Analysis for binary chaotic sequences generated by cascade chaotic maps

Hyojeong Choi, Daekyeong Kim, Sangwon Chae, Hong-Yeop Song
School of Electrical and Electronic Engineering
Yonsei University
Seoul, Korea
{hjchoi3022, daky33, sw.chae, hysong}@yonsei.ac.kr

Yundong Lee, Sangung Shin, Hongjun Noh
Tactical Communication Systems Waveform R&D, LIG Nex1
Gyeonggi-do, Korea
{yundong.lee, sangung.shin, hongjun.noh}@lignex1.com

***Abstract*—This paper analyzes the characteristics of sequences generated using cascade chaotic maps employing two or three seed maps. We begin by comparing their Lyapunov exponents and also propose a new conjecture for the Lyapunov exponent of a cascade chaotic map using three seed maps. Furthermore, their real-valued output sequences are translated into binary sequences using two distinct binary mapping methods. Subsequently, we compare the correlation and balance properties of each converted binary sequence, and show the results of statistically validating these sequences by NIST SP 800-22.**

***Index Terms*—DSSS, PN code, Chaotic map, Lyapunov exponent**

I. Introduction

In general, a chaos means a state of disorder. These terms are frequently used in dynamic systems and were defined by R. L. Devaney [2], [6]. The chaotic map is a nonlinear function characterized by its sensitivity to initial values, where even slight differences in initial values can lead to completely distinct outcomes. Due to this characteristic, it becomes possible to easily generate infinitely different sequences solely by varying the initial values.

The PN codes used in conventional Direct Sequence Spread Spectrum (DSSS) systems have the fixed period, which limits the size of the sequence set. On the other hand,, sequences generated by chaotic maps can produce an infinite number of non-periodic signals with strong correlation characteristics, solely based on differences in initial values. Therefore, the use of chaotic sequences in existing DSSS systems employing PN codes has been studied [3], [8]–[10].

Directly proving the chaotic performance of chaotic map is a highly challenging task. Lyapunov Exponents (LE) can be utilized to explain the chaotic behavior of a chaotic system, as they provide a quantitative description of the variation between two adjacent output values in a dynamic system [7], [15]. The application of one-dimensional traditional chaotic maps in more secure communications has been a subject of extensive research, driven by the relatively small parameter space and low LEs. Efforts have been made to enhance the LE for improved security communication purposes [1], [7], [11], [14], [15]. In [7] and [15], the authors proposed a Cascade Caotic system with better chaotic behavior than single maps.

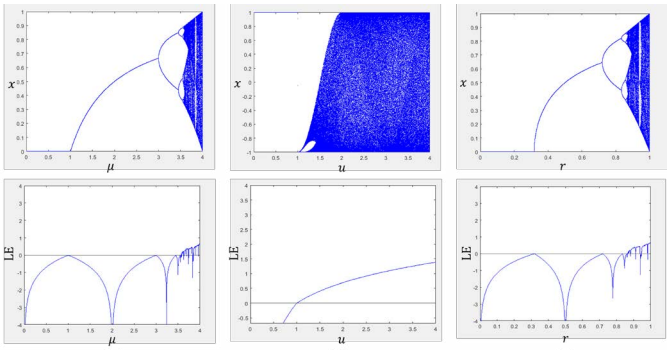

Fig. 1. The first and second rows are bifurcation diagrams and Lyapunov exponents of (a) logistic map, (b) Chebyshev map, and (c) sine map.

In [7] and [15], a cascade chaotic system (CCS) with better chaotic behavior than one-dimensional maps using two seed maps was introduced. By combining two existing one-dimensional chaotic maps, a new one-dimensional chaotic map can be generated. In [7], LE is employed for analyzing the chaotic performance of a CCS using two seed maps. Ultimately, it conclude that the combination of the LE values of the two seed maps was established for the case of a CCS employing two seed maps.

In this paper, we further extend our consideration to a CCS employing three seed maps. Furthermore, we compare the binary sequences generated by the pseudorandom number generators (PRNGs) proposed in [7] with the binary sequences generated by the Threshold method.

In Section II, we introduces some traditional chaotic maps. In Section III, we introduce CCS. In Section IV, we analyze the properties of binary sequences generated by two binary mapping schemes. Section V concludes the paper with some concluding remarks.

