https://doi.org/10.7840/kics.2025.50.5.741

연접 카오스 맵으로부터 생성된 의사 랜덤 실수 수열과 이진 수열의 랜덤 특성 분석

최 효 정◆, 김 강 산*, 송 홍 엽°, 신 상 웅**, 이 철 호**, 노 홍 준**

Analysis of Random Characteristics of Pseudo-Random Real Number and Binary Sequences Generated by Cascade Chaotic Maps

Hyojeong Choi◆, Gangsan Kim*, Hong-Yeop Song°,
Sangung Shin**, Chulho Lee**, Hongjun Noh**

요 약

본 논문에서는 Logistic, Sine, Chebyshev 맵을 다양한 방식으로 연접한 연접 혼돈 맵에 대해 리아푸노프 지수(Lyapunov Exponent), 근사 엔트로피(Approximate Entropy), 순열 엔트로피(Permutation Entropy)를 사용하여 이들의 동적 특성과 출력 실수 수열의 복잡성 및 난수성을 평가한다. 또한, 실수 수열을 두 가지 이진 맵핑 방식을 사용하여 이진 변환된 수열의 자기 상관 및 상호 상관 특성을 m-수열과 비교하고, NIST 테스트를 통한 랜덤성을 m-수열과 추가로 비교 분석한다. 실험 결과, 연접 혼돈 맵을 기반으로 생성된 이진 수열은 다양한 초기값과 제어 변수 설정을 통해 상관 특성 및 랜덤성이 우수한 매우 많은 코드 집합을 생성할 수 있다.

키워드 : 혼돈 맵, 연접 혼돈 맵, 리아푸노프 지수, 의사 랜덤 수열
Key Words : Chaotic map, Cascade chaotic map, Lyapunov exponent, Pseudorandom sequence

ABSTRACT

In this paper, we evaluate the dynamic properties, complexity, and randomness of cascaded Logistic, Sine, and Chebyshev maps using the Lyapunov Exponent (LE), Approximate Entropy (ApEn), and Permutation Entropy (PE). Additionally, we convert the real-number sequences generated by these maps into binary sequences using two different binary mapping methods, and we compare the autocorrelation and cross-correlation properties of the binary sequences with those of m-sequences. The experimental results show that the binary sequences generated from cascaded chaotic maps can produce a large set of codes with excellent correlation properties and randomness, depending on various initial conditions and control parameters.

※ 이 논문은 2024년도 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).
◆ First Author : Yonsei University School of Electrical and Electronic Engineering, hjchoi3022@yonsei.ac.kr, 학생회원
° Corresponding Author : Yonsei University School of Electrical and Electronic Engineering, hysong@yonsei.ac.kr, 종신회원
* Yonsei University School of Electrical and Electronic Engineering, gs.kim@yonsei.ac.kr, 학생회원
** LIG Nex1 C4I R&D Laboratory, sangung.shin@lignex1.com; chulho.lee2@lignex1.com, 정회원; hongjun.noh@lignex1.com, 정회원
논문번호 : 202410-256-B-RN, Received October 25, 2024; Revised November 26, 2024; Accepted December 26, 2024

Ⅰ. 서 론

혼돈(chaos)은 동적 시스템에서 복잡하고 예측 불가능한 무질서 상태를 의미하며, 이러한 혼돈의 특성을 갖는 비선형 함수를 혼돈 맵(Chaotic map)이라고 한다[1,2]. 혼돈 맵은 초기 조건에 민감하여 미세한 차이만으로도 완전히 다른 수열을 생성할 수 있으며, 이러한 특성으로 인해 암호학 및 의사 난수 생성기(Pseudo Random Number Generator, PRNG) 등 다양한 분야에서 활발히 연구되어 왔다[3-7].

혼돈 맵의 혼돈 성능을 직접적으로 증명하는 것은 매우 어렵다. 따라서, 동적 시스템에서 혼돈 행동을 정량적으로 설명하기 위해 리아프노프 지수(Lyapunov Exponent, LE)가 사용되며, 이는 인접한 궤적들 사이의 발산 속도를 수치적으로 나타내는 중요한 지표이다[7,9]. 특히, LE가 양수일 경우 인접한 궤적들이 점점 지수적으로 멀어지게 되며, 이는 시스템이 예측 불가능한 혼돈 상태임을 의미한다. 따라서, LE가 양수라는 것은 시스템이 혼돈 상태에 있음을 나타내는 중요한 근거가 된다[7,9,10].

단일 혼돈 맵은 상대적으로 낮은 LE 값을 가지는 경우가 많아, 보안 성능이 중요한 시스템에서는 충분히 높은 혼돈 성능을 제공하지 못할 수 있다. 이를 개선하기 위해 LE를 높이고 더 복잡한 혼돈 특성을 구현하려는 다양한 연구가 진행되었다[7,10,11,12,13,14]. 특히, [7], [10]에서는 단일 맵보다 더 우수한 혼돈 성능을 갖춘 연접 혼돈 시스템(Cascade Chaotic System, CCS)을 제안했다. [7]에서는 Logistic, Sine, Tent 맵을 사용하여 이들을 두 개씩 연접한 맵의 LE를 분석했으며, 두 개의 단일 혼돈 맵을 사용한 연접 혼돈 시스템의 LE가 두 단일 맵의 LE의 합이 된다는 사실을 증명했다. [10]에서는 Logistic, Cubic, Tent 맵을 사용하여 LE의 분석을 통해 여러 개의 단일 혼돈 맵을 결합하여 생성된 혼돈 맵은 더욱 복잡하고 예측 불가능한 혼돈 특성을 가질 수 있음을 보였다.

