Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 7, No. 1, 2024

Design of Pseudo-random Sequence Generator based on Three-dimensional Discrete Chaotic System

Lijie Wang, Xiyin Liang *, Qi Liang

College of Physics and Electronic Engineering, Northwest Normal University, Lanzhou Gansu, 730070, China
* **Corresponding author**: Xiyin Liang

Abstract: In this paper, a pseudo-random sequence generator with better randomness is constructed through the targeted improvement of chaotic system. Firstly, a new three-dimensional discrete chaotic system is proposed on the basis of the existing one-dimensional logistic chaotic system by improving and optimizing the dimensionality and coupling mode, and its Lyapunov exponent and other characteristics are analyzed; then, based on the chaotic system, a pseudo-random sequence generator is designed by using post-processing and heterodyne, etc.; after that, the performance of the pseudo-random sequence is discussed by using the evaluation methods of relevance, homogeneity, and NIST test. After that, the performance of the pseudo-random sequence is discussed using correlation, uniformity, NIST test and other evaluation methods. The results show that the three-dimensional discrete chaotic system has good chaotic properties, and the pseudo-random sequence generator based on this three-dimensional discrete chaotic system has good random performance and can pass the NIST test. The work in this paper provides an idea for the improvement of logistic mapping chaotic system and enriches the application form of pseudorandom sequence generator in information security.

Keywords: Chaotic System; Logistic Mapping; NIST Test; Pseudo-random Sequence Generator.

1. Introduction

In recent years, with the advancement of science and technology, the issue of information security has been gradually emphasized by various fields, which leads to the fact that the relevant research content about information security protection has become particularly important nowadays. Since ancient times, people have been using different encryption means to protect their information security, and then cryptography has appeared as an important discipline in the history of human development. Pseudo-random sequences are widely used in the field of information security protection as a common encryption means, so the design of pseudo-random sequence generator with good performance has more important research significance. The chaotic sequences generated by chaotic systems are inextricably linked with cryptography, and thus the pseudorandom sequences generated by chaotic systems have become a hot issue in current research [1-3]. Chaotic systems have different classifications, which can be divided into continuous chaotic systems and discrete chaotic systems according to the relationship of time sequence, and the continuous chaotic systems can be changed into discrete chaotic systems by first discretization [4]; compared with the continuous chaotic systems, the discrete chaotic systems and pseudo-random sequences generators can be better adapted to each other. However, due to the finite word length effect in computers, the chaotic properties of chaotic systems will be gradually degraded, the effect of which is that the chaotic sequences will be short-periodic and multi-periodic, and the degraded chaotic systems are called digitized chaotic systems [5-8]. Chaotic systems can also be divided into high-dimensional chaotic systems and low-dimensional chaotic systems through dimensionality [9], at present, the commonly used low-dimensional chaotic systems are Logistic mapping [10], Henon mapping [11] and so on, and experiments [5] show that the low-dimensional chaotic system has a more serious degradation of chaotic characteristics, which can be improved in terms of dimensionality of one-dimensional Logistic chaotic system, and coupling to achieve the final chaotic system is called digital chaotic system [5-8]. The one-dimensional Logistic chaotic system can be improved in terms of dimensionality, and the final improvement can be achieved by coupling, and a new three-dimensional discrete chaotic system can be constructed in the end. The data analysis of the new three-dimensional discrete chaotic system demonstrates that the improved chaotic system has more complex nonlinear dynamics behavior, and can resist the degradation of certain chaotic characteristics and produce better chaotic sequences.

One of the important applications of chaotic systems is the design of pseudo-random sequence generators, Bernstein et al [12] in 1990 for the first time using first-order digital phase-locked loop chaotic circuits to generate safe random numbers, for the design of pseudo-random sequence generators based on chaotic systems to provide theoretical support for the idea. Subsequently some studies [13-15] focused on the direction of pseudo-random sequence generators based on chaotic systems. Pseudo-random sequence generators are essentially algorithms that produce a pseudo-random sequence of length m (m>k) by using a binary sequence of length k as an input, which is processed by a deterministic algorithm of its own design; where the input k is referred to as the seed of the generator, and m is referred to as the pseudo-random sequence.

In this paper, based on the determined parameters and initial values, three chaotic sequences of x, y, and z are generated by the constructed three-dimensional discrete chaotic system, respectively, and then the new three chaotic random sequences are obtained by the algorithm of quantization by post-processing [16] in the way of obtaining the exact digits after the decimal point and judging their odd and even. Finally, the three chaotic sequences are processed through heterodyne processing to produce the final pseudo-random sequences, and the produced pseudo-random

sequences are analyzed by correlation, uniformity and other indexes test with NIST test. Through the analysis, it is proved that the pseudo-random sequences produced by the pseudo-random sequence generator algorithm designed in this paper have better performance, and the work in this paper provides a method for the design of pseudo-random sequence generator and provides a research basis in security information protection.