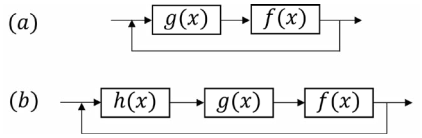

Fig. 2. $g(x), h(x)$ and $f(x)$ are chaotic seed maps. (a) and (b) are the structure of CCS applied with two and three seed maps, respectively.

II. Traditional Chaotic Maps

In this section, we briefly review the three chaotic maps. The three maps under consideration here will be employed as seed maps for the CCS.

A. Logistic map

The Logistic map, which is widely used as a discrete chaotic map, was first introduced as a statistical model in [12]. The Logistic map is defined

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

where $0 \leq \mu \leq 4$, $x_n \in [0, 1]$, and x_{n+1} is the iterative result. When the fractal parameter $\mu \in [3.57, 4]$, the Logistic map is in chaotic state. Figure 1(a) shows the Lyapunov exponent and bifurcation diagram of the Logistic map.

B. Chebyshev map

The Chebyshev map, initially investigated in [4], is a chaos map developed in the form of Chebyshev polynomials. The Chebyshev map is defined

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

where $0 \leq u \leq 4$, $x_n \in [-1, 1]$, and x_{n+1} is the iterative result. When the fractal parameter $u \geq 2$, the Chebyshev map is in chaotic state. Figure 1(b) shows the Lyapunov exponent and bifurcation diagram of the Chebyshev map.

C. Sine map

The sine map is an traditional chaotic map displaying chaotic behaviors, and it shares a strong resemblance to the logistic map [5]. The Sine map is defined

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

where $0 \leq r \leq 1$, $x_n \in [0, 1]$, and x_{n+1} is the iterative result. When the fractal parameter $u \in [0.867, 1]$, the Sine map is in chaotic state. Figure 1(c) shows the Lyapunov exponent and bifurcation diagram of the Sine map.

III. Cascade Chaotic Maps

In [7] and [15], a CCS using two seed maps was introduced. As illustrated in Figure 2(a), by combining two existing one-dimensional chaotic maps, a new one-dimensional chaotic map can be generated. The output of function $g(x)$ is utilized as the input for function $f(x)$, and subsequently, the output of function $f(x)$ is fed back as the input for function $g(x)$ for recursive iterations. Mathematically, the CCS using two seed maps is defined in the following:

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

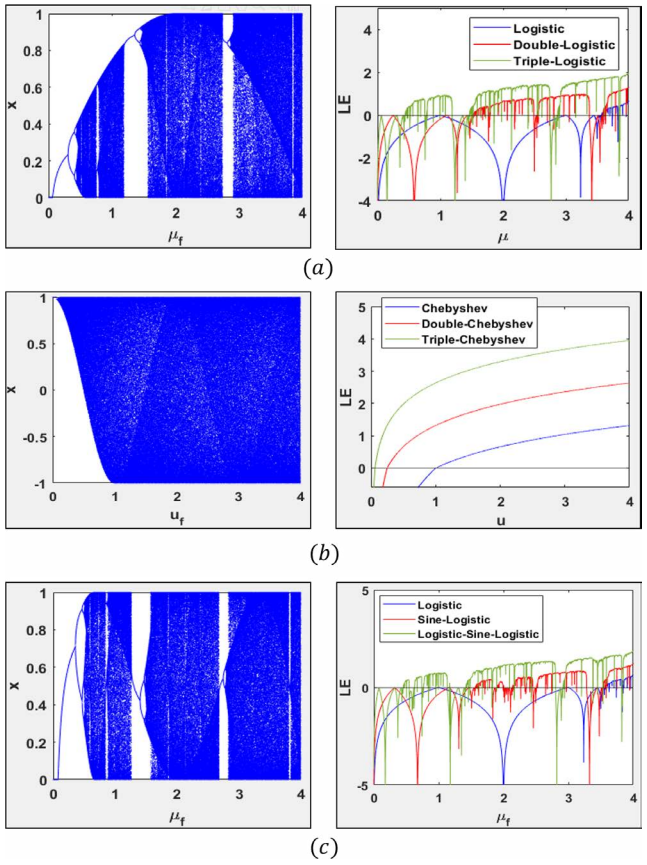

Fig. 3. The left columns of (a), (b), and (c) show the bifurcation diagrams of the Triple-Logistic map, Triple-Chebyshev map, and Logistic-Sine-Logistic map, respectively. The second column is the LE of CCS.

