Bit extension method for improving dynamic degradation of digital chaotic maps

Hyojeong Choi, Gangsan Kim, Hongjun Noh*, Hong-Yeop Song

dept. of Electrical and Electronic Engineering
Yonsei University
Seoul, Republic of Korea

dept. of C4I R&D Center
LIG Nex1*
Gyeonggi-do, Korea

ICMIC 2024

Contents

Introduction

- Chaotic maps are nonlinear functions that are very sensitive to initial values. Even small differences in initial values can lead to completely different sequences.

- Because of this property, changing the initial value can easily generate infinitely different sequences.

- Therefore, in DSSS (Direct Sequence Spread Spectrum) systems, chaotic sequences are considered instead of PN (Pseudo Random Noise) codes, which have fixed periods and limited sequence sets [2], [5], [6].

Introduction

- When implemented in digital systems, chaotic maps defined in the real number domain face dynamic degradation.
- This dynamic degradation can result in chaotic maps having short periods or converging to specific values [4], [7].
- This paper introduces a bit extension method to improve dynamic degradation.
- We apply the bit extension method to single and combined chaotic maps to analyze their periods and randomness.

Contents

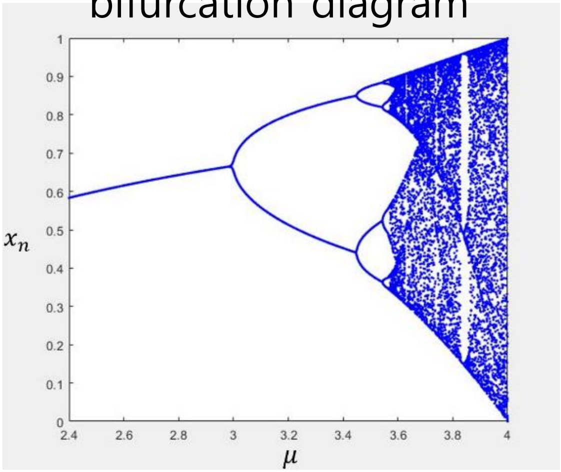
Chaotic Maps

❖ Logistic map

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

where, $0 < \mu \leq 4$ and $x_n \in [0,1]$.

bifurcation diagram

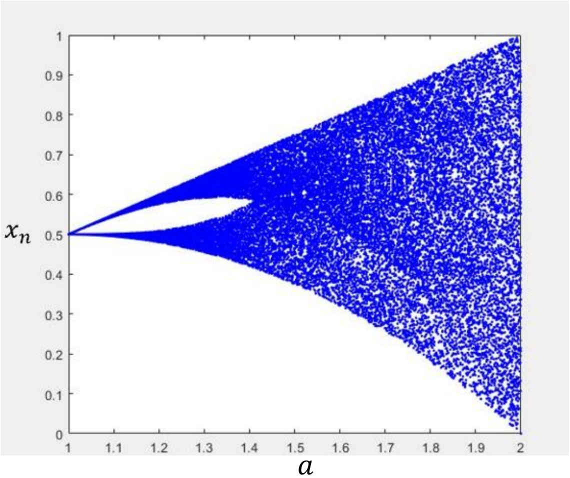


Chaotic state when $\mu = 4$

❖ Tent map

$$x_{n+1} = \begin{cases} a x_n, & 0 \leq x_n \leq 1/2 \\ a(1 - x_n), & 1/2 \leq x_n \leq 1 \end{cases}$$

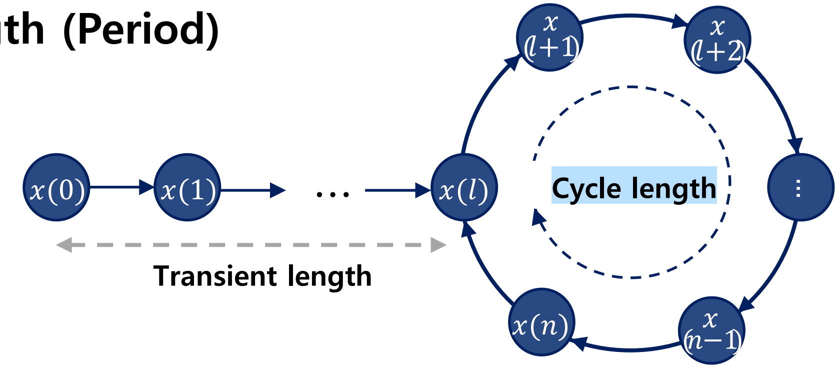
where, $1 < a \leq 2$ and $x_n \in [0,1]$.