2. Design and Analysis of Three-Dimensional Discrete Chaotic Systems

2.1. Improvement of 3D Discrete Chaotic Systems

One-dimensional Logistic chaotic system [17] is a classical model of chaotic system, which is widely used in the design of sequence generators due to its irreversibility in time series and good initial value sensitivity. However, with the development of information science and technology, the chaotic properties exhibited by the one-dimensional Logisti chaotic system with fewer parameters are not enough to be adapted to the design of pseudo-randomized sequence generators. In this paper, based on the research of Tao Hong et al [18], a new three-dimensional discrete chaotic system is finally constructed by changing the coupling term [19] for the one-dimensional Logisti chaotic system to extend the dimension extension to three dimensions, and then combining the sine mapping with the improved three-dimensional Logisti chaotic system through the coupling, and the complexity of the system is shown by analyzing and visualizing it. Enhancement.

2.1.1. Improvement of One-dimensional Logistic Chaotic Systems

The one-dimensional Logistic mapping is the classical mapping in chaotic systems, which is essentially a nonlinear dynamical system. Its mathematical expression is carried out by the recursive equation as:

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

where the initial value of the system $x_n \in (0,1]$ and the system control parameter $\mu \in (0,4]$.It has been studied [10] that the system enters into a chaotic state when the parameter when $\mu \in (3.57,4]$.Through the system Lyapunov exponent [20] with the parameterμits intuitive changes as shown in Figure 1, it can be more intuitively seen that whenμ> 0.57, the Lyapunov exponent of the system is positive that is greater than 0, then it indicates that the system enters into a chaotic state.

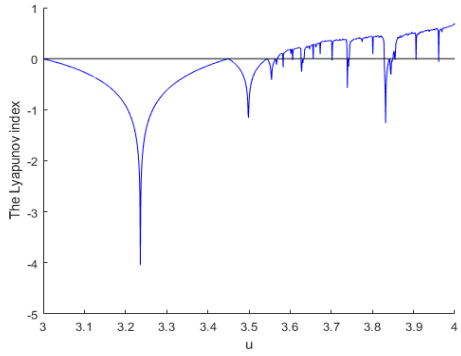

Figure 1. Variation of parameter μ with respect to Lyapunov exponent

Can be one-dimensional Logistic chaotic system in the x and μas a coupling term, through the increase of the coupling term, can be increased from the x variable on the increase to x, y, z, will be constructed into a system model of the three expressions will be completed by the original one-dimensional to the three-dimensional enhancement; at the same time, with the increase in x, y, z coupling term produced by the upgrading of the changes in the parameters to match the original x for the parameters corresponding to the expansion of the x, y, z, respectively, to the α, β, γ three parameters, and finally the use of the addition of three times, including the coupling term of the changes in the x^3,y^3, z^3, and by the way of the product each other to ultimately constitute a new system. After the above improved method, x, y, z are used as the initial values of the system, and α, β, γ are used as the system control parameters, so that the overall expansion of the expression can be accomplished. The three-dimensional Logistic mapping expression obtained after the expansion is:

$$\begin{aligned} x_{n+1} &= \alpha \times x_n \times (1 - x_n) + \beta \times y_n^2 \times x_n + \gamma \times z_n^3 \\ y_{n+1} &= \alpha \times y_n \times (1 - x_n) + \beta \times z_n^2 \times y_n + \gamma \times x_n^3 \\ z_{n+1} &= \alpha \times z_n \times (1 - x_n) + \beta \times x_n^2 \times z_n + \gamma \times y_n^3 \end{aligned} \quad (2)$$

In the above expression, x, y, and z take typical values of 0.5, 0.7, and 0.2 respectively as the initial values of this system, and when α, β, and γ take typical values of 3.7, 0.15, and 0.01 respectively, after many experiments, the three Lyapunov exponents are derived as LE_x=0.3440, LE_y=0.3647, and LE_z=0.3541, which is in accordance with literature [21] it is proved that the three-dimensional Logistic mapping is constructed with chaotic nature.

2.1.2. Improved Three-dimensional Logistic Chaotic Systems based on Coupling

The one-dimensional Logistic chaotic system is improved to a three-dimensional Logistic chaotic system through the change of coupling terms, although in theory, it can make the chaotic characteristics improved to some extent, which is more suitable for the design of pseudo-random sequence generator.

However, a single chaotic mapping can be easily recognized if the mapping features are attacked during information protection, and literature [22] mentioned a similar problem in the study, so it is also necessary to carry out the coupling between chaotic systems [23] to improve the chaotic properties of chaotic systems. Common coupling methods include state coupling, local coupling, hybrid coupling, input coupling, etc. Considering the synchronization problem in the design of pseudo-random sequence generator, this paper adopts the input coupling method, which is to take the output of the chaotic system as the input of the next chaotic system, which means that the output of the original chaotic system will have an effect on the chaotic system of another chaotic system, and it is able to enhance the chaotic system's iteration and chaos. and chaos.

