Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **7**, Number **2**, May **2022**

A Novel Anti-Degradation Method for the Dynamics of Digital Chaotic Maps in Finite Precision Domain

Chunlei Fan*

Electronic Engineering College
Heilongjiang University
No. 74 Xuefu Road, Harbin, China
*Corresponding author: 2020021@hlju.edu.cn

Qun Ding

Electronic Engineering College
Heilongjiang University
No. 74 Xuefu Road, Harbin, China
1984008@hlju.edu.cn

Received January 2022; revised March 2022

Abstract. *The relevant properties of chaotic systems are closely related to the basic principles of confusion and diffusion in cryptography, which make chaotic systems widely used in chaotic secure communications. However, when the chaotic system is implemented on hardware devices with limited computational precision, the dynamics of chaos will be degraded to varying degrees. In order to resist the dynamic degradation of digital chaos, we proposed a new anti-degeneration method to improve the complexity, randomness, and ergodicity of discrete chaotic sequences. Numerical simulations were performed to evaluate the effectiveness of the proposed method. Moreover, a PRNG is designed with good performance.*
Keywords: Digital chaotic map; dynamical degradation; anti-degradation method; PRNG

1. **Introduction.** At present, the mobile Internet information security has become an important issue of concern. In recent decades, cryptography has developed rapidly as an important means to ensure information security [1]. In addition, chaos theory has played an important role in promoting the development of nonlinear dynamics. Since the good characteristics of chaotic systems are very suitable for secure communication and other fields, encryption systems based on chaos theory have been continuously proposed, such as chaotic multimedia data encryption [2–4], security systems based on chaotic synchronization [5], chaotic pseudo-random number generator [6, 7] and chaotic steganography [8], authentication protocol based on chaotic system [9–11], etc. However, when the chaotic system is implemented in hardware devices with limited computational precision, the characteristic degradation of chaotic dynamics will be inevitable [12, 13]. This phenomenon affects the security of chaotic cryptography to a certain extent, and hinders the application of chaos theory in engineering practice.

In order to enhance the security of chaotic cryptographic algorithms, relevant scholars have put forward some corresponding schemes to resist the dynamic degradation of digital chaotic systems, which can be roughly divided into the following four categories: one way is to use supercomputers with high computational precision increases the period length

of the chaotic sequence by expanding the state space of the digital chaotic map [14]. The second way is to enhance the randomness and complexity of the discrete chaotic sequence by cascading multiple identical or different chaotic systems [15, 16]. The third way is through the method of analog-digital mixing, that is, by introducing an analog chaotic system as a coupled controller to control the given digital chaotic map [17, 18]. The fourth way is to increase the complexity and period length of the chaotic sequence by perturbing the state variables and control parameters of the digital chaotic system [19, 20]. This kind of method is also the commonly used resistance method. In addition, there are methods such as constructing high-dimensional chaotic systems [21], using symbolic dynamics theory [22] to improve the performance of digital chaotic systems.

However, in order to design an anti-degeneration method with strong generality and good performance, multiple aspects should be considered comprehensively, such as ease of engineering implementation, sequence balance, sequence complexity, and hardware resource consumption. In addition, the above methods rarely design anti-degeneration schemes from the essence of digital chaos degradation. In view of this, this paper firstly analyzes the dynamic degradation of digital chaos in detail. We found that the chaotic state variables falling into periodic cycles are the root cause of the degradation of chaotic systems. Furthermore, we designed a new anti-degeneration method to enhance the complexity, randomness, ergodicity of discrete chaotic sequences. The relevant simulation results also show that this method has good performance and can improve the dynamic characteristics of the chaotic system. Compared with the proposed schemes, our anti-degeneration method has the advantages of easy hardware implementation, simple structure, high complexity and long period.

The rest of this paper is organized as follows: Sect. 2 describes the dynamical degradation of digital chaotic systems. A novel anti-degradation method is proposed in Sect. 3. The performance of the improved logistic map is analyzed in Sect. 4. Sect. 5. proposes a PRNG. Finally, Sect. 6 summarizes the conclusions of this paper.

