# Skew Tent 맵에 비트 확장 기법을 적용하여 생성된 의사 혼돈 수열에 대한 분석

최효정, 김강산, *노홍준, 송홍엽
연세대학교, *LIG 넥스원
{hjchoi3022, gs.kim, hysong}@yonsei.ac.kr, *hongjun.noh@lignex1.com

# Analysis of Pseudo Chaotic Sequences Generated by Applying Bit Expansion Technique to Skew Tent Map

Hyojeong Choi, Gangsan Kim, *Hongjun Noh, Hong-Yeop Song
Yonsei Univ., *LIG Nex1

요 약

본 논문은 디지털 시스템에서 혼돈 맵(Chaotic map)을 구현할 때 발생하는 동적 저하(dynamic degradation)를 개선하기 위한 기법인 비트 확장(Bit extension) 기법을 소개하고, Skew Tent 맵에 비트 확장 기법을 적용하여 생성된 의사 혼돈 수열(Pseudo-chaotic sequence)의 주기와 상관 특성을 분석한다.

## Ⅰ. 서 론

무한한 실수 영역에서 정의되는 혼돈 맵은 미세한 초기 값의 차이만으로도 무한한 주기를 갖는 수열을 쉽게 생성할 수 있어 통신 시스템 및 이미지 암호화 등 여러 응용 분야에서 널리 사용되고 있다. 하지만 혼돈 맵을 디지털 시스템에서 구현하는 경우, 유한 정밀도로 인해 연산의 오차가 발생하여 혼돈 맵의 정의와 달리 짧은 주기를 갖거나 임의의 값으로 수렴하는 등 동적 저하 현상이 발생한다. 이러한 동적 저하 현상을 개선하기 위해 여러 혼돈 맵을 연접하거나 연산 과정에서 특정 비트를 확장하는 등 다양한 연구가 이루어지고 있다[1-4].

[2]에서는 혼돈 맵의 동적 저하를 개선하고자 이진 시프트 혼돈 맵에서 LSB를 확장하는 기법이 제안되었고, 이 기법은 적용할 수 있는 맵과 파라미터가 한정적이다. [3]에서는 [2]의 기법을 변형하여 다양한 맵과 파라미터를 적용할 수 있는 비트 확장 기법을 소개하고 Logistic 맵과 Tent 맵에 해당 기법을 사용하여 생성된 의사 혼돈 수열의 주기와 여러 특성을 분석하였다.

본 논문에서는 Skew Tent 맵에 비트 확장 기법을 적용하여 생성된 의사 혼돈 수열의 주기와 상관 특성을 분석하고, [3]에서 Tent 맵에 비트 확장 기법을 적용한 경우와 비교하여 논의한다.

## Ⅱ. 본론

본 논문에서는 비트 확장 기법을 적용할 혼돈 맵으로 Digital Skew Tent 맵을 고려한다. 먼저, 실수 영역에서 정의된 Skew Tent 맵은 다음 식 (1)과 같다.

$$x_{n+1} = \begin{cases} \dfrac{x_n}{p}, & 0 \le x_n \le p \\ \dfrac{1-x_n}{1-p}, & p < x_n \le 1 \end{cases} \quad (1)$$

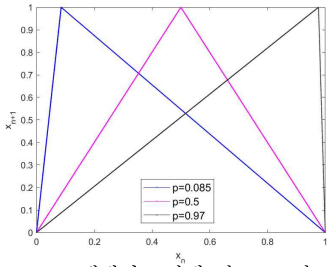


그림 1. Skew Tent 맵에서 $p$값에 따른 $x_n$과 $x_{n+1}$의 관계

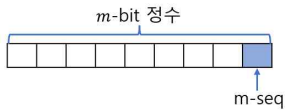


그림 2. m-수열을 사용한 비트 확장 기법

여기서 $0 < p < 1$이다. 그림 1은 $p$에 따른 $x_n$과 $x_{n+1}$사이의 관계를 보여준다. 0부터 1까지의 실수 상에서 정의된 식 (1)의 맵을 디지털 버전으로 변형하여 맵의 출력을 1부터 $2^m$까지의 정수로 표현할 수 있는 Digital Skew Tent 맵이 [5]에서 계산되었으며, 본 논문에서는 비트 확장 기법에 적용을 위해 맵의 출력을 0부터 $2^m-1$까지의 $m$비트 정수로 표현할 수 있도록 Digital Skew Tent 맵을 다음 식 (2)와 같이 변형하였다.

