Period and autocorrelation of some pseudo chaotic sequences with LSB extension by m-sequences

Hyojeong Choi, Sangwon Chae, Daekyeong Kim , Hong-Yeop Song
Yonsei University

Yundong Lee, Sangung Shin, Hongjun Noh
LIG Nex1

This paper analyzes the period and autocorrelation properties of pseudo chaotic sequences generated using the Least Significant Bit (LSB) extension method for the digital implementation of chaotic systems. For the application of the LSB extension method, we consider Bernoulli maps, Tent maps, and Chebyshev maps. We employed m-sequences for LSB extension, and we confirmed that the resulting pseudo chaotic sequences have some periodic orbits due only to the period of the m-sequence and some ideal autocorrelation properties.

Introduction

- Chaotic maps are nonlinear functions sensitive to initial values, resulting in distinct outcomes for slightly different initial values, enabling the generation of infinite non-periodic signals.
- Chaotic sequences in digital systems using fixed or floating-point arithmetic may converge to some value or exhibit short periods due to round-off and truncation errors.
- To overcome digital implementation challenges, particularly in cryptography, the LSB extension method has been proposed [5,6]. It avoids fixed or floating-point arithmetic and instead utilizes logical operations (e.g., AND, OR, NOT).
- The LSB extension method for Binary Shift Chaotic Maps (BSCMs) in [5] uses a PRNG to generate pseudo chaotic and true periodic sequences.
- The BSCM is defined as chaotic maps where multiplications are binary shift operations and do not have overflows during additions.
- This paper analyzes the period and autocorrelation properties of pseudo chaotic sequences generated by BSCMs based on the algorithm proposed in [5].

Binary Shift Chaotic Maps

- **Bernoulli map** $S : [0,1) \to [0,1)$ is defined as follows

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

The Bernoulli map S involves only the operation of doubling x, which can be described as discarding the most significant bit and performing a left shift operation by one position.

- **Tent map** $T : [0,1] \to [0,1]$ is defined as follows

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

The implementation of Tent map is essentially the same as the Bernoulli map, with the only difference being the application of the operation $(1 - x)$.

- **Chebyshev map** $f : [-1,1] \to [-1,1]$ defined as follows

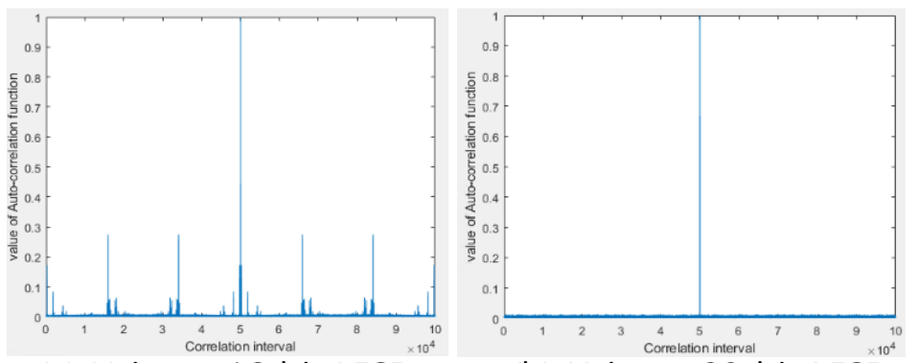
$$f(x) = 8x^4 - 8x^2 + 1$$

The operation of this map can be implemented by applying the twice iterated Bernoulli map $S^2 = S \circ S$ and its conjugate function $h(x) = \cos(2\pi x)$.

LSB Extension Method

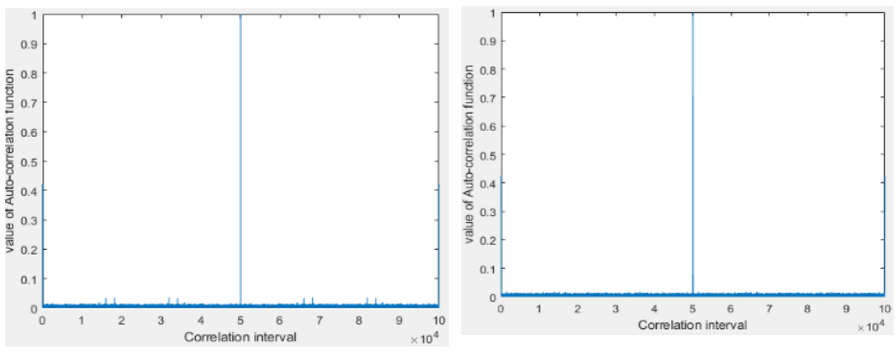
- In this approach, all operations are conducted on an L-bit memory unit representing the initial L bits of binary numbers. When performing a k-bit left shift, the least significant k bits become zeros. In such cases, these zeros are replaced by random bits using a PRNG.
- In this paper, we consider m-sequences generated by 16-bit and 32-bit LFSRs as the PRNGs used for LSB extension.

Period and Autocorrelation Properties



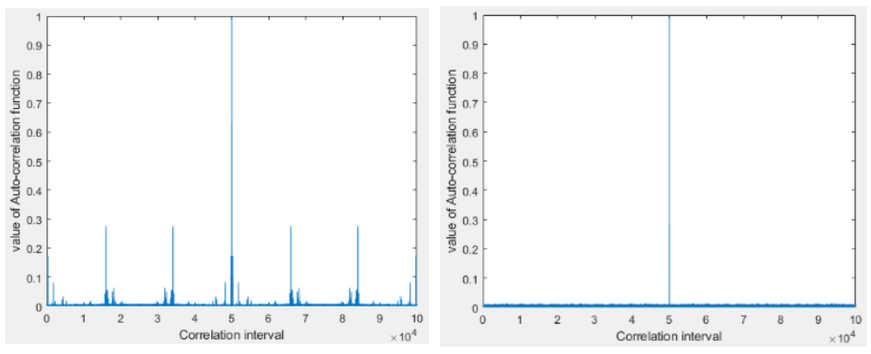
(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 1. The autocorrelation of the output sequences of ***Bernoulli map***



(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 2. The autocorrelation of the output sequences of ***Tent map***



(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 3. The autocorrelation of the output sequences of ***Chebyshev map***

- The Bernoulli map and the Chebyshev map undergo simple left shift operations, so they have the same period as the used m-sequence.
- Tent map incorporates not only simple left shift operations but also a process of taking complements for L bits. Its period becomes the product of the period of the m-sequence and the number of memory units.

REFERENCES

[5] 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.

[6] I. Öztürk and R. Kilic, "Utilizing true periodic orbits in chaos-based cryptography," *Nonlinear Dynamics*, vol.103, pp. 2805-2818, 2021.