2. **Dynamical Degradation of Digital Chaotic Systems.**

Based on the chaotic definitions such as Devaney [23] and Li-Yorke [24], the original chaotic system is defined in the continuous domain. However, when the chaotic system is implemented on the hardware equipment with limited computational accuracy, the digitized chaotic system is not the original chaos in the strict mathematical sense. Therefore, due to the limited calculation accuracy, digital chaos is bound to be discretized in time and space. The digital chaotic system will introduce inevitable truncation error and rounding error in each iterative operation. This error will lead to uncontrollable deviation between the digital iterative trajectory in the finite field and the chaotic trajectory originally defined in the continuous field. Undoubtedly, with the different computing precision of hardware devices, the digitized chaotic system will have different degrees of dynamic degradation. The inherent randomness, ergodicity, and initial value sensitivity of chaotic systems will also be negatively affected to varying degrees.

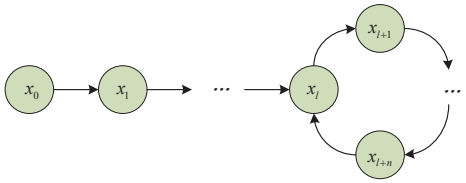


FIGURE 1. Schematic diagram of digital chaotic orbit

Chaos definition points out that chaotic systems in the continuous field have aperiodic properties. However, the most important problem of digital chaotic systems in the finite field is the irresistible periodicity. Let us assume that m is the computational precision, the range of state variables of the digital chaotic system will be limited to a discrete space with only 2^m elements. Due to the "pigeon nest principle" and finitely countable state, infinite chaotic orbits in chaotic systems will collapse into several periodic orbits. When chaotic systems are implemented in digital circuits, they will exhibit multi-periodic behavior. Moreover, the schematic diagram of digital chaotic orbit is shown in Figure 1. According to the figure, each digital chaotic orbit includes two connected parts: $x_0, x_1, , \cdots , , x_{l-1}$ and $x_l, x_{l+1}, , \cdots , , x_{l+n}$. These two parts are called transient and cycle states, respectively. Correspondingly, l and $n+1$ are called transient length and cycle period. For the same digital chaotic system, all digital chaotic orbits will eventually fall into a few periodic cycles. This means that the discrete phase space will collapse on an attractor whose size is less than 2^m. In this section, the digital logistic map is selected as an example to describe the phenomenon. The iterative equation of the digital logistic map can be defined as

$$z_{n+1} = \varphi(z_n) = \left\lfloor \mu z_n \left(1 - \frac{z_n}{2^m}\right) \right\rfloor, \quad z_n \in [0, 2^m - 1] \tag{1}$$

where $\lfloor \cdot \rfloor, m$ and μ denotes the numeric rounding operation, limited calculation accuracy and bifurcation parameter, respectively.Based on Eq. (1), we can plot the state-mapping graph of the digital logistic map with the precision $m = 6$, which is shown in Figure 2. According to the figure, no matter what the initial value is, it eventually converges into two fixed points (0, 48) and a periodic cycle (3, 63, 36, 11) after several iterations. The collapse of phase space will have a negative impact on the ergodicity and internal randomness of digital chaos. Therefore, it is crucial to resist the dynamical degradation of digital chaotic maps.

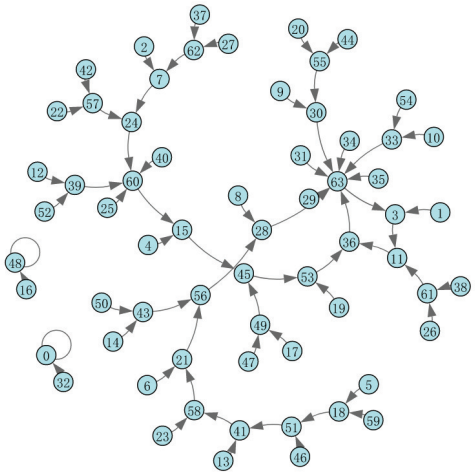


FIGURE 2. The state-mapping graph of the digital logistic map with the precision $m = 6$