In this paper, we further extend our consideration to a CCS employing three seed maps, as depicted in Figure 2(b). In a similar manner to the case where two seed maps are employed, the CCS using three seed maps is defined as follows:

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

Existing one-dimensional chaotic maps can serve as seed maps for the CCS. Users have the flexibility to configure the seed maps $f(x), g(x)$, and $h(x)$ as identical or distinct chaotic maps.

A. Lyapunov Exponent

In [7] and [15], LE is employed for analyzing the chaotic performance of a CCS using two seed maps. Ultimately, it conclude that the combination of the LE values of the two seed maps was established for the case of a CCS employing two seed maps, as follows:

$$\lambda_{\Gamma(x)} = \lambda_{f(x)} + \lambda_{g(x)}, \tag{6}$$

where $\lambda_{f(x)}$ and $\lambda_{g(x)}$ are LEs for $f(x)$ and $g(x)$, respectively.

In this paper, we further extend our consideration to a CCS employing three seed maps, as depicted in Figure 2(b). We hereby examine the following six CCS: the Double-Logistic map, Triple-Logistic map, Double-Chebyshev map,

TABLE I
CORRELATION PROPERTIES FOR BINARY CHAOTIC SEQUENCES AND M-SEQUENCE

Classification	**Length:** 10000 Initial value: $0.4001 - 0.4100$				**Length:** 100000 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								
Triple-Logistic								
Double-Chebyshev	≈ 0.008	≈ 0.04	≈ 0.008	≈ 0.04	≈ 0.002	≈ 0.01	≈ 0.002	≈ 0.01
Triple-Chebyshev	≈ -21dB	≈ -14dB	≈ -21dB	≈ -14dB	≈ -27dB	≈ -20dB	≈ -27dB	≈ -20dB
Logisitc-Sine								
Logisitc-Sine-Logisitc								
m-sequence	≈ 0.006 ≈ -22dB	≈ 0.02 ≈ -16dB	–	–	≈ 0.001 ≈ -28dB	≈ 0.007 ≈ -21dB	–	–

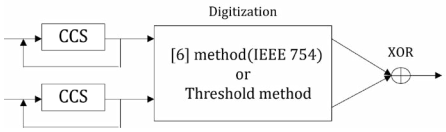

Fig. 4. Structure of PRNG

Triple-Chebyshev map, Logistic-Sine map, and Logistic-Sine-Logistic map. Where, the Double-Logistic map means the case where $g(x)$ and $f(x)$ are logistic maps with distinct fractal parameters, and the Triple-Logistic map is also in a similar manner.

Figure 3 shows their bifurcation diagrams and Lyapunov exponent. In Figure 3, The left columns of (a), (b), and (c) show the bifurcation diagrams of the Triple-Logistic map, Triple-Chebyshev map, and Logistic-Sine-Logistic map, respectively. The second column is the LE of CCS. As mentioned earlier, the positive Lyapunov Exponents (LE) of a dynamic system signify the substantial divergence of trajectories from extremely close initial values in successive iterations. Larger positive LE values indicate faster divergence of output trajectories, thus implying superior chaotic performance.

One can observe that, CCSs employing three seed maps have larger LE values than employing two seed maps in most parameter ranges.

Based on the result presented in Figure 3, we can expect that the LE of the CCS employing three seed maps can be anticipated as a combination of the LE values of each individual seed map. Consequently, we formulate the conjecture for the LE of the CCS employing three seed maps as follows:

$$\lambda_{\Gamma(x)} = \lambda_{f(x)} + \lambda_{g(x)} + \lambda_{h(x)}, \tag{7}$$

where $\lambda_{f(x)}, \lambda_{g(x)}$ and $\lambda_{h(x)}$ are LEs for $f(x), g(x)$ and $h(x)$, respectively.

IV. PSEUDO-RANDOM NUMBER GENERATORS

In this paper, the real-valued output sequences of CCSs are translated into binary sequences using two distinct binary mapping methods. Figure 4 shows the block diagram of PRNG for CCSs.

In digitization, the method of [15] outputs an 8-bits binary mapping sequence of an 8-bits symbol sequence. The method for generating an 8-bit symbol sequence in [15] involves converting a 52-bit binary sequence based on the IEEE 754 standard and subsequently truncating it to 8 bits. Therefore, whenever CCS is iterated, an 8-bit binary sequence is output and concatenated. The second method involves mapping each x_n value to binary using half of the range of x_n corresponding to each map as a threshold. We will call this the "Threshold method".

