSSS 시스템에 PN 코드 대신 혼돈 수열의 적용이 고려 되어옴[1][4]
 - 혼돈 수열은 군용 통신 시스템에서도 고려할 수 있음
- 디지털 시스템에서 혼돈 수열을 부동 소수점 산술로 구현하는 경우, 연산의 오차가 발생
 - 혼돈 맵의 정의와 달리 짧은 주기성이 발생하거나 임의의 값으로 수렴함
- 디지털 구현 문제를 해결하기 위해 연접 혼돈 맵[2]과 이진 시프트 혼돈 맵에서 LSB를 확장하는 기법[3]이 제안됨
- 본 논문에서는 혼돈 맵을 연접하고 LSB 확장 기법을 적용하여 생성된 의사 혼돈 수열의 랜덤 특성, 주기성, 자기 상관 특성을 분석함



I. 서론

II. 혼돈 맵과 LSB 확장 기법

- 이진 시프트 혼돈 맵 (Binary Shift Chaotic Maps, BSCM)
- LSB 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 랜덤 특성, 주기성, 자기 상관 특성 분석 파라미터
- 실험 결과

IV. 결론



- ❖ 이진 시프트 혼돈 맵(Binary Shift Chaotic Map, BSCM)은 곱셈이 이진 시프트 연산이고, 덧셈 연산 중에 오버플로우가 발생하지 않는 혼돈 맵으로 정의

예) ■ Bernoulli map $S : [0, 1) \rightarrow [0, 1)$

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

Notice that S is just a left shift operation with discarding the most significant bit b_1 .

$$\text{i.e., } S(b_1 b_2 b_3 \dots)_2 = (b_2 b_3 b_4 \dots)$$

- Tent map $T : [0, 1) \rightarrow [0, 1)$ $T(x) = \begin{cases} 2x, & 0 \leq x < 1/2 \\ 2(1-x), & 1/2 \leq x \leq 1 \end{cases}$

LSB 확장 기법[3]

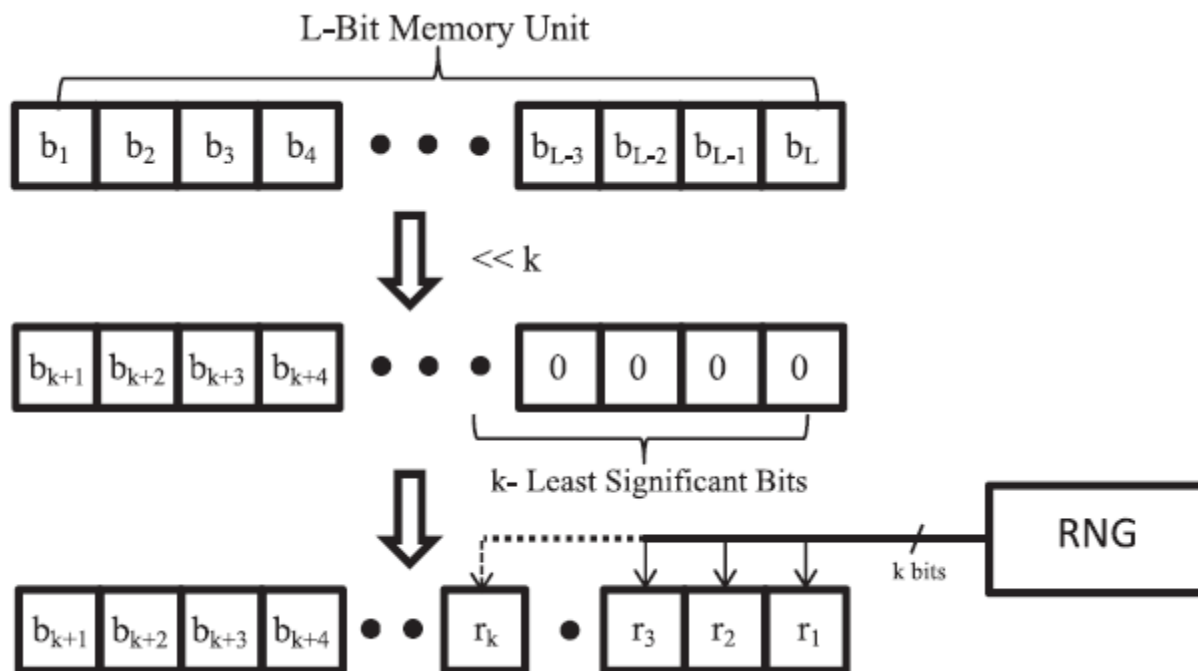


그림 1. LSB 확장 기법

- RNG로 PRNG의 사용 : 매우 긴 주기를 가질 수 있음.