Sine mapping is a kind of mathematical mapping constructed according to the sine function, and its expression under the constraint of a certain parameter range has the characteristics of nonlinearity, variable parameter, and intuition, so this paper proposes a new three-dimensional discrete chaotic system by coupling the sine mapping with the three-dimensional Logistic chaotic system accomplished in the previous stage, and its expression is as follows:

$$x_{n+1} = \theta \sin(\pi(\alpha \times x_n \times (1 - x_n) + \beta \times y_n^2 \times x_n + \gamma \times z_n^3))$$

$$y_{n+1} = \theta\sin(\pi(\alpha \times y_n \times (1 - x_n) + \beta \times z_n^2 \times y_n + \gamma \times x_n^3))$$

$$z_{n+1} = \theta\sin(\pi(\alpha \times z_n \times (1 - x_n) + \beta \times x_n^2 \times z_n + \gamma \times y_n^3))(3)$$

Where, x_n,y_n,$z_n$are used as initial values and α, β, γ,θ are used as system control parameters.

Adopting the empirical values of x, y, and z of 0.5, 0.7, and 0.2 respectively in the previous stage as the initial values of this system, and α, β, and γ, taking the typical values of 3.7, 0.15, 0.01, and 0.5, respectively, the Lyapunov exponents of this three-dimensional discrete chaotic system are calculated to be LE_x = -0.3029, LE_y = -1.1260, and LE_z = 0.3959, which can prove that the system is a three-dimensional discrete chaotic system. Up to this point has been from one-dimensional Logistic chaotic system to complete the improvement, from the original variables x, parameters; to the improved variables x, y, z, parameters α, β, γ,θ.

Next, the three-dimensional discrete chaotic system constructed above is experimentally analyzed, and this paper adopts the Jacobian approach [24] for the calculation of the relationship between the Lyapunov exponent and α, β, γ,θ parameters, when three of the parameters are selected as the constant values, and the other parameter as the variable, to carry out the calculation of the Lyapunov exponent. In order to have a more streamlined, representative representation, this is only to Lyapunov index with the parameter α, two parameter changes in the calculation, the final results of the calculation are shown in Figure 2, Figure 3, respectively, the horizontal axis of the figure represents α,θ the different parameters, respectively, represented by a, d; the vertical axis represents the change of Lyapunov index with a, d in a certain range of the calculation when the calculation is carried out.

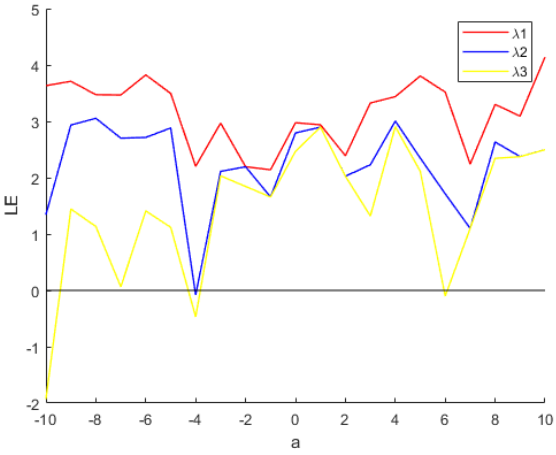

Figure 2. Variation of Lyapunov index with parameter a

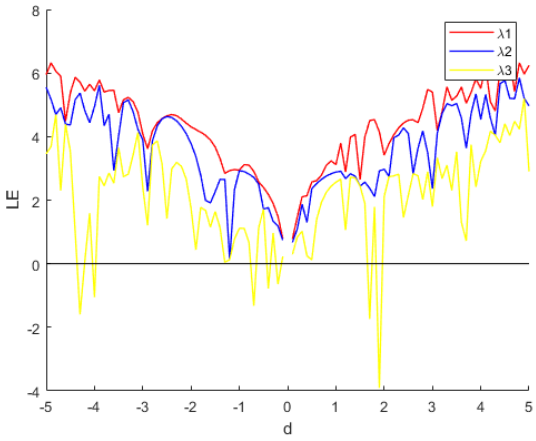

Figure 3. Variation of Lyapunov index with parameter d

Repeat the above calculations to complete the effect of the change of parameters α, β, γ,θ on the Lyapunov exponent, respectively, and finally determined to use x, y, and z to take the classical value of 0.5, 0.7, and 0.2 of the previous stage as the initial value of this system, respectively, to obtain the parameter α, β, γ and θ as 7, 5, 2, and 1, respectively, for the chaotic system of the current design of the pseudosequence generator, and calculated this three-dimensional The three Lyapunov exponents of this three-dimensional discrete chaotic system are LE_x=3.0417, LE_y=2.2273, and LE_z=2.3446, respectively.