$$z_{n+1} = \begin{cases} \left\lfloor \dfrac{(z_n+1)2^m}{a} \right\rfloor - 1, & 0 \le z_n \le a-1 \\ \left\lfloor \dfrac{2^m(2^m-(z_n+1))}{2^m-a} \right\rfloor, & a-1 < z_n \le 2^m-1 \end{cases} \quad (2)$$

여기서 $1 < a \le 2^m-1$이다.

[3]에서 소개한 비트 확장 기법은 디지털 혼돈 맵을 구현할 비트 정밀도 $m$을 선택하고 그림 2의 예시와 같이 고정소수점 연산에서 특정 비트를 m-수열로 확장 시키는 기법이다. 먼저 식 (2)에서 $m=7$인 경우 마지막

표 1. 7비트 연산으로 생성된 Digital Skew Tent 맵의 출력 수열과 비트 확장 기법을 적용하여 생성된 수열의 주기 비교

| $a$ | 식(2)의 주기 | 비트 확장 후 주기 |
|---|---|---|
| 55 | 2, 56, 70 | 127, 508, 2032, 5461 |
| 56 | 1, 2, 29, 96 | 1905, 6223 |
| 57 | 2, 3, 30, 93 | 127, 1397, 2794, 3810 |
| 58 | 1, 3, 9, 115 | 127, 254, 762, 1397, 5461 |
| 59 | 4, 14, 32, 37, 41 | 381, 1778, 2413, 3556 |
| 60 | 2, 4, 118 | 381, 1524, 2159, 4064 |
| 61 | 3, 6, 16, 22, 29, 52 | 127, 254, 508, 762, 1270, 5207 |
| 62 | 10, 30, 31, 57 | 127, 254, 508, 762, 1016, 5334 |
| 63 | 1, 7, 8, 11, 24, 37 | 127, 508, 2794, 4445 |
| 64 | 8 | 127, 889 |
| 65 | 1, 127 | 127, 889 |
| 66 | 5, 123 | 254, 635, 762, 6477 |
| 67 | 1, 48, 79 | 889, 1016, 1778, 4445 |
| 68 | 8, 9, 10, 14, 16, 24, 37 | 127, 1143, 6731 |

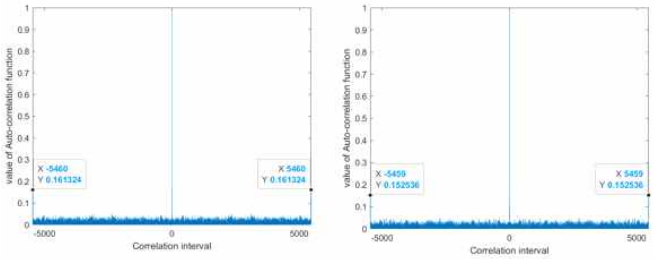


그림 3. $a=55$일 때 비트 확장 후(좌) 이진 맵핑 후(우)

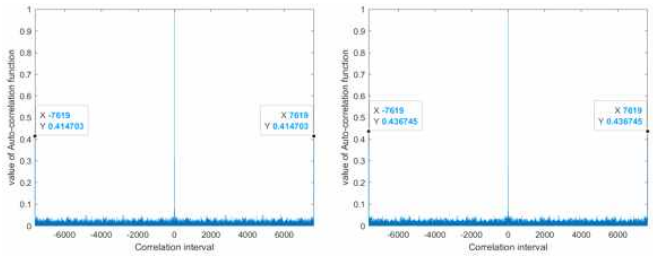


그림 4. $a=92$일 때 비트 확장 후(좌) 이진 맵핑 후(우)