Bernoulli map $S : [0, 1) \rightarrow [0, 1)$

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

Notice that S is just a left shift operation with discarding the most significant bit b_1 .

[2]

Algorithm 1 The pseudocode of the LSB extended Bernoulli map implementation.

```

function Bernoulli(initval,N)
: initval // floating point number between [0,1) → 첫 L bit가 됨
        N // a positive integer.
output: orbit // a 1xN array of floating point numbers.
variable: memunit // L-bit unsigned integer → uint 8, 16, 32, 64
begin function
    orbit[1] = initval
    memunit := floor(2^L * initval) // typecast to L-bit unsigned integer
    for i = 1 to N-1
        memunit := memunit << 1
        if rand() == 1
            memunit := memunit bitwise or 1
        end if
        orbit[i + 1] := 2^-L * double(memunit) → 실수 출력
    end for
end function

```

- 주기는 PRNG의 주기에 영향을 받음

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- 이진 시프트 혼돈 맵 (Binary Shift Chaotic Maps, BSCM)
- LSB 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 랜덤 특성, 주기성, 자기 상관 특성 분석 파라미터
- 실험 방식 및 결과

IV. 결론

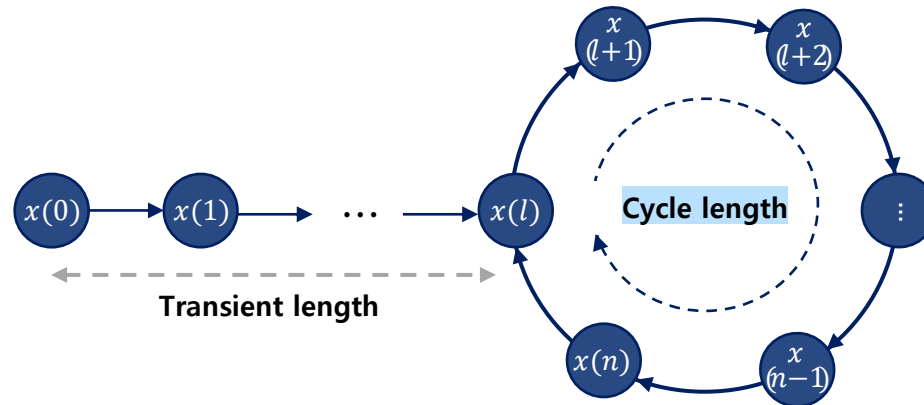


혼돈 수열의 분석 파라미터

➤ 랜덤 특성

- 샤논 엔트로피 (Shannon Entropy, SE)
- 근사 엔트로피 (Approximate Entropy, ApEn)
- 순열 엔트로피 (Permutation Entropy, PE)

➤ 주기성



의사 혼돈 수열의 궤적



혼돈 수열의 분석 파라미터

➤ 랜덤 특성

- 샤논 엔트로피 (Shannon Entropy, SE)
- 근사 엔트로피 (Approximate Entropy, ApEn)[4]
- 순열 엔트로피 (Permutation Entropy, PE)[5]

✓ Discrete random variable X 의 확률 질량 함수가 $p(x)$ 일 때,

$$H(X) = - \sum p(x) \log_2 p(x)$$

✓ Shannon Entropy는 수열에 대한 복잡도 차이를 구분할 수 없음

➤ ex) $p(x = 1) = 0.5, p(x = 0) = 0.5$

$$X_1 = [1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0]$$

$$X_2 = [1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0]$$

$$H(X_1) = H(X_2) = - \sum_{i=1}^2 p(x = i) \log p(x = i) = -2(0.5 * \log 0.5)$$



혼돈 수열의 분석 파라미터

➤ 랜덤 특성

- 샤논 엔트로피 (Shannon Entropy, SE)
- **근사 엔트로피 (Approximate Entropy, ApEn)[4]**
- 순열 엔트로피 (Permutation Entropy, PE)[5]