3. **A Novel Anti-Degradation Method for the Dynamics of Digital Chaos.** In order to enhance the dynamic characteristics of digital chaotic systems, a new anti-degradation method is designed to improve the randomness, complexity, and period length of chaotic sequences. Schematic diagram of the anti-degradation method is shown in Figure 3. First, y_0 and z_0 are used as initial values to perform two digital logistic maps

for iterative operations and generate chaotic sequences $y_1y_2\cdots$ and $z_1z_2\cdots$. Then, the two sequences are merged into a new sequence $z_1y_1z_2y_2\cdots$ after passing through the delay module. After XOR operation between the new sequence and $X_1X_2X_3\cdots$, the final output sequence $u_0u_1u_2u_3\cdots$ is generated. Where LCG is called linear congruential generators. On the one hand, LCG acts as a random disturbance source to control the number of iterations of the two digital logistic maps with the purpose of preventing state variables from getting trapped in periodic cycles. On the other hand, the good ergodicity of LCG can improve the balance of the final output sequence $u_0u_1u_2u_3\cdots$. The mathematical expression of LCG is defined as

$$X_{n+1} = (aX_n + c) \bmod M, \quad n \geq 0 \tag{2}$$

where M, a and c denotes the modulus, multiplier, and increment, respectively. When the parameters a, b and M take appropriate values, LCG can output the longest discrete sequence (i.e., full cycle) with length M. Furthermore, the LCG defined by m, a, c has period length M if and only if: (i) c is relatively prime to m. (ii) $b = a - 1$ is a multiple of p, for every prime p dividing m. (iii) b is a multiple of 4, if m is a multiple of 4. When the above three criteria are fulfilled, the LCG can output a full cycle with length M. For example, when $a = 13$, $c = 1$ and $M = 16$, the LCG can output a sequence with length 16. When the number of iterations of the two digital logistic maps reaches the control value X_i, the iteration values y_i and z_i at this time are used as the parameters of the function $g()$ and two new initial values Y_i and Z_i are generated. The mathematical expression of the function $g()$ is given by

$$g(y_i, z_i) = \begin{cases} Y_i = (y_i)_{\mathrm{H}} \,\|\, (z_i)_{\mathrm{L}} \\ Z_i = (z_i)_{\mathrm{H}} \,\|\, (y_i)_{\mathrm{L}} \end{cases} \tag{3}$$

where subscripts H and L denotes the high and low $m/2$ bits of the iteration value. The symbol $\|$ represents the bit connector.Moreover, these two latest initial conditions (i.e., Y_i and Z_i) are assigned to the logistic iterative equation to increase the complexity of the system. Next, the system continuously outputs the improved discrete chaotic sequence $u_0u_1u_2u_3\cdots$ according to the above rules.