Chaotic state when $a = 2$

Analysis metrics

➢ **Cycle length (Period)**



Typical orbit of a digital chaotic sequence

➢ **Random properties**

- Shannon Entropy (SE)
- Approximate Entropy (ApEn)
- Permutation Entropy (PE)

Analysis metrics

➢ **Random properties**

- **Shannon Entropy (SE)**
- Approximate Entropy (ApEn) [11]
- Permutation Entropy (PE) [1]

✓ **When the probability mass function of the discrete random variable X is $p(x)$, SE is defined as,**

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

✓ **Cannot distinguish complexity differences in sequences**

➢ ex) $p(x=1) = 0.5, \; p(x=0) = 0.5$

$$X_1 = [1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0]$$
$$X_2 = [1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0]$$
$$H(X_1) = H(X_2) = -\sum_{i=1}^{2} p(x=i)\log p(x=i) = -2(0.5 * \log 0.5)$$

Analysis metrics

➢ **Random properties**

- Shannon Entropy (SE)
- **Approximate Entropy (ApEn) [11]**
- Permutation Entropy (PE) [1]

✓ **Measures the likelihood that patterns of length m will remain similar in the next window of length $m+1$ (in logarithmic form)**

$$\mathbf{ApEn}(m) = \Phi^{m} - \Phi^{m+1}$$

✓ **Higher ApEn indicates more complex, less predictable sequences.**

[11] S. M. Pincus, ''Approximate entropy as a measure of system complexity,'' Proc. Nat. Acad. Sci. USA, vol. 88, pp. 2297–2301, Mar. 1991.

Analysis metrics

- **Random properties**
  - Shannon Entropy (SE)
  - Approximate Entropy (ApEn) [11]
  - **Permutation Entropy (PE) [1]**

✓ **Measuring complexity by considering the order of elements within a sequence**

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

- Consider the size of elements

(4,7,9) represent the permutation π_1 =(1,2,3).
(7,9,10) represent the permutation π_1 =(1,2,3).
(9,10,6) represent the permutation π_4 =(2,3,1)
⋮

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

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

[1] C. Bandt and B. Pompe, “Permutation entropy: A natural complexity measure for time series,” Phys. Rev. Lett., vol. 88, no. 17, Apr. 2002.

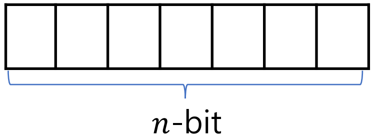
Contents

Bit extension method

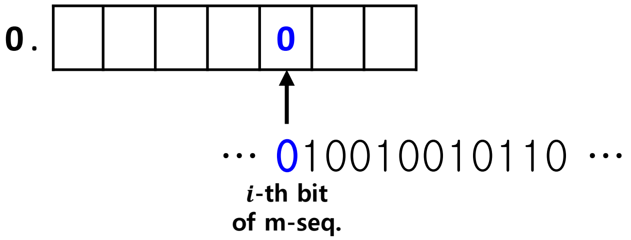
- Select a computation precision to implement the chaotic map using fixed-point arithmetic

- Compute x_{i+1} at the i-th iteration under the selected precision (n-bit)

$$\mu x_i(1 - x_i) = x_{i+1} = \mathbf{0}.$$



- A specific bit of x_{i+1} is extended into a i-th bit of m-sequence.