- ✓ m 길이의 내부 수열(window) 패턴의 일관성이 다음 $m + 1$ 길이의 내부 수열에서도 계속해서 유사하게 유지될 가능성을 (로그 형태로) 측정

$$\text{ApEn}(m, r) = \Phi^m(r) - \Phi^{m+1}(r)$$

- ✓ 어떤 패턴이 반복되는 빈도 또는 규칙성을 측정하는 것



혼돈 수열의 분석 파라미터

➤ 랜덤 특성

- 샤논 엔트로피 (Shannon Entropy, SE)
- 근사 엔트로피 (Approximate Entropy, ApEn)[4]
- **순열 엔트로피 (Permutation Entropy, PE)[5]**

✓ 수열 내부 성분들의 **순서**에 대해 고려하여 복잡도 측정

ex) $x = (4\ 7\ 9\ 10\ 6\ 11\ 3)$ and $n=3$

$(4,7,9)$ represent the permutation $\pi_1 = (1,2,3)$.

$(7,9,10)$ represent the permutation $\pi_1 = (1,2,3)$.

$(9,10,6)$ represent the permutation $\pi_4 = (2,3,1)$

⋮

$$p(\pi_1) = \frac{2}{5}, \quad p(\pi_2) = 0, \quad p(\pi_3) = \frac{1}{5}, \quad p(\pi_4) = \frac{2}{5}, \quad p(\pi_5) = 0, \quad p(\pi_6) = 0$$

$$PE(n) = - \sum_{j=1}^{n!} p(\pi_j) \log p(\pi_j)$$

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- 이진 시프트 혼돈 맵 (Binary Shift Chaotic Maps, BSCM)
- LSB 확장 기법

III. 의사 혼돈 수열의 특성 분석

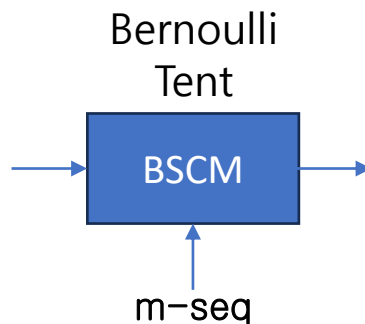
- 랜덤 특성, 주기성, 자기 상관 특성 분석 파라미터
- 실험 방식 및 결과

IV. 결론

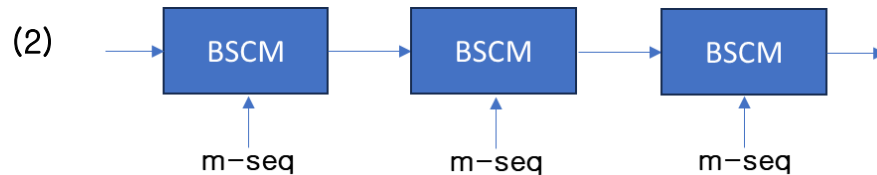
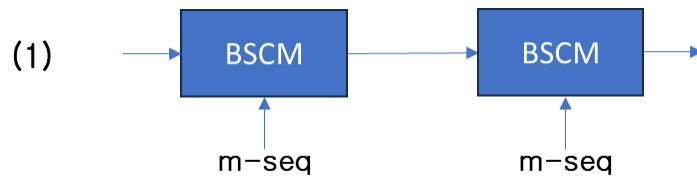