2.2. Analysis of Three-dimensional Discrete Chaotic Systems

By improving the above three-dimensional discrete chaotic system, the final three-dimensional discrete chaotic system equations are determined, and this subsection makes a comparative analysis by using the scatter plot and Lyapunov exponent as the analysis content. Through the analysis, it is proved that the three-dimensional discrete chaotic system constructed by this method has better system sensitivity and chaotic characteristics; and in discrete form, it is more suitable for the design of pseudo-random sequence generator. The variables and parameters of one-dimensional logistic chaotic system, three-dimensional logistic chaotic system and three-dimensional discrete chaotic system are shown in Table 1

Table 1. Chaotic system parameter

Chaotic system umber Variable and parameter names	x	y	z	μ	α	β	γ	θ
One-dimensional logistic chaotic system	0.5	\	\	3.9	\	\	\	\
Three dimensional logistic chaotic system	0.5	0.7	0.2	\	7	5	2	\
Three-dimensional discrete chaotic system	0.5	0.7	0.2	\	7	5	2	1

2.2.1. Scatter Plot Analysis of Three Chaotic Systems

The scatter plot of a chaotic system is the representation of the system state in phase space, where each point represents the state of the system at a certain moment. In chaotic systems, since the system has an initial value sensitivity even a small difference in the initial value may lead to a huge separation between the trajectories of the system. Therefore, the pattern of a scatterplot can demonstrate the complex and unpredictable behavior of a system. The structure, distribution and shape of the trajectories in the scatterplot usually reflect the chaotic nature of the system. The scatter plots of each of the three chaotic systems in the x-plane were solved for the same number of iterations through the parameters selected in Table 1 above, as shown in Figure 4-6, where the horizontal axis represents the number of iterations, i.e., the time series, and the vertical axis represents the state of the system at x at the corresponding time series. It can be clearly seen that after 10,000 iterations, the improved 3D discrete chaotic system has a more uniform distribution in the x-plane from 0 to 1 compared to the other two systems and exhibits better chaotic properties.

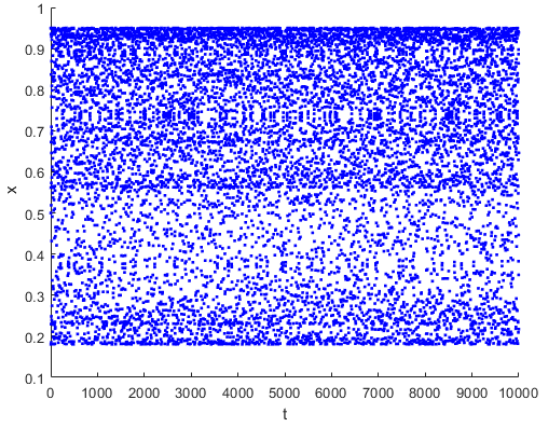

Figure 4. X-plane scatter plot of the one-dimensional logistic chaotic system

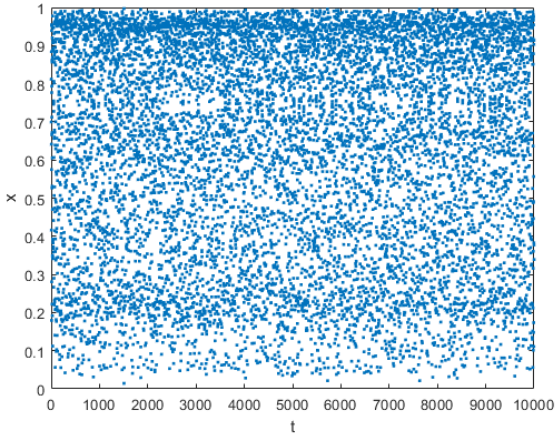

Figure 5. X-plane scatter plot of the 3D logistic chaotic system

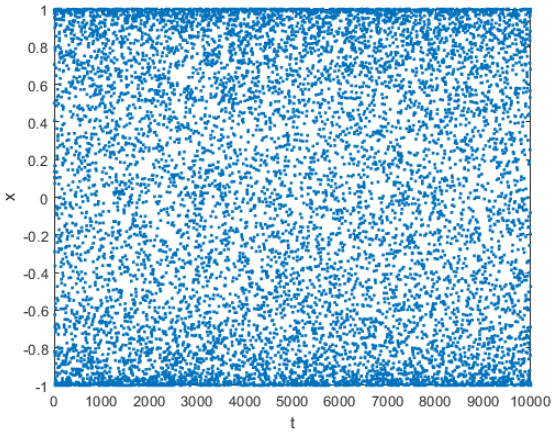

Figure 6. X-plane scatter plot of 3D discrete chaotic system

After the improvement in a coupled way, under the same number of iterations, the 3D scatter plots of 3D logistic chaotic system and 3D discrete chaotic system are solved by computation, as shown in Figure 7-8, comparing the 3D scatter plots of the two systems, it can be intuitively seen that the distribution of the scatter pass map of the 3D chaotic system after the coupling treatment is more even and the distribution of the scatter plots is no regularity in the intuitive view.