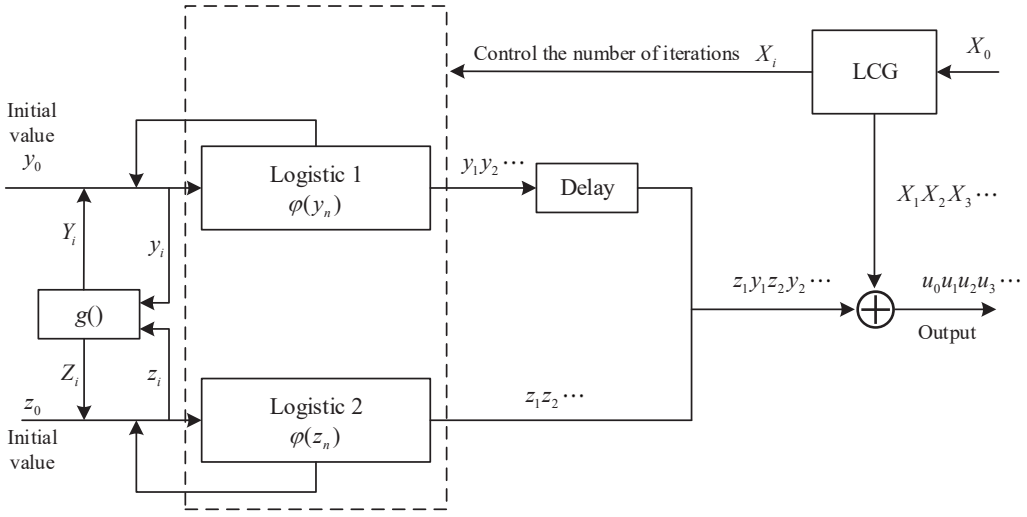


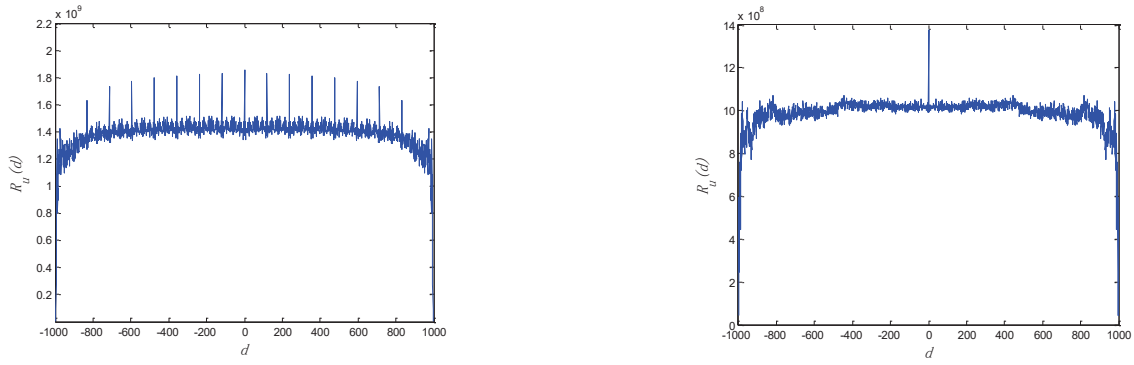
FIGURE 3. Schematic diagram of the anti-degradation method

4. **Performance Analysis of Improved Logistic Map.**

4.1. **Autocorrelation.** Autocorrelation test is used to detect the correlation degree between the binary $\{u_i\}$ sequence to be tested and the new sequence obtained by shifting the sequence (i.e., $\{u_i\}$) to the left by d bits. For the binary sequence with good randomness, it should be satisfied that the new sequence obtained by shifting any bit to the left has a very low correlation degree. The method is generally realized by the autocorrelation function of the sequence, and its mathematical formula is

$$R_u(d) = \frac{1}{N - |d|} \sum_{n=0}^{N-1-|d|} u_n u_{n+d} \tag{4}$$

where N denotes the length of the binary sequence. In this section, we set the computational precision $m = 16$ and generate two digital logistic sequences. Here, we set $y_0 = 5$, $z_0 = 8$ and $X_0 = 38$, and numerical simulation results are shown in Figure 4. As presented in Figure 4(a), the autocorrelation for the original digital logistic sequence has some peak spectral lines with approximately equal height, which indicates short period. Nevertheless, for improved logistic sequence, the autocorrelation function is like the impulse function, which display longer periodic length and good pseudo-randomness.