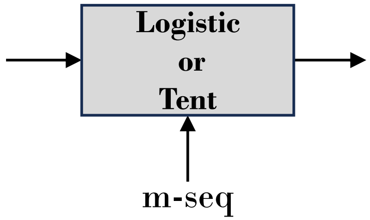


- Proceed to the next iteration with

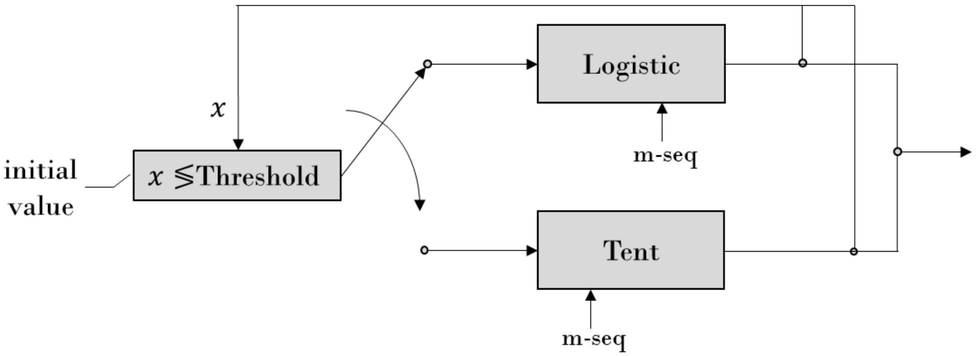
Bit extension method

1) Logistic map / Tent map (fixed-point arithmetic)

2) Bit extension method for Single chaotic map



3) Bit extension method for Combined chaotic map



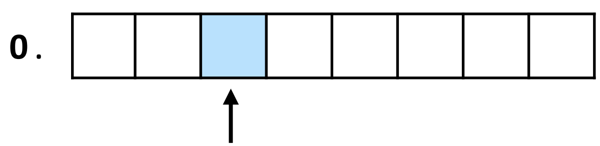
Single Chaotic map + Bit extension method

1) Logistic map

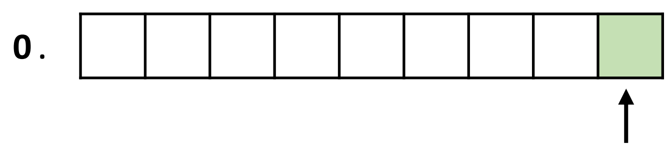
Precision	Initial Value	Fractal parameter μ	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	3.9921875 $(11.11111110)_2$	**4**	**0.0001**	**2.0025**	**2.0025**
9	0.001953125 $(0.000000001)_2$	3.998046875 $(11.111111111)_2$	**7**	**0.1980**	**2.8085**	**2.8085**

2) Logistic map + Bit extension method

Precision	Initial Value	Fractal parameter μ	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	3.9921875 $(11.11111110)_2$	**3**	**765** (255×3)	**0.5826**	**5.1127**	**5.9136**
9	0.001953125 $(0.000000001)_2$	3.998046875 $(11.111111111)_2$	**9**	**1022** (511×2)	**0.6343**	**5.9085**	**7.3156**



m-seq with periods of $2^8 - 1$



m-seq with periods of $2^9 - 1$

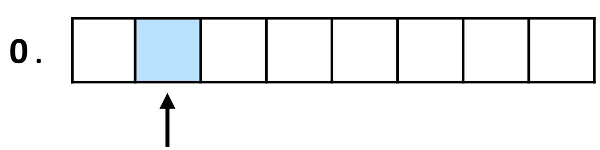
Single Chaotic map + Bit extension method

1) Tent map

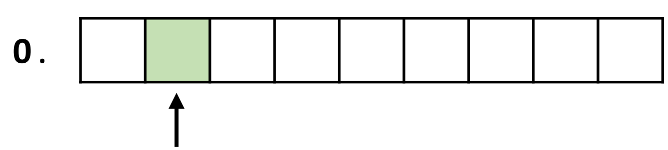
Precision	Initial Value	Fractal parameter a	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	1.96875 $(1.11111000)_2$	**33**	**0.2869**	**4.9837**	**5.0473**
9	0.001953125 $(0.000000001)_2$	1.984375 $(1.111111000)_2$	**65**	**0.9334**	**5.5799**	**6.0250**