혼돈 시스템은 PRNG 설계에 있어서 그 활용 가능성이 주목받고 있으며, 그 중 대표적인 응용 사례가 직접 수열 대역 확산 스펙트럼(Direct Sequence Spread Spectrum, DSSS) 시스템이다[4-7]. DSSS 시스템에서는 여러 사용자가 동시에 통신할 수 있도록 각 사용자에게 서로 다른 PN 코드(Pseudo-Noise Code)가 할당된다. 기존의 PN 코드는 고정된 주기를 가지므로, 생성 가능한 수열의 수에 한계가 있다. 반면, 혼돈 맵을 통해 생성된 수열은 이론적으로 초기값의 미세한 차이만으로도 무한히 많은 비주기적 신호를 생성할 수 있어 이러한 한계를 극복할 수 있다. 이에 따라, 기존 PN 코드를 대체하거나 보완하기 위해 혼돈 기반 수열을 DSSS 시스템에 적용하려는 연구가 진행되어왔다[4,5,8,13,14]. 이러한 혼돈 수열은 더 큰 보안성을 제공할 수 있으며, 다중 사용자 환경에서도 우수한 성능을 발휘할 수 있을 것으로 기대된다.

본 논문에서는 Logistic, Sine, Chebyshev 맵을 다양한 방식으로 연접하여 LE 변화를 분석하는 것뿐만 아니라, 출력 실수 수열의 복잡성과 무작위성을 평가하기 위한 척도인 근사 엔트로피(Approximate Entropy, ApEn)와 순열 엔트로피(Permutation Entropy, PE)를 사용하여 연접에 따른 복잡성 변화를 분석한다. 또한, 출력 실수 수열을 두가지 이진 맵핑 방식으로 이진 변환한 후 생성된 이진 수열의 상관 특성과 NIST 테스트 결과를 기존 PN 코드인 m-수열과 비교한다.

본 논문의 구조는 다음과 같다. Ⅱ장에서는 혼돈 맵으로 잘 알려진 Logistic, Chebyshev, Sine 맵을 소개한다. Ⅲ장에서는 Ⅱ장에서 소개한 혼돈 맵들을 연접한 연접 혼돈 시스템의 LE들을 비교하고, 출력 실수 수열들의 복잡성 및 무작위성을 분석한다. Ⅳ장에서는 이러한 실수 수열로부터 두 가지 이진 맵핑 방식으로 이진 수열을 생성하여 상관 특성 및 랜덤 특성을 실험적으로 분석한다. Ⅴ장에서는 실험 결과를 정리하여 결론과 함께 본 논문을 마무리한다.

Ⅱ. 혼돈 맵과 리아푸노프 지수

본 장에서는 연접 혼돈 맵에 사용할 세 가지 혼돈 맵과 각 맵의 특성을 간략히 살펴본다.

2.1. Logistic 맵

Logistic 맵은 혼돈적 행동을 보여주는 대표적인 단일 맵으로 다음과 같이 정의된다[15].

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

여기서 $0 \le \mu \le 4$, $x_n \in [0,1]$이며, 제어변수 $\mu \in [3.57,4]$일 때, 일부 예외를 제외한 나머지 μ에 대해 LE가 양수이므로, Logistic 맵은 이 구간에서 혼돈 상태로 알려져 있다. 그림 1(a)는 Logistic 맵의 분기 다이어그램과 LE를 보여준다. 여기서 분기 다이어그램은 임의의 초기값에서 일정 반복 계산 후에 불안정한 과도(transient)상태를 지나 안정된 상태에 도달했을 때의 궤적을 시각화한 것이다.

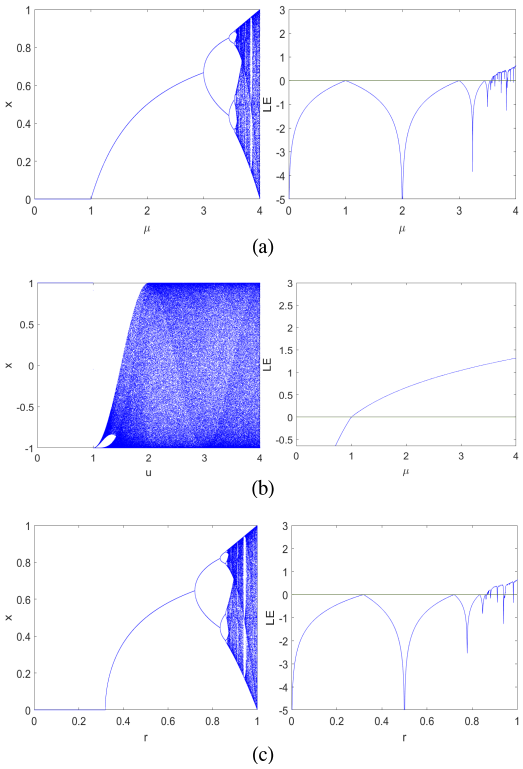


그림 1. 혼돈 맵의 분기 다이어그램과 리아푸노프 지수, (a) Logistic, (b) Chebyshev, (c) Sine 맵.
Fig. 1. Bifurcation Diagram and Lyapunov Exponent of Chaotic Maps

2.2 Chebyshev 맵

Chebyshev 맵은 [16]에서 처음 연구된 혼돈 맵으로, Chebyshev 다항식 형태로 표현된다. Chebyshev 맵은 다음과 같이 정의된다.

$$x_{n+1} = \cos(u\cos^{-1}(x_n)) \tag{2}$$

여기서 $0 \le u \le 4$, $x_n \in [-1,1]$이고, 제어변수 $2 \le u \le 4$일 때 Chebyshev 맵은 혼돈 상태이다. 그림 1(b)는 Chebyshev 맵의 분기 다이어그램과 LE를 보여준다.