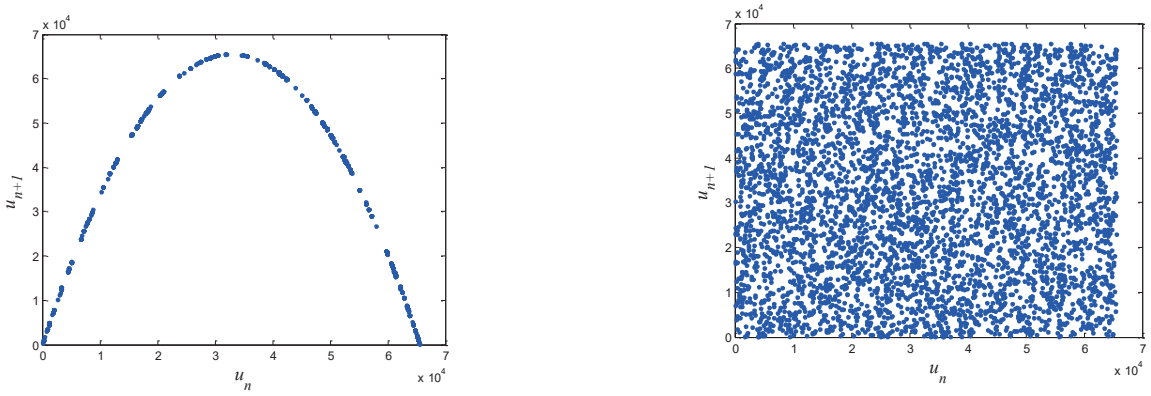


(a) (b)

FIGURE 4. Autocorrelation test. (a) digital logistic sequence, (b) improved logistic sequence.

4.2. **Phase portraits.** Due to the limited computational accuracy of hardware equipment, the continuous phase space $[0, 1] \times [0, 1]$ for the original logistic map will be transformed into a discrete phase space $[0, 2^m - 1] \times [0, 2^m - 1]$.In order to compare the relevant characteristics of different digital logistic maps, there is still set limited calculation accuracy $m = 16$ and the phase portraits of two digital logistic maps are shown in Figure 5. The phase space of the digital logistic map has some discrete points and the overall shape is a parabola (see Figure 5(a)). This indicates that the state space utilization of the chaotic map is lower and has obvious periodicity. For improved logistic map, its phase portrait exhibits dense points in the phase space, which indicates that the map achieves good ergodicity and sufficiently destroys the parabola structure. Therefore, the improved logistic map can resist phase space reconstruction and enhance the complexity of digital chaos.

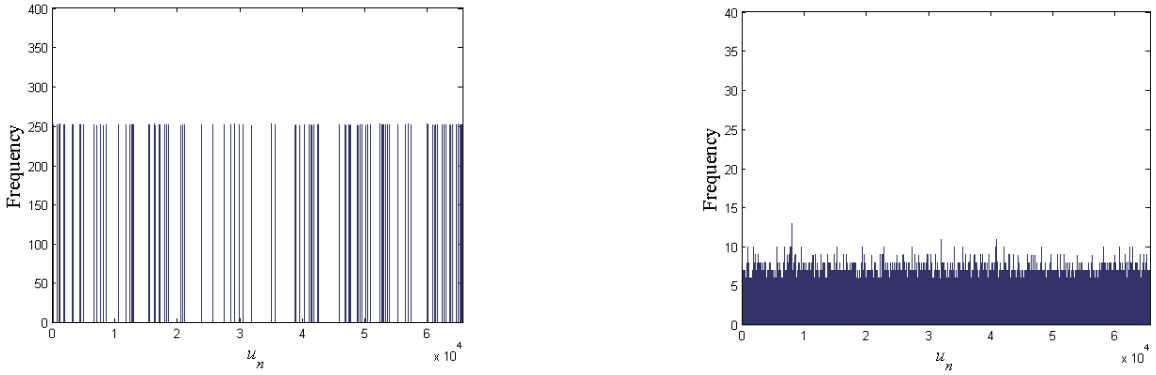
4.3. **Histogram test.** A frequency histogram is a graph that represents the frequency distribution in statistics. In order to analyze whether the chaotic state variables are uniformly distributed in the value range $[0, 2^m - 1]$, we analyze the frequency distribution histogram of the two digital logistic maps with the calculation accuracy $m = 16$. The



(a) (b)

FIGURE 5. Phase portraits. (a) digital logistic sequence, (b) improved logistic sequence.

simulation results are shown in Figure 6. From Figure 6(a), the distribution of state variables of the digital logistic sequence is extremely uneven. In cryptography, such sequences are vulnerable to frequency analysis attacks and have obvious security risks. However, the improved logistic sequence has more uniform distribution of state variables, good ergodicity, and statistical characteristics, which can resist frequency analysis attacks.