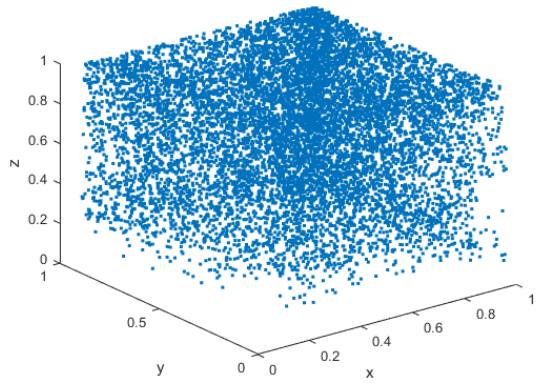

Figure 7. 3D spatial scatter plot of logistic chaotic system

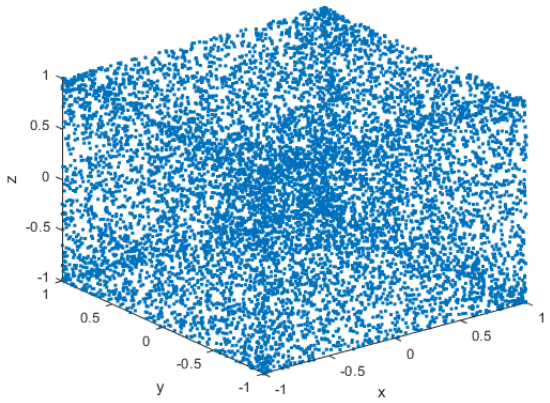

Figure 8. 3D spatial scatter plot of 3D discrete chaotic system

2.2.2. Lyapunov Exponent Analysis

Meanwhile, literature [25] shows that the Lyapunov exponent as is a measure of system sensitivity and chaotic nature, positive values indicate that the system is chaotic, negative values of the surface of the system tends to converge; in multi-dimensional chaotic systems, it is necessary to ensure that at least one of the Lyapunov exponent is positive, and the larger usually indicates that the system is more chaotic. Next, the Lyapunov exponents are obtained by taking the three chaotic systems as inputs conditional on the parameters identified in Table 1 above, by calculating the trajectories, the tangent directions, and then by logarithmically averaging the Jacobi matrices of the tangents. The obtained results are tabulated.

Table 2. Lyapunov exponent of chaotic system

Chaotic systemumber Lyapunov exponent	Lyapunov_x	Lyapunov_y	Lyapunov_z
One-dimensional logistic chaotic system	0.4371	/	/
Three dimensional logistic chaotic system	0.4525	0.4341	0.4950
Three-dimensional discrete chaotic system	3.0417	2.2273	2.3446

The change of Lyapunov exponent can be clearly seen

through Table 2, in the improved 3D discrete chaotic system, the Lyapunov exponent is not only all positive, but also compared with the magnitude of the exponent before the improvement, the 3D discrete chaotic system improved by this kind of method has more significant chaotic characteristics, which proves that the improved 3D discrete chaotic system in this paper is more suitable for the design of the pseudo-randomized sequence generator. design.

3. Design of Pseudo-random Sequence Generator based on Chaotic System

Pseudo-random sequences [26] are transformed over time and there is also no pattern to be found. It is one with uncertainty and the uncertainty is caused by external factors. The essence of the design of the pseudo-random sequence generator is determined by the algorithm, which is based on the principle of expanding an input of length k bits to length m (m>>k) bits by the algorithm so that it appears to satisfy that it is a random bit stream. The chaotic system is also one that is very sensitive to the initial conditions and coefficient parameters and can produce chaotic signals that are irreversible and irregular in timing. The characteristics of the two are somewhat related, so chaotic systems can be used as the basis for the design of pseudo-random sequence generators.

In pseudo-random numbers, the concept of "seed" is often used, and the output of the pseudo-random number is determined by the seed. So it can be understood that the input of the pseudorandom number generator can be called as the seed of the generator, so in this section, the modified three-dimensional discrete chaotic system mentioned above is used as a part of generating the pseudorandom sequences, in which the initial value of the system and the parameters of the system are used as the seed. This is then combined with a defined algorithm to finally obtain the pseudo-random sequence.

3.1. Design Method of Pseudo-random Sequence Generator

The initial value of the chaotic system and the system parameters are used as inputs to the improved three-dimensional discrete chaotic system to determine the seed chaotic sequence x, y, z. In order to enhance the stochasticity of the system, the computational quantization is carried out by post-processing, i.e., each element of the seed sequence is taken out one by one to the Nth digit after the decimal point (N is the number of natural numbers) for the judgment of the odd and even; the quantization of the data through the odd and even is to quantize odd as 1 and even as 0, and the final output pseudo-random sequence is obtained. The quantization of the data by odd and even numbers is to quantize the odd number as 1 and the even number as 0 to get the chaotic sequence x1, y1, z1, and then the chaotic sequence can get the final output pseudo-random sequence after appropriate combination processing. The workflow diagram of the entire pseudorandom sequence generator is shown in Figure 9.