We now proceed to generate binary chaotic sequences using the [15] method and the Threshold method, as illustrated in Figure 4. Subsequently, we compare the characteristics of these sequences.

A. Correlation property

To analyze the correlation property, we consider binary sequences of lengths $10,000$ and $100,000$ for both binary mapping methods illustrated in Figure 4. In addition to comparing the binary sequences generated by the six CCSs mentioned in III-A, we also compare them with the auto-correlation of m-sequences widely employed as PN codes.

The initial values for each map are considered from 0.4001 to 0.4100 at intervals of 0.0001, as shown in the Table I. We observe the average auto-correlation and cross-correlation values of the 100 binary sequences corresponding to these 100 initial values.

In Table I, the sidelobe average of auto-correlation means the total average of all sidelobes excluding the peak value (here, 1 because it is the normalized version). The sidelobe

TABLE II
BALANCE PROPERTIES FOR BINARY CHAOTIC SEQUENCES USING TWO DISTINCT BINARY MAPPING METHOD

Classification	Length: 10000 Initial value: $0.4001 - 0.4100$			
	0 Average Percentage		1 Average Percentage	
	[15] method	Threshold	[15] method	Threshold
Double-Logistic	49.9898	49.9767	50.0102	50.0233
Triple-Logistic	50.0285	50.0581	49.9715	49.9419
Double-Chebyshev	49.9731	49.9442	50.0269	50.0558
Triple-Chebyshev	50.0076	50.0068	49.9924	49.0068
Logisitc-Sine	50.0243	50.2240	49.9757	49.7760
Logisitc-Sine-Logisitc	49.9675	50.0081	50.0325	49.9919

TABLE III
RESULTS OF NIST STATISTICAL TEST FOR BINARY CHAOTIC SEQUENCES USING TWO DISTINCT BINARY MAPPING METHOD AND M-SEQUENCE

Classification		Frequency	Run	Rank	DFT	Linear Comp.	Cusum
Double-Logistic	[15] method	0.739918	0.911413	0.213309	0.534146	0.350485	0.911413
	Threshold	0.534146	0.739918	0.122325	0.017912	0.739918	0.350485
Triple-Logistic	[15] method	0.739918	0.991468	0.534146	0.350485	0.739918	0.534146
	Threshold	0.350485	0.534146	0.739918	0.122325	0.739918	0.350485
Double-Chebyshev	[15] method	0.911413	0.122325	0.122325	0.122325	0.122325	0.213309
	Threshold	0.319084	0.595549	**0.000000**	**0.000320**	0.162606	0.534146
Triple-Chebyshev	[15] method	0.213309	0.739918	0.350485	0.911413	0.350485	0.534146
	Threshold	0.115387	0.181557	**0.002374**	0.213309	0.102526	0.437274
Logisitc-Sine	[15] method	0.534146	0.350485	0.534146	0.213309	0.350485	0.534146
	Threshold	0.213309	0.122325	0.739918	0.534146	0.534146	0.122325
Logisitc-Sine-Logisitc	[15] method	0.739918	0.213309	0.122325	0.911413	0.213309	0.739918
	Threshold	0.066882	0.911413	0.739918	0.213309	0.350485	0.739918
m-sequence		0.262249	0.224821	**0.000000**	**0.000320**	**0.000000**	**0.002559**

max average of auto-correlation is the average of the sidelobe max values for 100 sequences. The cross-correlation average means the total average of all cross correlations corresponding to 100 sequences. And Max average of cross-correlation means the average of the maximum cross-correlation values of each sequence.

In Table I, the results are highly similar for the two binary mapping methods we are considering, so they are not indicated separately. The m-sequence used in Table Table I generated a longer m-sequence than the length of the sequence being considered, and the experiment was conducted with its truncated version. As a result of observation, the m-sequence has about 1dB better auto-correlation than the binary chaotic sequences. In addition, all values exhibit an improvement of approximately 6dB in correlation performance as the sequence length increases by a factor of 10.

B. Balance property

We analyze the balance property according to two binary mapping methods. The sequence lengths and initial values are provided in Table II. Table II shows the average ratio of 0 and 1 of sequences generated by two binary mapping methods with 100 initial values. According to the experimental results, it can be observed that the ratio of 0s and 1s is uniform for all cases.