(a) (b)

FIGURE 6. Histogram test. (a) digital logistic sequence, (b) improved logistic sequence.

4.4. **Complexity test.** Permutation entropy (PE) was proposed by two German scholars C. Bandt and B. Pompe in 2002 [25]. This algorithm has the advantages of fast calculation speed and strong robustness. Therefore, it is widely used to measure the complexity of discrete chaotic sequences. The larger the PE value, the higher the complexity of discrete time series. In this section, we calculate the complexity of two digital logistic sequences with different calculation accuracy and length 1000. The parameters (i.e., embedding dimension and delay time) of PE are set as $\theta = 6$ and $\tau = 1$. the results are listed in Table 1. The PE value of the improved logistic sequence is much higher than that of the original digital logistic sequence. In addition, for computational precisions $m = 12, 16$ and 24, the complexity of the improved logistic sequence is close to the ideal value 1 and shows a good sequence complexity.

TABLE 1. PEs of two digital logistic sequences with various computational precisions

Precision m	Digital logistic sequence	Improved logistic sequence
8	0.22761	0.73461
12	0.37992	0.93789
16	0.58823	0.93465
24	0.61841	0.93491

5. **A Pseudorandom Number Generator Based on Improved Logistic Map.** In this section, we deal with the improved logistic chaotic sequence by threshold quantization method to construct a pseudorandom number generator (PRNG). Suppose that $\{u_n\}$ and $\{s_n\}$ represent a chaotic real-valued sequence and a quantized binary sequence, respectively.The mathematical equation of threshold quantization can be given by

$$S_n = \begin{cases} 0 & u_n < t_d \\ 1 & u_n \geq t_d \end{cases} \tag{5}$$

where t_d denotes the threshold of the quantization method. Based on Eq. (5), we can construct an PRNG. Subsequently, the security of the proposed PRNG is analysed in this paper.

5.1. **Balance analysis.** Balance test is also known as single-bit frequency test. The purpose of this test is to determine whether the number of 0 and 1 elements in the chaotic binary sequence are approximately the same as would be expected for a truly random sequence. In this section, Let us assume that n_0, n_1, N denotes the number of 0 elements, the number of 0 elements and the length of the chaotic binary sequence, respectively. In order to test the balance of chaotic binary sequences, the following statistics can be constructed as

$$\chi^2 = \frac{(n_0 - n_1)^2}{N} \tag{6}$$

where $N \geq 100$. Here, the significance level can be selected as 5%, and the corresponding χ^2 value is 3.841. Furthermore, the balance of the improved logistic binary sequences with different lengths are tested, and the test results are shown in Table 2. The final values of binary sequences with different lengths are less than 3.841, which show that the improved logistic binary sequence has good balance.

TABLE 2. Balance test of improved logistic binary sequences

Length N	Number of 0	Number of 1	χ^2
1000	473	527	2.916
3000	1487	1513	0.2253
5000	2493	2507	0.0392

5.2. **Linear complexity analysis.** The purpose of the linear complexity test is to determine whether or not the improved logistic binary sequence is complex enough to be considered random. The linear complexity of chaotic binary sequences is generally calculated by Berlekamp-Massey algorithm. Based on the PRNG proposed in this paper, we generate an improved chaotic binary sequence with length 1000 and analyze the linear complexity. The simulation results are shown in Figure 7. From the figure, the linear complexity of the binary sequence basically fluctuates up and down in steps around the

straight-line $N/2$, which means that the improved logistic binary sequence has better linear complexity.