2.3 Sine 맵

Sine 맵은 Logistic 맵과 유사한 혼돈 특성을 갖는 맵으로 다음과 같이 정의된다[17].

$$x_{n+1} = r\sin(\pi x_n) \tag{3}$$

여기서 $0 \le r \le 1$, $x_n \in [0,1]$이고, 제어변수 $r \in [0.867,1]$일 때 Sine 맵은 혼돈 상태이다. 그림 1(c)는 Sine 맵의 분기 다이어그램과 LE를 보여준다.

Ⅲ. 연접 혼돈 맵의 동적 특성 분석

그림 2는 연접 혼돈 맵의 구조이며, 여기서 f, g, h는 단일 혼돈 맵이다. 그림 2(a)는 혼돈 맵 두 개를 결합하여 혼돈 맵 g의 출력을 f의 입력으로 사용하고, f의 출력을 반복적인 계산을 위해 다시 g로 되먹임(feedback)한다. 수학적으로, 두 개의 혼돈 맵을 사용하는 연접 혼돈 맵은 다음과 같이 표현된다.

$$x_{n+1} = \Gamma(x_n) = f(g(x_n)) \tag{4}$$

세 개의 혼돈 맵을 사용하는 그림 2(b)의 경우도 유사한 방식로 다음과 같이 표현할 수 있다.

$$x_{n+1} = \Gamma(x_n) = f(g(h(x_n))) \tag{5}$$

(4)와 (5)에서 사용하는 단일 혼돈 맵 f, g, h는 동일한 혼돈 맵으로 설정할 수도 있고, 서로 다른 혼돈 맵으로 구성할 수도 있다.

본 논문에서는 Double-Logistic 맵, Triple-Logistic 맵, Double-Chebyshev 맵, Triple-Chebyshev 맵, Logistic-Sine 맵, Logistic-Sine-Logistic 맵의 여섯 가지 연접 혼돈 맵을 고려한다. 여기서, Double-과 Triple-맵을 구성하는 단일 맵들은 서로 동일한 혼돈 맵이지만, 서로 다른 제어변수를 고려한다.

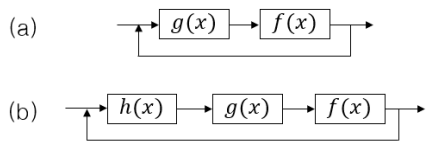


그림 2. 연접 혼돈 맵의 구조: (a) 두 개의 혼돈맵을 연접한 경우, (b) 세 개의 혼돈 맵을 연접한 경우
Fig. 2. Cascade Chaotic System structure using chaotic maps: (a) two seed maps, (b) three seed maps

3.1 연접 혼돈 맵의 동적 특성 분석

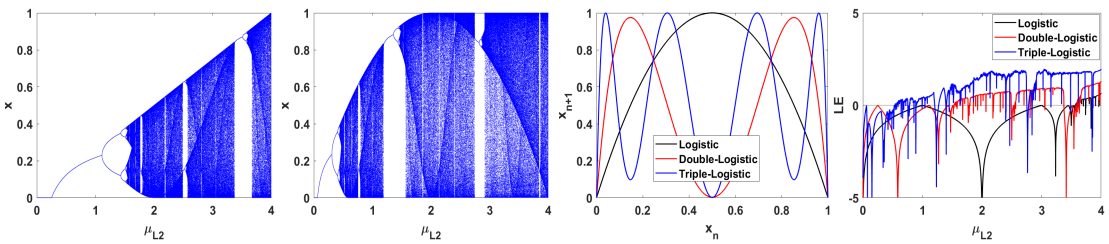
본 장에서는 연접 혼돈맵의 동적 특성의 분석을 위해 분기 다이어그램, 위상 도식(Phase Portrait), LE를 분석한다. 여기서 위상 도식은 x_n과 x_{n+1}의 관계를 시각화하여 시스템의 동적 특성을 보여주며, 복잡한 궤적이 나타날수록 더 혼돈적인 시스템임을 의미한다.

본 실험에서 각 연접 혼돈 맵의 제어변수는 다음과

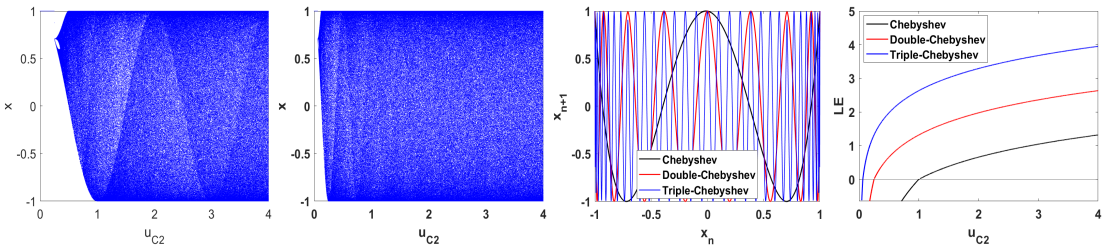
같이 표기한다. Double-Logistic 맵의 각 제어변수는 μ_{L1},μ_{L2}로, Triple-Logistic 맵에서는 μ_{L1},μ_{L2},μ_{L3}로 표기한다. Chebyshev 맵의 경우도 마찬가지로, Double-Chebyshev에서는 u_{C1},u_{C2} Triple-Chebyshev에서는 u_{C1}, u_{C2}, u_{C3}로 표기한다. Logistic-Sine 맵에서는 μ_{L1}, r_{S2}로, Logistic-Sine-Logistic 맵에서는 μ_{L1}, r_{S2}, μ_{L3}로 각각 표기한다.