2) Tent map + Bit extension method

Precision	Initial Value	Fractal parameter a	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	1.96875 $(1.11111000)_2$	**2**	**1020** $(\mathbf{255 \times 4})$	**1.3895**	**7.8367**	**7.8063**
9	0.001953125 $(0.000000001)_2$	1.984375 $(1.111111000)_2$	**2**	**2555** $(\mathbf{511 \times 5})$	**1.3343**	**8.0524**	**8.8404**



m-seq with periods of $2^8 - 1$



m-seq with periods of $2^9 - 1$

Combined Chaotic map + Bit extension

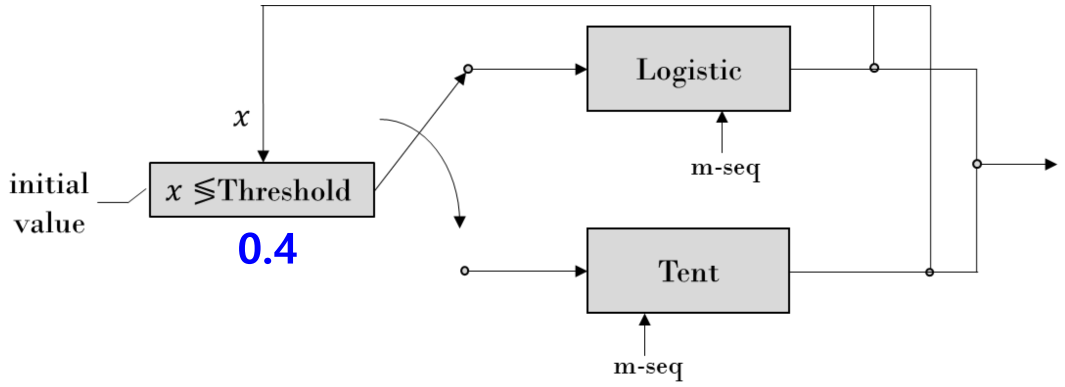
2) Logistic map +Bit extension method

Precision	Initial Value	Fractal parameter μ	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	3.9921875 $(11.11111110)_2$	3	765 (255×3)	0.5826	5.1127	5.9136
9	0.001953125 $(0.000000001)_2$	3.998046875 $(11.111111111)_2$	9	1022 (511×2)	0.6343	5.9085	7.3156

2) Tent map +Bit extension method

Precision	Initial Value	Fractal parameter a	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	1.96875 $(1.11111000)_2$	2	1020 (255×4)	1.3895	7.8367	7.8063
9	0.001953125 $(0.000000001)_2$	1.984375 $(1.111111000)_2$	2	2555 (511×5)	1.3343	8.0524	8.8404

3) combined map +Bit extension method



Combined Chaotic map + Bit extension

2) Logistic map +Bit extension method

Precision	Initial Value	Fractal parameter μ	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	3.9921875 $(11.11111110)_2$	3	**765** (255×3)	**0.5826**	**5.1127**	**5.9136**
9	0.001953125 $(0.000000001)_2$	3.998046875 $(11.111111111)_2$	9	**1022** (511×2)	**0.6343**	**5.9085**	**7.3156**

2) Tent map +Bit extension method

Precision	Initial Value	Fractal parameter a	Extended bit	Cycle length	ApEn	PE	SE
8	0.00390625 $(0.00000001)_2$	1.96875 $(1.11111000)_2$	2	**1020** (255×4)	**1.3895**	**7.8367**	**7.8063**
9	0.001953125 $(0.000000001)_2$	1.984375 $(1.111111000)_2$	2	**2555** (511×5)	**1.3343**	**8.0524**	**8.8404**

3) combined map +Bit extension method

Precision	Initial Value	Fractal parameter		Extended bit		Cycle length	ApEn	PE	SE
		μ	a	Logistic	Tent				
8	0.00390625 $(0.00000001)_2$	3.9921875 $(11.11111110)_2$	1.96875 $(1.11111000)_2$	3	2	**9435**	**1.2584**	**7.6826**	**7.7944**
9	0.001953125 $(0.000000001)_2$	3.998046875 $(11.111111111)_2$	1.984375 $(1.111111000)_2$	9	2	**18396**	**1.1546**	**7.5294**	**8.8026**

Contents

Concluding remark

- In this paper, we introduce a bit extension method to improve the dynamic degradation that occurs when implementing chaotic maps in digital systems.

- Applying the bit extension method to the combined chaotic map results in long periods and good random characteristics, even with low bit precision.

- Determining which bits to extend and what threshold to set in combined chaotic maps to achieve better period and randomness remains as future work.

Thank you for listening