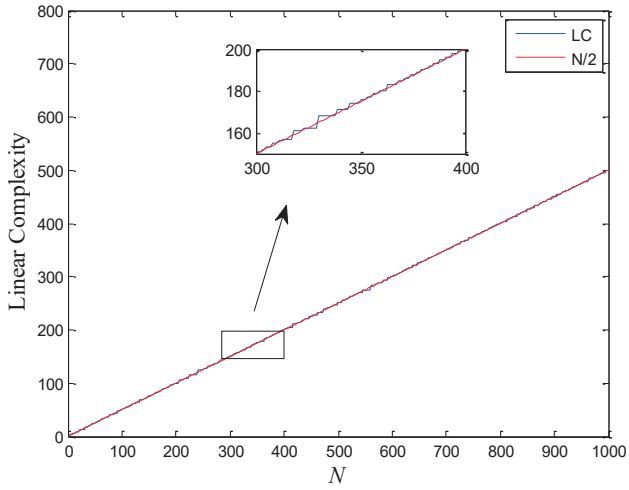


FIGURE 7. Linear complexity of improved logistic binary sequence

6. **Conclusion.** Due to the influence of finite computational precision of hardware devices, the dynamic characteristics of digital chaotic systems are degraded. To solve this problem, we designed a new anti-degeneration method to enhance the performance of digital chaos. Numerical simulations were executed to evaluate the effectiveness and correctness of the proposed scheme in terms of autocorrelation, phase space, complexity, and histogram. It can be found that the dynamic characteristics of the improved chaotic map have been significantly improved. Furthermore, based on the threshold quantization method, a simple PRNG is constructed. The performance analysis results show that this PRNG has good performance and can be applied to cryptographic algorithms and chaotic secure communications.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (Grant No. 62101178) and the Fundamental Research Funds for the Higher Institutions in Heilongjiang Province (Grant No. 2020-KYYWF-1033).

REFERENCES.

[1] R. Farah, T. Shareef, Secure Communication by combined Diffe-Hellman key exchange Based AES Encryption and Arabic Text Steganography, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 12, pp. 186-198, 2021.

[2] W. J. Zhou, X. Y. Wang, M. X. Wang, D. Y. Li, A New Combination Chaotic System and its Application in a New Bit-Level Image Encryption Scheme, *Optics and Lasers in Engineering*, vol. 149, 106782, 2022.

[3] P. Chen, S. M. Yu, X. Y. Zhang, J. B. He, Z. S. Lin, C. Q. Li, J. H. Lu, ARM-embedded Implementation of a Video Chaotic Secure Communication via WAN Remote Transmission with Desirable Security and Frame Rate, *Nonlinear Dynamics*, vol. 86, no. 2, pp. 725-740, 2016.

[4] S. M. Seyedzadeh, S. Mirzakuchaki, A Fast Color Image Encryption Algorithm Based on Coupled Two-Dimensional Piecewise Chaotic Map, *Signal Processing*, vol. 92, pp. 1202-1215, 2012.

[5] A. Bouhous, K. Kemih, Novel Encryption Method Based on Optical Time-Delay Chaotic System and a Wavelet for Data Transmission. *Optics and Laser Technology*, vol. 108, pp. 162-169, 2018.

[6] R. Hamza, A Novel Pseudo Random Sequence Generator for Image-Cryptographic Applications, *Journal of information security and applications*, vol. 35, pp. 119-127, 2017.

[7] E. Z. Dong, M. F. Yuan, S. Z. Dua, Z. Q. Chen, A New Class of Hamiltonian Conservative Chaotic Systems with Multistability and Design of Pseudo-Random Number Generator, *Applied Mathematical Modelling*, vol. 73, pp. 40-71, 2019.

[8] A. Akgul, A. Kacar, B. Aricioglu, A New Two-Level Data Hiding Algorithm for High Security Based on a Nonlinear System, *Nonlinear Dynamics*, vol. 90, pp. 1123-1140, 2017.