그림 3(a)에서는 Double-Logistic 맵과 Triple-Logistic 맵을 비교한다. 첫 번째 그림은 Double-Logistic 맵에서 $\mu_{L1}=3.9997$로 설정하고 μ_{L2}의 변화에 따른 분기 다이어그램을 보여준다. 이는 그림 1(a)의 단일 Logistic 맵의 경우에 비해, 더 복잡한 분기 구조가 나타남을 알 수 있다. 그림 3(a)의 두 번째 그림은 Triple- Logistic 맵에서 $\mu_{L1}=3.9997$, $\mu_{L3}=3.999$로 설정하고 μ_{L2}의 변화에 따른 분기 다이어그램을 보여주며, 이는 Double-Logistic보다도 더욱 복잡한 분기 구조를 갖는 것을 알 수 있다. 위상 도식과 μ_{L2}에 대한 LE 그래프에서도 이러한 복잡성의 증가는 명확히 확인된다. Triple-Logistic 맵은 위상 도식에서 더욱 복잡한 궤적을 나타내며, LE 값도 전반적으로 더 높은 값을 보여 혼돈성이 더 강화되었음을 확인할 수 있다.

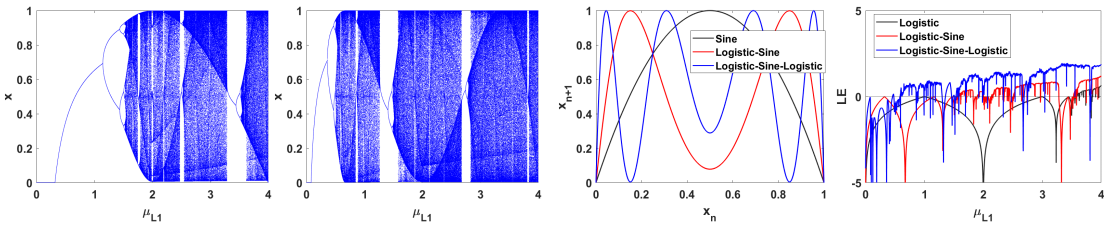
그림 3(b)와 3(c)에서의 비교에서도 유사한 양상을 확인할 수 있다. 그림 3(b)의 첫 번째 그림은 Double-Chebyshev 맵에서 $u_{C1}=3.9997$로 설정하고, u_{C2}를 변화시킨 분기 다이어그램이며, 두 번째 그림은 Triple-Chebyshev 맵에서 $u_{C1}=3.9997$, $u_{C3}=3.999$로 설정하고 u_{C2}를 변화시킨 분기 다이어그램이다. 그림 3(c)에서는 Logistic-Sine과 Logistic-Sine-Logistic 맵에서 각각 μ_{L1}을 변화시키고, $r_{S2}=0.999$, $\mu_{L3}=3.999$로 설정하였다. 결과적으로, 세 개의 혼돈 맵을 연접한 경우들은 각각 더 복잡한 분기 구조와 궤적을 보이며, LE 값도 전반적으로 더 높은 값을 보여 혼돈성이 더 강화된 것을 알 수 있다.



(a) Double-Logistic 맵과 Triple-Logistic 맵의 비교



(b) Double-Chebyshev 맵과 Triple-Chebyshev 맵의 비교



(c) Logistic-Sine 맵과 Logistic-Sine-Logistic 맵의 비교

그림 3. 연접 혼돈 맵의 분기 다이어그램, 위상 도식, LE
Fig. 3. Bifurcation Diagram, Phase Portrait, and LE of Cascade Chaotic Maps

3.2 근사 엔트로피와 순열 엔트로피

본 장에서는 앞에서 다룬 여섯 개의 연접 혼돈 맵으로부터 출력된 실수 수열의 복잡성을 근사 엔트로피(ApEn)와 순열 엔트로피(PE)를 통해 비교한다.

ApEn은 주어진 수열 내에서 반복되는 패턴의 복잡성을 측정하는 방법이다. 수열을 일정 길이의 부분 수열로 나누고, 각 부분 수열 간의 유사성을 기반으로 패턴의 예측 가능성을 계산한다[18]. 본 실험에서는 [18]에 따라 부분 수열의 길이를 2로 설정하고, 허용오차는 수열의 표준편차×0.2로 설정하였다.

PE는 수열 내 값들의 순열 패턴을 분석하여 복잡성을 측정하는 방법이다[19]. 수열을 일정 길이의 부분 수열로 나눈 후, 원소들의 크기 순서를 기반으로 엔트로피를 계산하며, 본 실험에서는 윈도우 크기를 6으로 설정하였다.