C. NIST SP 800-22 Statistical Test

NIST statistical tests (called NIST SP 800-22) are based on testing hypotheses, the testing is a procedure for determining whether claims about characteristics of a population are acceptable. That test involves determining whether a particular sequence is random (this is called the null hypothesis). For each test, the relevant randomness statistic be selected and used to determine the acceptance or rejection of the null hypothesis. Under the null hypothesis, the theoretical reference distribution of this statistic is determined by mathematical methods and a corresponding probability value (P-value) is

calculated that summarizes the strength of evidence for the null hypothesis. A P-value calculated for each test greater than 0.01 means that the test is satisfied with 99% confidence [13]. We have suitably selected 6 test (Frequency, Rank, Run, DFT, Linear Complexity, Cumulative Sum) out of 15 tests for binary pseudorandom sequences, and the test results for the two binary mapping methods are shown in Table III.

The number of bitstreams required for the test is set to 100, and the length of the bitstream is set to 10000. The parameters related to the testing are applied the same as the initial value of NIST 800-22. Table 3 shows the NIST test results of binary chaos sequences generated by two different mapping methods, as well as the NIST test results of truncated m-sequences of the same length.

When [15] method is used, it is acceptable in all tests. For Threshold method, it is not acceptable in Rnak and DFT tests when Chebyshev map is used as a seed map. This implies the need for an analysis to choose an appropriate threshold in digitization. The m-sequence is not acceptable for most tests.

V. CONCLUSION

This paper analyzes the characteristics of sequences generated using cascade chaotic maps employing two or three seed maps. To determine the sensitivity to tinitial values, we calculate the LE for each map. Based on the results, we propose a new conjecture for the LE of the cascade chaotic map using three seed maps. The real-valued output sequences of cascade chaotic systems are converted to the binary sequences using two binary mapping methods. The binary sequences generated in this manner exhibit good correlation and balance properties. In addition, as a result of the NIST test, this is acceptable in all tests when using the [15] method, but not in the Rnak and DFT tests when using the Chebyshev map as the seed map for the threshold method. This implies the need for an analysis to choose an appropriate threshold in digitization. The binary sequence generated by the chaotic map can generate an infinite number of signals with non-periodic, good correlation and balance characteristics even with very small differences in initial values. Therefore, it is expected that the use of chaotic binary sequences can be considered in the existing DSSS system using PN codes.

ACKNOWLEDGMENT

This work was supported by Korea Research Institute for defense Technology planning and advancement(KRIT) grant funded by the Korea government(DAPA(Defense Acquisition Program Administration)). (No. 11-202-205-010(KRIT-CT-22-086, Aperiodic, non-predictable, randomness and denseness signaling ultra-low-probability-of-detection and covert communication technology, 2023.)

REFERENCES

[1] G. Ablay, "Lyapunov Exponent Enhancement in Chaotic Maps with Uniform Distribution Modulo One Transformation," *Chaos Theory Appl.*, vol 4, pp. 45–58, 2022.

[2] R. L. Devaney, *An introduction to chaotic dynamical systems*, CRC press, 2003.

[3] H.B. Ghobad and M. Clare D, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Transactions on communications*, vol 42, no. 2/3/4, pp.1524-1527, 1994.

[4] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Physics Letters*, vol. 105, no. 6, pp. 263-266, Aug. 1984.

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

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

[7] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.

[8] H. Jiang and C. Fu, "A chaos-based high quality PN sequence generator," *International Conference on Intelligent Computation Technology and Automation*, pp. 60-64, 20–22 October 2008.

[9] T. Kohda and A. Tsuneda, "Pseudonoise sequences by chaotic nonlinearmaps and their correlation properties," *IEZCE Trans.*, vol. E76-B, no. 8, pp. 855-862, 1993.

[10] F. Liu, S. Jia, X. Xu and M. Tian, "Improved Chaotic Sequence Generation Method Based on Direct Spread Spectrum." *Journal of Physics: Conference Series*, vol. 1237, no. 4, 2019.

[11] C. Li, K. Qian, S. He, H. Li and W. Feng, "Dynamics and optimization control of a robust chaotic map," *IEEE Access*, vol. 7, pp. 160072–160081, 2019.

[12] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no.5560, pp. 459–467, June 1976.

[13] A. L. Rukhin et al., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22, Apr. 2010.

[14] 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.

[15] 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.