[9] C. T. Li, C. L. Chen, C. C. Lee, C. Y. Weng, C. M. Chen, Novel Three-party Password-based Authenticated Key Exchange Protocol with User Anonymity Based on Chaotic Maps, *Soft Computing*, vol. 22, no. 8, pp. 2495-2506, 2018.

[10] C. M. Chen, L. L. Xu, K. H. Wang, S. Liu, T. Y. Wu, Cryptanalysis and improvements on three-party-authenticated key agreement protocols based on chaotic maps, *Journal of Internet Technology*, vol. 19, no. 3, pp. 679-687, 2018.

[11] C. M. Chen, W. C. Fang, T. Y. Wu, S. Liu, T. Y. Wu, J. S. Pan, K. H. Wang, Improvement on a Chaotic Map-based Mutual Anonymous Authentication Protocol, *Journal of Information Science and Engineering*, vol. 34, no. 2, pp. 371-390, 2018.

[12] Y. L. Luo, Y. Q. Liu, J. X. Liu, S. B. Tang, J. Harkin, Y. Cao, Counteracting Dynamical Degradation of a Class of Digital Chaotic Systems via Unscented Kalman Filter and Perturbation. *Information Sciences*, vol. 556, pp. 49-66, 2021.

[13] C. F. Wang, Q. Ding, Theoretical Design of Controlled Digitized Chaotic Systems with Periodic Orbit of Upper Limit Length in Digital Circuit, *Nonlinear Dynamics*, vol. 98, no. 1, pp. 257-268, 2019.

[14] D. Wheeler, R. Matthews, Supercomputer Investigations of a Chaotic Encryption Algorithm, *Cryptologia*, vol. 15, pp. 140-152, 1991.

[15] G. Heidari-Bateni, C. D. McGillem, A Chaotic Direct-Sequence Spread-Spectrum Communication System, *IEEE Transactions on Communications*, vol. 42, pp. 1524-1527, 1994.

[16] Z. Y. Hua, Y. C. Zhou, One-dimensional Nonlinear Model for Producing Chaos, *IEEE Transactions on Circuits and Systems I-Regular Papers*, vol. 65, no. 1, pp. 235-246, 2018.

[17] H. P. Hu, Y. S. Deng, L. F. Liu, Counteracting the Dynamical Degradation of Digital Chaos via Hybrid Control, *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1970-1984, 2014.

[18] L. F. Liu, H. P. Hu, Y. S. Deng, An Analogue-Digital Mixed Method for Solving the Dynamical Degradation of Digital Chaotic Systems, *IMA Journal of Mathematical Control and Information*, vol. 32, no. 4, pp. 703-715, 2015.

[19] Y. Q. Liu, Y. L. Luo, S. X. Song, L. C. Cao, J. X. Liu, J. Harkin, Counteracting Dynamical Degradation of Digital Chaotic Chebyshev Map via Perturbation, *International Journal of Bifurcation and Chaos*, vol. 27, 1750033, 2016.

[20] T. Sang, R. Wang, Y. Yan, Perturbance-Based Algorithm to Expand Cycle Length of Chaotic Key Stream, *Electronics Letters*, vol. 34, pp. 873-874, 1998.

[21] J. B. He, S. M. Yu, J. H. Lü, Constructing Higher-Dimensional Nondegenerate Hyperchaotic Systems with Multiple Controllers, *International Journal of Bifurcation and Chaos*, vol. 27, no. 9, 1750146, 2017.

[22] J. Zheng, H. P. Hu, X. Xia, Applications of Symbolic Dynamics in Counteracting the Dynamical Degradation of Digital Chaos, *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1535-1546, 2018.

[23] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, Redwood City, Addison-Wesley, 1989.

[24] T. Y. Li, J. A. Yorke, Period Three Implies Chaos, *American Mathematical Monthly*, vol. 82, pp. 985-992, 1975.

[25] C. Bandt, B. Pompe, Permutation Entropy: A Natural Complexity Measure for Time Series, *Physical Review Letters*, vol. 88, 174102, 2002.