그림 4는 연접 혼돈 맵으로부터 생성된 출력 실수 수열의 복잡성을 비교하기 위한 ApEn와 PE의 실험 결과이다. 그림 4(a)와 4(b)에서는 각각 Double 및 Triple 구조의 Chebyshev, Logistic, Logistic-Sine 맵들의 근사 엔트로피 값을 비교한다. 두 그래프 모두에서 Chebyshev 계열 맵이 가장 높은 ApEn 값을 기록한다. 특히 Triple-Chebyshev는 제어변수 값이 증가함에 따라 근사 엔트로피 값이 일관되게 높은 수준을 유지하고 있어, 다양한 제어변수에 대해 매우 복잡한 수열을 생성함을 확인할 수 있다. Double- Logistic, Triple-Logistic, Logistic-Sine 계열의 맵들은 비슷한 패턴을 보이며, 제어변수가 커질수록 ApEn 값이 증가하나, 특정 구간에서는 변동폭이 큰 것을 확인할 수 있다.

그림 4(c)와 4(d)에서는 PE 값을 비교한 결과를 보여준다. ApEn과 마찬가지로, Chebyshev 계열이 가장 높은 PE 값을 기록하며, 특히 Double-Chebyshev와 Triple-Chebyshev는 제어변수 값이 증가함에 따라 매우 일관된 높은 값을 유지한다. 이는 이들 맵이 더 복잡하고 무작위적인 수열을 생성함을 나타낸다. 반면, Double-Logistic, Triple-Logistic, Logistic-Sine 계열의 맵들은 제어변수가 커질수록 PE 값이 증가하지만, ApEn과 마찬가지로 특정 구간에서 값의 변동폭이 크게 나타난다.

Ⅳ. 의사 랜덤 수열 생성기

III장의 여섯 개의 연접 혼돈 맵들에 대해 LE, ApEn, PE를 사용하여 동적 특성을 분석한 결과, 각 맵에서 제어변수에 따라 동적 특성이 매우 우수한 구간들이 나타났다. 그중에서 $\mu_{L2}(u_{C2})$가 3.9에서 4사이일 때는 모든 맵에서 ApEn과 PE의 값이 특히 뛰어난 성능을 보였다. 이에 따라, 본 장에서는 이 구간에서 생성된 실수 수열을 두 가지 이진 맵핑 방식을 적용하여 이진 수열로 변환한 후, m-수열과 상관특성 및 NIST 테스트 결과를 비교한다.

주어진 실수 출력 수열 $x=\{x_1, x_2, \cdots, x_n\}$에서 각각의 실수 값 x_i는 두 가지 방식으로 이진 비트 b_i로 변환하여 이진 수열 $b=\{b_1, b_2, \ldots, b_n\}$을 생성한다.

첫 번째 이진 맵핑 방식은 실수 출력 수열의 평균값을 임계값으로 설정하여, 수열의 각 값이 평균보다 크면 1, 평균보다 작으면 0으로 변환하는 방식이다. 두 번째 이진 맵핑 방식은 IEEE 754 표준[20]을 사용하여 실수 값을 64비트 부동소수점 표현으로 변환한 후, 52비트의 소수 부분에서 39번째 비트와 41번째 비트를 XOR 연산하여 이진 수열을 생성하는 방식이다.

4.1 이진 수열의 상관 특성

표 1과 표 2는 연접 혼돈 맵으로부터 생성된 이진 수열의 자기 상관 및 상호 상관 특성의 분석 결과를 보여준다. 본 논문에서 사용한 두 가지 이진 맵핑 방식에서 유사한 결과가 도출되어 결과를 하나의 표로 통합하였다.

본 연구의 목적은 완벽한 상관 특성을 가지는 수열을 생성하는 것이 아니라, 특정 조건에서 비교적 우수한

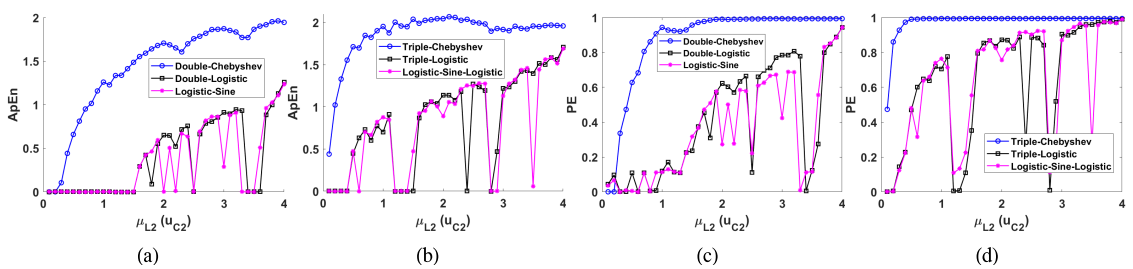


그림 4. 연접 혼돈 맵으로부터 생성된 출력 실수 수열의 근사 엔트로피(ApEn) 및 순열 엔트로피(PE)
Fig. 4. Approximate entropy and Permutation entropy of Real Number Sequences Generated from Cascade Chaotic Maps

표 1. 연접 혼돈 맵과 m-수열의 상관특성 (초기값 변화에 따른 비교)
Table 1. Correlation property of cascaded chaotic maps and m-sequences (comparison based on initial value)

Classification	**Length : 10000** $\mu_{L2}(u_{C2})=4$, **Initial value : 0.4001-0.4100**				**Length : 100000** $\mu_{L2}(u_{C2})=4$, **Initial value : 0.4001-0.4100**			
	Normalized Auto-correlation		Normalized Cross-correlation		Normalized Auto-correlation		Normalized Cross-correlation	
	Average (sidelobe)	Average (sidelobe max)	Average	Max Average	Average (sidelobe)	Average (sidelobe max)	Average	Max Average
Double-Logistic	≈0.008	≈0.04	≈0.008	≈0.04	≈0.002	≈0.01	≈0.002	≈0.01
Triple-Logistic								
Double-Chebyshev								
Triple-Chebyshev								
Logisitc-Sine								
Logisitc-Sine-Logisitc								
m-sequence	≈0.006	≈0.02	-	-	≈0.001	≈0.007	-	-