실험 방식

1. LSB 확장 기법



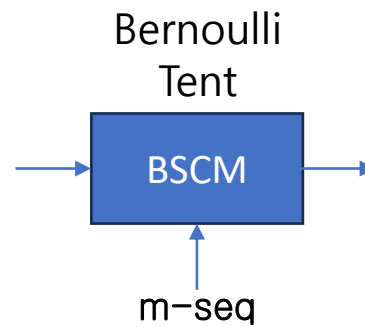
2. 연접 혼돈 맵과 LSB 확장 기법



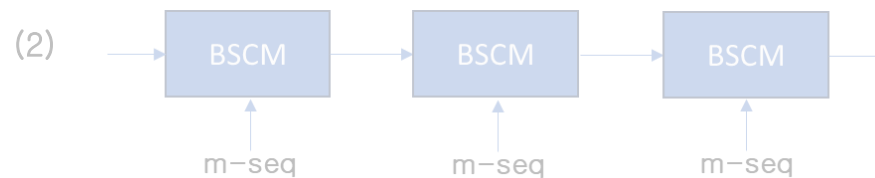
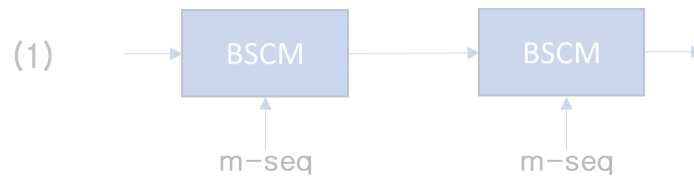


실험 방식

1. LSB 확장 기법



2. 연접 혼돈 맵과 LSB 확장 기법





부동소수점 산술 및 LSB 확장 기법

- **Bernoulli map S**: $[0, 1) \rightarrow [0, 1)$ $S(x) = 2x \pmod{1} = \begin{cases} 2x, & 0 \leq x < 1/2 \\ 2x - 1, & 1/2 \leq x < 1 \end{cases}$

길이 : 50000

초기값 : 0.7

window 크기 : 2 window 크기 : 3

	type	Quantization	ApEn	PE (max : $\log_2 6 \approx 2.585$)	SE	주기
부동 소수점	Single 32 bit	2^{23}	0.567	2.531	12.863 (max : 23)	주기 : 6532
LSB 확장 기법	메모리 유닛 수 : 16 LFSR 유닛 수 : 16	2^{16}	0.693	2.461	15.609 (max : 16)	주기 : 65535
	메모리 유닛 수 : 16 LFSR 유닛 수 : 32	2^{16}	0.693	2.460	14.952 (max : 16)	주기 : $2^{32} - 1$

m-seq 주기

더 낮은 정밀도임에도 불구하고 랜덤 특성은 비슷하게 유지되며, 주기 증가함



부동소수점 산술 및 LSB 확장 기법

- **Tent map T** : $[0,1) \rightarrow [0, 1)$

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

길이 : 50000

초기값 : 0.7

window 크기 : 2 window 크기 : 3

	type	Quantization	ApEn	PE (max : $\log_2 6 \approx 2.585$)	SE	주기
부동 소수점	Single 32 bit	2^{23}	0.642	2.158	12.437 (max : 23)	주기 : 4949
LSB 확장 기법	메모리 유닛 수 : 16 LFSR 유닛 수 : 16	2^{16}	0.651	2.150	14.957 (max : 16)	주기 : 41556
	메모리 유닛 수 : 16 LFSR 유닛 수 : 32	2^{16}	0.653	2.151	14.951 (max : 16)	주기 : $\approx 10^{11}$