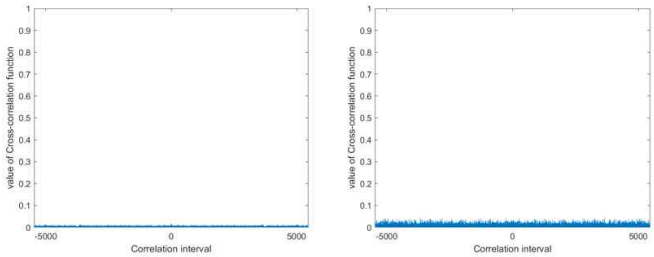


그림 5. $a=55$인 경우와 $a=92$인 경우의 상호 상관

비트에 비트 확장 기법을 적용하기 전과 후의 주기를 일부 $a$값에 대해 표 1에 나타내었다. 비트 확장을 적용한 경우에는 마지막 비트의 확장을 위해 생성 다항식 $x^7+x+1$을 사용하여 생성된 주기 127인 m-수열을 사용하였다. 표 1에서 볼 수 있듯이 5비트 연산으로 생성된 Digital Skew Tent 맵의 출력 수열은 아주 짧은 주기를 갖지만, 주기 31인 m-수열로 LSB를 확장 시킨 경우에는 주기가 크게 증가하였다. 본 논문에는 일부 $a$ 값에 대해서만 표에 나타내었지만, 실험 결과 가능한 모든 $a$값에 대해 주기가 크게 확장됨을 확인하였다.

[3]에서는 동일한 방식을 Tent 맵 연산에 적용하였는데, Tent 맵 연산에서 위 실험과 동일하게 마지막 비트를 확장하는 경우에는 대부분의 fractal parameter에 대해서 비트 확장을 위해 사용한 m-수열의 주기정도로만 주기가 확장되었고, 일부 fractal parameter에 대해서는 주기가 크게 증가하였다. 즉, 비트 확장 기법은 Tent에 적용하는 경우보다 Digital Skew Tent 맵에 적용하는 경우에 주기 확장에 있어서 더 효과적임을 알 수 있다.

그림 3은 7비트 연산에서 $a=55$인 경우에 비트 확장 기법을 적용하여 출력된 수열의 자기 상관 특성과 이진 맵핑 후의 자기 상관 특성을 보여준다. 이진 맵핑은 해당 출력 수열의 정수 원소가 64보다 같거나 작으면 0으로 맵핑하고, 64보다 크면 1로 맵핑하여 이진 수열로 변형하였다. 그림 4는 $a=92$인 경우에 비트 확장 기법을 적용하여 출력된 수열의 자기 상관 특성과 이진 맵핑 후의 자기 상관 특성을 보여준다. 모든 $a$값에 대해 자기 상관 특성을 분석해 본 결과 사이드로브의 특정 위치들에서 피크값이 존재하는 것을 확인하였다. 따라서 추후 연구로서 자기 상관 특성을 개선시킬 수 있는 방안에 대한 연구가 필요하다.

그림 5는 $a=55$인 경우와 $a=92$인 경우의 상호 상관 특성을 보여준다. 각 수열의 주기가 5461과 7620으로 상이하므로 짧은 주기인 5461로 길이를 맞추고 실험을 진행하였다. 실험 결과 $a$값을 달리하는 경우 출력 수열의 상호 상관 특성이 우수한 것을 확인했다.

## ACKNOWLEDGMENT

이 (성과)는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2023-00209000).

## 참 고 문 헌

[1] 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.

[2] 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.

[3] 최효정, 김강산, 노홍준, 송홍엽, “디지털 혼돈 맵의 동적 저하 개선을 위한 비트 확장 기법,” 제 34회 통신정보 합동학술대회 (JCCI 2024).

[4] L. Liu, J. Wang, “A shift coupling digital chaotic model with counteracting dynamical degradation,” *Nonlinear Dyn.* vol. 111, no. 20, pp. 19459 - 19486, 2023.

[5] C.L. Fan, Q. Ding, “Analyzing the period distribution of digital chaos with graph theory,” *Phys. Scr.* vol. 96, no. 8, 2021.