표 2. 연접 혼돈 맵과 m-수열의 상관특성 (제어변수 변화에 따른 비교)
Table 2. Correlation property of cascaded chaotic maps and m-sequences (comparison based on control parameter)

Classification	Length : 10000 $\mu_{L2}(u_{C2})$: $3.901-4$, Initial value : 0.4001				Length : 100000 $\mu_{L2}(u_{C2})$: $3.901-4$, Initial value : 0.4001			
	Normalized Auto-correlation		Normalized Cross-correlation		Normalized Auto-correlation		Normalized Cross-correlation	
	Average (sidelobe)	Average (sidelobe max)	Average	Max Average	Average (sidelobe)	Average (sidelobe max)	Average	Max Average
Double-Logistic	≈0.008	≈0.13	≈0.008	≈0.04	≈0.017	≈0.104	≈0.002	≈0.01
Triple-Logistic	**≈0.008**	**≈0.05**			**≈0.004**	**≈0.040**		
Double-Chebyshev	**≈0.007**	**≈0.03**			**≈0.002**	**≈0.015**		
Triple-Chebyshev	**≈0.007**	**≈0.03**			**≈0.002**	**≈0.014**		
Logisitc-Sine	≈0.046	≈0.15			≈0.043	≈0.156		
ogisitc-Sine-Logisitc	≈0.011	≈0.12			≈0.007	≈0.116		
m-sequence	**≈0.006**	**≈0.02**	-	-	**≈0.001**	**≈0.007**	-	-

상관 특성을 가지는 의사 랜덤 수열을 생성하는 데 있다. 따라서, 여전히 좋은 상관 특성을 갖는 것으로 알려진 특정 길이 10,000 및 100,000의 잘린 m-수열과 비교한다[21].

비교에 사용된 m-수열은 각각 주기 $2^{14}-1$과 $2^{17}-1$인 경우로, 해당 주기에서 10,000과 100,000 길이로 잘라 실험에 활용하였다. 주기 $2^{14}-1$인 m-수열은 특성다항식 $x^{14}+x^8+x^6+x+1$을, 주기 $2^{17}-1$인 수열은 특성다항식 $x^{17}+x^3+1$을 사용하여 생성하였다.

표 1은 제어변수 $\mu_{L2}(u_{C2})$를 4로 고정하고, 맵의 초기값을 0.4001에서 0.4100까지 0.0001 간격으로 변화시키며 100개의 이진 수열을 생성한 후 그 상관 특성을 분석한 결과이다. 자기 상관 특성은 100개의 이진 수열 각각의 자기 상관 사이드로브들의 평균값과 자기 상관 사이드로브 최대값의 평균을 평가하였고, 상호 상관 특성은 100개의 이진 수열 간 상호 상관의 평균값과 상호 상관의 최대값의 평균을 분석하였다.

표 1에서 확인할 수 있듯이, 제어변수 $\mu_{L2}(u_{C2})$를 4로 고정한 경우에는 여섯 개의 연접 혼돈 맵에서 생성된 이진 수열들이 고려한 모든 초기값에 대해 안정적인 상관 특성을 보였다. m-수열과 비교했을 때 약간의 성능 차이는 있으나, 전반적으로 충분히 우수한 수준의 상관 특성을 유지하고 있음을 확인할 수 있다.

표 2는 초기값을 0.4001로 고정하고, 제어변수

표 3. 연접 혼돈 맵과 m-수열의 NIST test 결과
Table 3. NIST test results for cascaded chaotic maps and m-sequences

Classification		Frequency	Run	Rnak	FFT	Universal	Serial	Liner Complexity
Threshold	Double-Logistic	P	**F**	P	P	P	**F**	P
	Triple-Logistic	P	**F**	P	P	P	**F**	P
	Double-Chebyshev	P	P	P	P	P	P	P
	Triple-Chebyshev	P	P	P	P	P	P	P
	Logisitc-Sine	P	**F**	P	**F**	**F**	P	P
	Logisitc-Sine-Logisitc	P	**F**	P	P	P	P	P
IEEE 754	Double-Logistic	P	P	P	P	P	P	P
	Triple-Logistic	P	P	P	P	P	P	P
	Double-Chebyshev	P	P	P	P	P	P	P
	Triple-Chebyshev	P	P	P	P	P	P	P
	Logisitc-Sine	P	P	P	P	P	P	P
	Logisitc-Sine-Logisitc	P	P	P	P	P	P	P
m-sequence		P	P	**F**	**F**	**F**	**F**	**F**

$\mu_{I2}(u_{C2})$ 값을 3.901에서 4까지 0.001 간격으로 100개의 제어변수를 고려하여 상관 특성을 분석한 결과이다. Double-Logistic, Logistic-Sine, Logistic-Sine-Logistic 맵에서는 제어변수가 3.901에 가까워질수록 상관 특성의 저하가 발생하여 자기 상관 평균값이 상대적으로 높게 나타났다. 반면, Chebyshev 계열 맵들은 제어변수가 변해도 우수한 자기 상관 특성을 유지하였으며, 특히 Triple-Chebyshev 맵은 m-수열과 유사한 수준의 상관 특성을 갖는 것을 확인할 수 있었다.