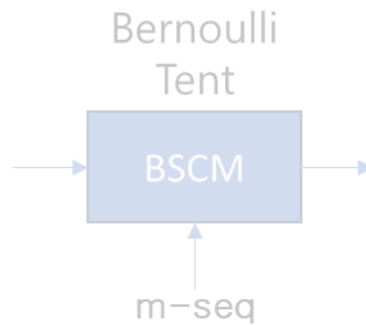
m-seq 주기 × 메모리 유닛 수

더 낮은 정밀도임에도 불구하고 랜덤 특성은 비슷하게 유지되며, 주기 증가함

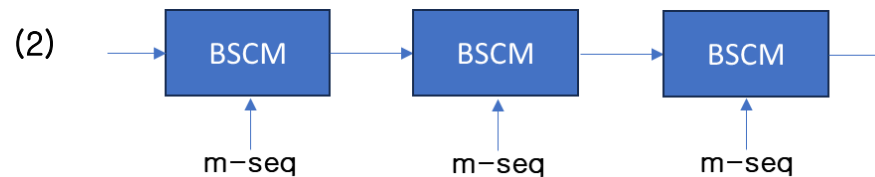
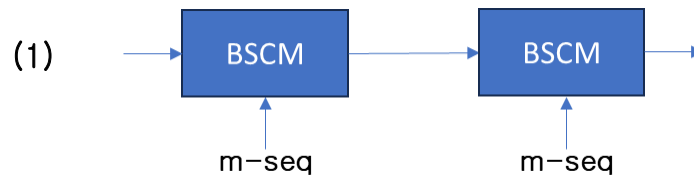


실험 방식

1. LSB 확장 기법



2. 연접 혼돈 맵과 LSB 확장 기법

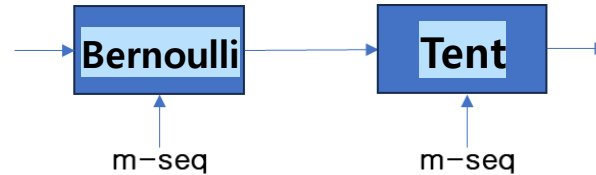




연접 혼돈 맵과 LSB 확장 기법

• Bernoulli + Tent

길이 : 50000
초기값 : 0.7



window 크기 : 2 window 크기 : 3

	type	Quantization	ApEn	PE (max : $\log_2 6 \approx 2.585$)	SE	주기
LSB 확장 기법	메모리 유닛 수 : 16 LFSR 유닛 수 : 16	2^{16}	1.263	2.571	14.958 (max : 16)	주기 : 524280
	메모리 유닛 수 : 16 LFSR 유닛 수 : 32	2^{16}	1.266	2.573	14.946 (max : 16)	주기 : $\approx 10^{11}$

$$\text{m-seq 주기} \times \frac{\text{메모리 유닛 수}}{2}$$

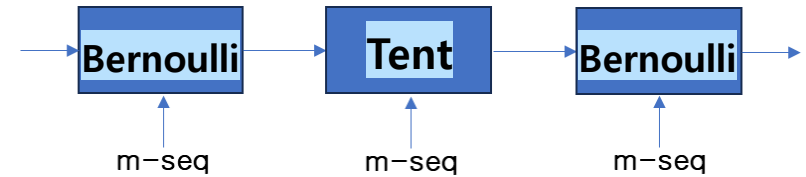
단일 맵 LSB 기법보다 랜덤 특성, 주기성 우수함



연접 혼돈 맵과 LSB 확장 기법

- Bernoulli + Tent + Bernoulli

길이 : 50000
초기값 : 0.7



window 크기 : 2 window 크기 : 3

	type	Quantization	ApEn	PE (max : $\log_2 6 \approx 2.585$)	SE	주기
LSB 확장 기법	메모리 유닛 수 : 16 LFSR 유닛 수 : 16	2^{16}	1.957	2.582	14.958 (max : 16)	주기 : 131070 (m-seq 길이 x 2)
	메모리 유닛 수 : 16 LFSR 유닛 수 : 32	2^{16}	1.959	2.582	14.954 (max : 16)	주기 : $\approx 10^{11}$