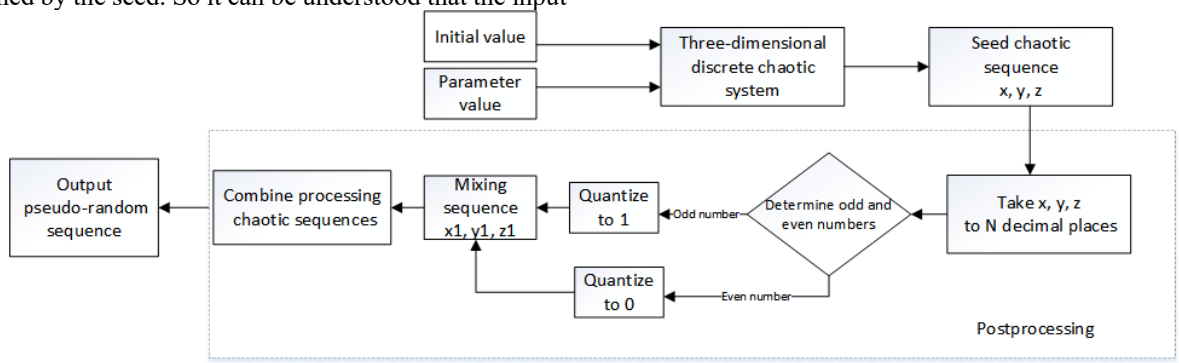

Figure 9. Schematic diagram of the design flow of the pseudo-random sequence generator

In order to carry out a test of the performance of the algorithm, it is convenient to compare with the random sequences generated by the algorithm by adding the post-processing proposed in this paper. In this paper, the seed chaotic sequence generated by the initial value and parameter values for the seed will be quantized by x, y, z according to whether it is greater than or equal to 0, to generate a set of comparison group chaotic sequences xx, yy, zz, the method of generating the comparison group is shown in Figure 10.

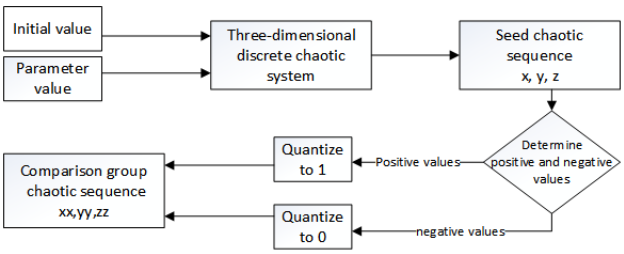

Figure 10. Schematic diagram of the design flow of the contrast group chaotic sequence generator

3.2. Improvement of 3D Discrete Chaotic Systems

In this section, firstly, through the three-dimensional discrete chaotic system produced by the timing diagram visualization, and from the perspective of correlation [27] on the seed chaotic sequence was analyzed, preliminary and intuitive judgment of random performance; secondly, through the algorithms proposed in this paper post-processing further quantization of the seed chaotic sequence to obtain the chaotic sequence, and on the sequence to complete through the uniformity [28], Fuzzy Entropy and Spectral Entropy [29] analysis; finally, the performance of the combined processed sequence is evaluated by the analysis method of NIST statistical test [30] system.

3.2.1. Performance Analysis of Seed Chaotic Sequences

A time series plot is a presentation of how the elements of a sequence change over time, i.e., as iterations are made here. Since chaotic sequences have random rows, then it can be determined whether some pattern, trend line or periodic oscillation is evident in the sequence in the timing diagram.

Figure 11 shows the timing diagram of a seeded chaotic sequence, the horizontal axis x represents the timing i.e. the number of iterations, the vertical axis y represents the values under the corresponding timing, and the three colors represent the three sets of seeded chaotic random sequences x, y, and z. It can be visualized from the graph that there is no obvious trend, periodicity or regular oscillations, and at the same time there is no aggregation of elemental values at certain time points or ranges. It can be preliminarily judged that the seeded chaotic random sequences have a certain degree of randomness through the time series diagram.

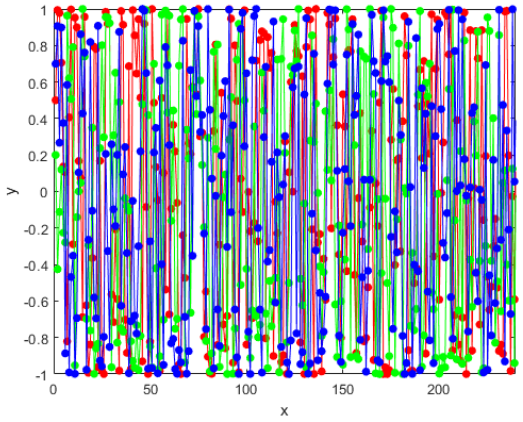

Figure 11. Timing diagram of seed chaotic random sequence

Correlation analysis plays a more important role in the random performance analysis of chaotic sequences; it is also one of the commonly used ways in the random performance analysis, and the more commonly used ones are autocorrelation and cross-correlation analysis, usually chaotic sequences have a better correlation is one of the important factors that chaotic sequences can be used.