4.2 이진 수열의 랜덤 특성

NIST 테스트는 수열의 난수성을 평가하는 중요한 도구로, 수열이 예측 불가능하며 통계적으로 랜덤 수열에 가까운지를 검증하는 데 사용된다. 총 15개의 다양한 검증을 통해 수열의 품질을 다각도로 평가할 수 있으며, 이는 혼돈 수열 기반 의사 난수 생성기의 성능을 평가하는 중요한 지표로 활용된다.

표 3은 여섯 개의 연접 혼돈 맵과 m-수열에 대한 NIST 테스트 결과를 보여준다. 각 맵과 m-수열은 10^6 비트 길이의 100개 수열을 대상으로 하였으며, 연접 혼돈 맵들은 제어변수 $\mu_{I2}(u_{C2})=3.97$로 설정하였을 때의 결과이다. 표 3은 15개의 NIST 테스트 중에서 일부 중요한 테스트 결과만을 선별하여 제시하고 있으며, 각 테스트의 결과는 간단한 표기를 위해 통과(P)와 실패(F)로 표기한다.

표 3의 NIST 테스트 결과를 분석한 결과, 첫 번째 이진 맵핑 방식인 임계값 기반의 이진 변환 방식에서는 일부 테스트에서 수열들이 난수성을 충분히 보이지 못하고 실패(F)한 경우가 많음을 알 수 있다. 특히, Run Test와 Serial Test에서 여러 맵이 통과하지 못했다. 두 번째 이진 맵핑 방식인 IEEE 754 표준 기반의 방식에서는 모든 연접 혼돈 맵이 모든 테스트를 통과(P)하며, 예측 불가능한 난수성을 가지고 있음을 보였다. m-수열의 경우, 선형적 구조로 인해 수열 내에 예측 가능성이 존재할 수 있으며, 이러한 특성으로 인해 많은 테스트에서 통과하지 못하는 결과를 보였다.

V. 결 론

본 논문에서는 연접 혼돈 맵으로부터 생성된 출력 실수 수열의 동적 특성과 이진 변환 후 수열의 성능을 분석했다. 고려한 여섯 가지 연접 혼돈 맵은 Double-Logistic, Triple-Logistic, Double-Chebyshev, Triple-Chebyshev, Logistic-Sine, Logistic-Sine-Logistic 맵이며, 이들의 출력 실수 수열의 복잡성을 리아푸노프 지수(LE), 근사 엔트로피(ApEn), 순열 엔트로피(PE)를 사용하여 평가했다. 그 결과, Chebyshev 계열이 가장 높은 복잡성을 보였으며, Logistic 및 Sine 계열 맵도 일정 수준 이상의 성능을 보였다.

이후, 실수 수열을 두 가지 이진 변환 방식(임계값 기반 및 IEEE 754 표준 기반)으로 변환한 후 상관 특성과 랜덤 특성을 분석했다. 상관 특성 분석에서는 Triple-Chebyshev 맵이 m-수열과 유사한 수준의 상관 특성을 갖는 것을 확인할 수 있었다. 나머지 맵들도 제

어변수의 변화에 따라 상관 특성에서 약간의 저하는 있었으나, 전반적으로 우수한 성능을 보였다. 또한, 이들의 랜덤 특성 분석을 위해 NIST 테스트를 수행한 결과, IEEE 754 표준 기반 변환 방식은 모든 테스트를 통과하며 우수한 난수성을 보였다.

결론적으로, 연접 혼돈 맵을 기반으로 생성된 이진 수열은 다양한 초기값과 제어변수 설정을 통해 상관 및 랜덤 특성이 좋은 매우 많은 코드 집합을 생성할 수 있어, DSSS 시스템에 유연하게 적용될 수 있을 것이다. 또한, 우수한 상관 특성은 다중 사용자 환경에서 간섭을 최소화하고, 높은 난수성은 보안성이 중요한 시스템에서 예측 불가능한 패턴을 형성하여 데이터 보호와 무작위성 요구를 충족시킬 수 있을 것으로 기대한다. 이러한 특성으로 인해 연접 혼돈 맵 기반 수열은 DSSS 시스템에서 PN 코드로 적용될 수 있으며, 더 안전하고 강력한 통신 시스템 설계에 기여할 수 있을 것으로 기대된다.

References

[1] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd Ed., Boulder, CO, USA: Westview Press, 2003. (https://doi.org/10.4324/9780429502309)

[2] B. Hasselblatt and A. Katok, *A first course in dynamics: With a panorama of recent developments*, Cambridge University Press, 2003.

[3] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.,* vol. 48, no. 12, pp. 1498-1509, Dec. 2001. (https://doi.org/10.1109/TCSI.2001.972857)

[4] H. B. Ghobad and M. Clare D, "A chaotic direct-sequence spread spectrum communication system," *IEEE Trans. commun.*, vol. 42, no. 2/3/4, pp. 1524-1527, 1994. (https://doi.org/10.1109/TCOMM.1994.582834)

[5] F. Liu, S. Jia, X. Xu, and M. Tian, "Improved chaotic sequence generation method based on direct spread spectrum," *J. Physics: Conf. Series*, vol. 1237, no. 4, 2019. (https://doi.org/10.1088/1742-6596/1237/4/042006)

[6] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs,* vol. 57, no. 12, pp. 996-1000, Dec. 2010. (https://doi.org/10.1109/TCSII.2010.2083170)

[7] 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. (https://doi.org/10.1109/TCYB.2014.2363168)

[8] A. Michaels, "Digital Chaotic Communications," Ph.D dissertation, Georgia Inst. of Technol., 2009.