ApEn, PE 가장 좋음

Auto correlation 우수

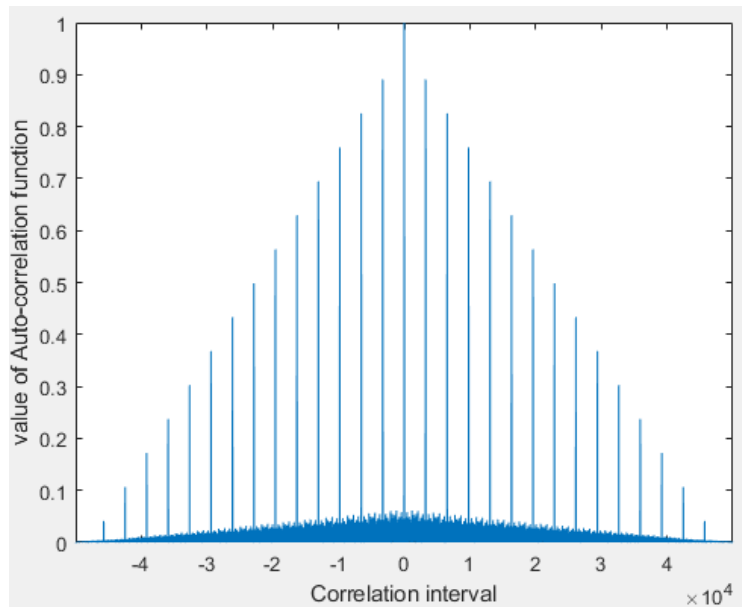
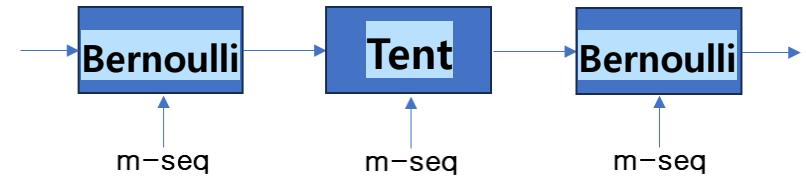


연접 혼돈 맵과 LSB 확장 기법

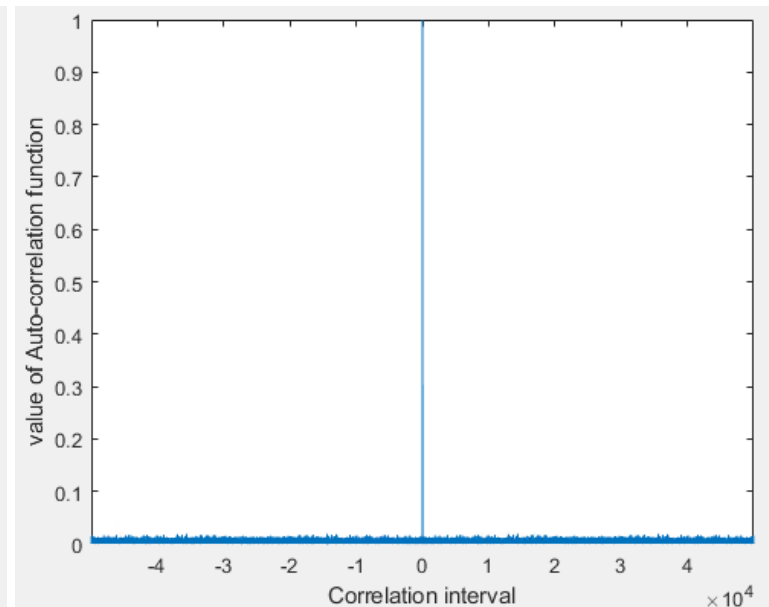
- Bernoulli + Tent + Bernoulli**

길이 : 50000

초기값 : 0.7



부동 소수점 단일 베르누이



side lobe max : 0.0194
side lobe mean : 0.0035

Auto correlation 우수

I. 서론

II. 혼돈 맵과 LSB 확장 기법

- 이진 시프트 혼돈 맵 (Binary Shift Chaotic Maps, BSCM)
- LSB 확장 기법

III. 의사 혼돈 수열의 특성 분석

- 랜덤 특성, 주기성, 자기 상관 특성 분석 파라미터
- 실험 방식 및 결과

IV. 결론

- 본 논문은 혼돈 맵의 디지털 구현을 위해 연접 혼돈 맵과 LSB 확장 기법을 결합하여 출력 수열의 랜덤 특성, 주기성, 자기 상관 특성을 분석함

- 실험 결과
 - LSB 확장 기법을 사용했을 때 부동 소수점 연산을 사용한 경우 보다 더 낮은 정밀도에서 좋은 랜덤 특성과 주기성을 가짐

 - 단일 맵에 경우보다 연접 혼돈 맵에 LSB 확장 기법을 적용한 경우에 더 좋은 랜덤 특성, 주기성, 자기 상관 특성을 가짐