The autocorrelation function is a functional method used in random sequences to evaluate the correlation between elements of the sequence and themselves. The autocorrelation function is usually computed at different lag orders (lag). The autocorrelation function of a random sequence with good random performance should be close to zero outside the lag order that is not 0, i.e., the autocorrelation coefficients are significantly non-zero only at the lag order of 0, while the coefficients of the other lag orders tend to be zero, then this usually indicates that the sequence is relatively independent and random. In this paper, the autocorrelation function is solved for the x-sequence in the seeded chaotic sequence, and the results are shown in Figure 12, where the horizontal axis represents the different lag orders and the vertical axis represents the autocorrelation coefficients. It can be seen that in the figure, the correlation coefficient of the lag order at 0 is 1, while the autocorrelation coefficient of the non-zero place tends to 0, and the decay rate is faster, the whole function is similar to the unit impulse function. Through the autocorrelation analysis, the seed chaotic random sequence has better randomness.

The inter-correlation function is a way to judge whether the given two sets of random sequences are independent and correlated or not, the inter-correlation of the random sequences with better random performance basically tends to be close to 0 at different lagging orders. Since the seed produces three sets of seeded chaotic random sequences, x, y, and z after passing through the three-dimensional chaotic system; it can be proved by judging the inter-correlation of the two sets of seeded chaotic random sequences respectively to this their sequences are independent of each other and random performance. In this paper, we take the x, y sequences to solve the inter-correlation as an example, and the results are shown in Figure 13, with the horizontal axis representing the different lag orders and the vertical axis representing the number of inter-correlations. From the literature [31], the correlation coefficient of 0±0.009 is considered as no correlation and 0. 1 ± 0. 30 is considered as weak correlation. As shown in Figure 3.5, the inter-correlation between its seed chaotic sequences performs well.

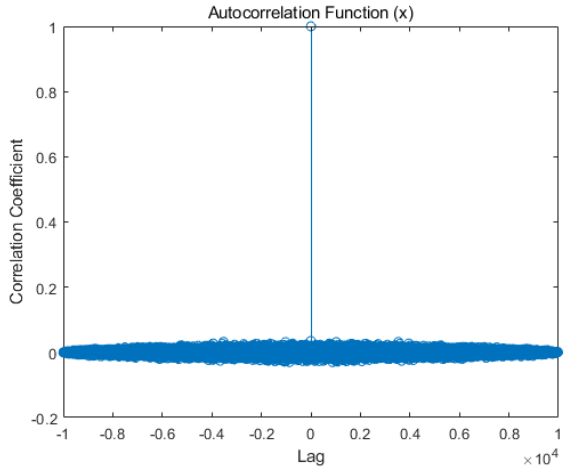

Figure 12. Autocorrelation plots of seed chaotic random sequences

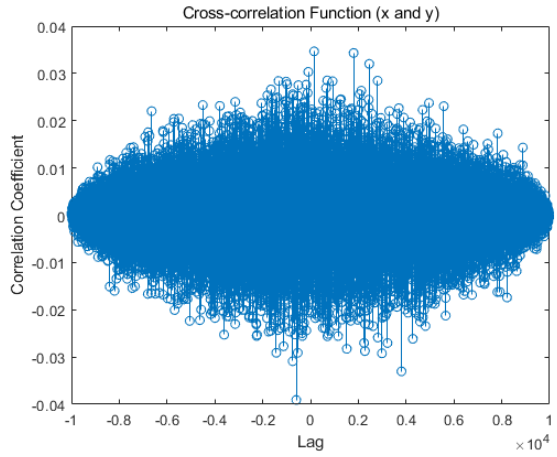

Figure 13. Interrelationship maps for seeded chaotic random sequences

3.2.2. Performance Analysis of Pseudo-random Sequences

After the above mentioned seeded chaotic random sequences are quantized by the above mentioned post-processing, the chaotic sequences x1, y1, z1 are generated and analyzed for homogeneity respectively, and the results of this paper are shown in Table 3 after their statistical analysis here.

Table 3. Distribution of 1 and 0 of chaotic sequences

Sequence name 1, 0 distributions	1 Number of distributions	0 Number of distributions	The percentage of 1
x1	4831	5169	48.31%
y1	4946	5054	49.46%
z1	5090	4910	50.90%

If a chaotic sequence with better random performance, the distribution of the number of 0, 1 is average. Through the above table, it can be seen that after 10,000 iterations, the

number of 1 in the distribution of x1, y1, z1 are 4891, 4946, 5090; the proportion of 48%, 49%, 51%; basically, converging to the proportion of 50%, which can be preliminarily judged to be better randomness.