[9] E. Ott, *Chaos in Dynamical Systems*, New York: Cambridge University Press, 1993.

[10] F. Yuan, Y. Deng, Y. Li, and G. Chen, "A cascading method for constructing new discrete chaotic systems with better randomness," *Chaos, Interdiscipl. J. Nonlinear Sci.,* vol. 29, no. 5, 2019. (https://doi.org/10.1063/1.5094936)

[11] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electr.*, vol. 66, no. 2, pp. 1273-1284, Feb. 2019. (https://doi.org/10.1109/TIE.2018.2833049)

[12] T. Umar, M. Nadeem, and F. Anwer, "A new modified skew tent map and its application in pseudo-random number generator" *Comput. Standards Interfaces,* vol. 89, p. 103826, Apr. 2024. (https://doi.org/10.1016/j.csi.2023.103826)

[13] H. Choi, D. Kim, S. Chae, H.-Y. Song, Y. Lee, S. Shin, and H. Noh, "Analysis for binary chaotic sequences generated by cascade chaotic maps," *2023 Int. Conf. ICTC 2023*, Jeju, Korea, Oct. 2023. (https://doi.org/10.1109/ICTC58733.2023.10393257)

[14] H. Choi and H.-Y. Song, "Analysis of binary sequences generated by cascade chaotic maps," *KICS Fall Conf. 2023*, Gyeongju, Korea, Nov. 2023.

[15] M. J. Feigenbaum, "Quantitative universality for a class of nonlinear transformations," *J.*

Stat. Phys., vol. 19, no. 1, pp. 25-52, Jul. 1978. (https://doi.org/10.1007/BF01020332)

[16] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature,* vol. 261, no. 5560, pp. 459-467, Jun. 1976. (https://doi.org/10.1038/261459a0)

[17] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, 2nd Ed., New York, NY, USA: Oxford Univ. Press, 2001.

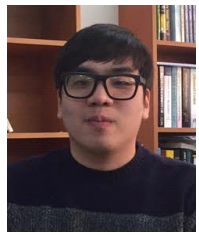
[18] S. M. Pincus, "Approximate entropy as a measure of system complexity," in *Proc. Nat. Acad. Sci.*, vol. 88, pp. 2297-2301, Mar. 1991. (https://doi.org/10.1073/pnas.88.6.2297)

[19] C. Bandt and B. Pompe, "Permutation entropy: A natural complexity measure for time series," *Phys. Rev. Lett.*, vol. 88, no. 17, 2002. (https://doi.org/10.1103/PhysRevLett.88.174102)

[20] D. Zuras, et al., "IEEE standard for floating-point arithmetic," *IEEE Std*, 754, pp. 1-70, 2008.

[21] M. Baldi, F. Chiaraluce, N. Boujnah, and R. Garello, "On the autocorrelation properties of truncated maximum-length sequences and their effect on the power spectrum," *IEEE Trans. Signal Process.*, vol. 58, 2010. (https://doi.org/10.1109/TSP.2010.2070500)

김 강 산 (Gangsan Kim)



2016년 2월 : 연세대학교 전기전자공학부 졸업
2016년 3월~현재 : 연세대학교 전기전자공학과 석박통합과정
2022년 5월~2023년 10월 : 육군교육사령부 인공지능과학기술연구병

<관심분야> 통신공학, 정보이론, 부호이론
[ORCID:0000-0002-3864-5379]

송 홍 엽 (Hong-Yeop Song)

1984년 2월 : 연세대학교 전자공학과 졸업
1986년 5월 : University of Southern California Dept. of EE. System 석사
1991년 12월 : University of Southern California Dept. of EE. System 박사
1992년 1월~1993년 12월 : University of Southern California 박사 후 연구원
1994년 1월~1995년 8월 : Qualcomm, San Diego, Senior Engineer
1995년 9월~현재 : 연세대학교 전기전자공학과 전임교수

<관심분야> 통신공학, 정보이론, 부호이론
[ORCID: 0000-0001-8764-9424]

최 효 정 (Hyojeong Choi)

2018년 2월 : 연세대학교 정보통신공학부 졸업
2021년 2월 : 연세대학교 전기전자공학과 석사
2021년 3월~현재 : 연세대학교 전기전자공학과 박사과정

<관심분야> 통신공학, 부호이론, 분산 저장 시스템, 카오스 이론
[ORCID:0000-0003-2305-5111]

신 상 웅 (Sangung Shin)

2021년 2월 : 인하대학교 전자공학과 졸업
2023년 2월 : 인하대학교 전자공학과 석사
2023년 2월~현재 : LIG넥스원 C4I연구소 연구원

<관심분야> 통신신호 처리, 모뎀 구현
[ORCID:0009-0008-1662-5327]

이 철 호 (Chulho Lee)

2005년 2월 : 건국대학교 전자정보통신공학과 졸업
2007년 2월 : 건국대학교 전자정보통신공학과 석사
2007년 3월~2012년 7월 : ㈜텔에이스 ASIC팀 선임연구원
2012년 7월~현재 : LIG넥스원 C4I연구소 수석연구원

<관심분야> 항재밍/저피탐 통신기법, 모뎀 구현

노 홍 준 (Hongjun Noh)

2008년 2월 : 아주대학교 정보및컴퓨터공학 학사
2015년 2월 : 아주대학교 컴퓨터공학 박사
2015년 3월~현재 : LIG넥스원 C4I연구소 수석연구원

<관심분야> 군위성 체계종합, 전술 네트워킹, 전술 데이터링크

[ORCID:0000-0001-6138-742X]