Secondly, this paper on the chaotic sequence x1, y1, z1 in accordance with the method of the literature [29], respectively, fuzzy entropy, spectral entropy algorithm calculation, and its literature for comparison; and calculated as shown in Figure 10 process of simple quantization of the resulting xx, yy, zz comparison of the group of chaotic sequences for comparative analysis, here are the x-sequence of the computation of the comparison, as shown in Table 4. It should be noted that the complexity of the size of the fuzzy entropy algorithm, spectral entropy algorithm measure value is proportional to the complexity of the sequence randomness.

Table 4. Results of sequence complexity analysis

Sequence name	Fuzzy entropy	Spectral entropy
org-x[29]	0.6722	0.6476
PRS-x[29]	0.7899	0.9312
Comparison group chaotic sequence xx	0.7114	0.7275
Chaotic sequence x1	0.9298	0.9799

From the comparative analysis of the above table, it can be seen that the random performance of the chaotic sequence of the comparison group is better than the randomness of the original sequence in the literature [29], but fails to be better than the improved random sequence in the literature; while the chaotic sequence quantized through the post-processing of this paper has a certain enhancement in fuzzy entropy and spectral entropy, and a certain decrease in intensity statistics, that is to say, it shows that the chaotic sequence x1 has a better random performance.

3.2.3. NIST Statistical Test

Through the XOR method of three groups of quantized random sequences one by one, the pseudo-random sequence was finally generated. To test its performance of pseudo random number of random, this paper adopted by the national institute of standards and technology (NIST) proposed by NIST test suite [30].

The NIST test suite is a set of 15 tests that measure the randomness of binary sequences of 1's and 0's generated in hardware or software by cryptographic random number or pseudo-random number generators (of arbitrary length). It contains 15 testing criteria such as Frequency, Block frequency, etc. Where P-value [31] is the level of significance, which is recommended by NIST to be 0.001-0.01, i.e. greater than 0.01 is considered as a pass. In this paper, the generated pseudo-random sequence is tested numerically by NIST based on Linux. And as shown in Table 5, the detailed data of P-value of them are listed and the P-value greater than 0.01 result is considered as pass.

Through the above results, it can be seen that the pseudorandom sequence can pass the NIST test for all the 15 criteria detected by the pseudorandom sequence. It shows that the pseudo-random sequence generator designed in this paper can produce pseudo-random sequences, and the pseudo-random sequences have better random performance.

Table 5. Results of NIST detection of pseudo-random sequences

Serial number	Test item	P-value	Pass or not pass
1	Frequency	0.042808	Pass
2	Block frequency	0.076029	Pass
3	Cumulative Sums	0.066882	Pass
4	Runs	0.046000	Pass
5	Longest Run	0.319084	Pass
6	Rank	0.010538	Pass
7	FFT	0.013569	Pass
8	Non Overlapping Template	0.971699	Pass
9	Overlapping Template	0.816537	Pass
10	Universal	0.213309	Pass
11	Approximate Entropy	0.020300	Pass
12	Random Excursions	0.032216	Pass
13	Random Excursions Variant	0.021060	Pass
14	Serial	0.554420	Pass
15	Linear Complexity	0.080519	Pass

4. Conclusion

The randomness performance of the pseudo-random sequences generated by the pseudo-random sequence generator based on the low-dimensional chaotic system has room for further improvement and needs to be further optimized. Therefore, in this paper, we improve and design a method of constructing a three-dimensional discrete chaotic system, and through the scatter plot and Lyapunov exponent, we intuitively and objectively verify that the above system has more complex chaotic characteristics, which is more suitable for the design of pseudo-random sequence generator. Then, based on the seed chaotic sequences produced by the 3D discrete chaotic system, a pseudo-random sequence generator is designed by combining with the post-processing method, and the pseudo-random sequences produced by the output of the pseudo-random sequence through the correlation and a series of indexes of the computation and analysis, which proves that the pseudo-random sequences produced by the pseudo-random sequence generator designed based on the 3D discrete chaotic system in this paper have a better randomness and the pseudo-random sequences have passed the NIST suite of tests. NIST suite of tests.

This paper provides a method for the construction of chaotic systems and combines the application with the pseudorandom sequence generator to produce pseudorandom sequences with better randomness, and the work in this paper also has a practical application background.

References

[1] Zhuo Liu. Characterization of complex chaotic systems and its application in image encryption [D]. Chongqing University of Posts and Telecommunications,2022.

[2] Liu Yu. Research on image encryption technology based on chaos theory and its cryptanalysis[D]. Hunan University,2021.

[3] Chuanfu Wang. Dynamics analysis and pseudo-random sequence generation algorithm design of digital chaotic system[D]. Heilongjiang University,2020.

[4] Wang T. A chaotic sequence characterization and FPGA implementation based on Chebyshev polynomials[D]. Yunnan University,2014.

[5] Chuanfu Wang. Dynamics analysis and pseudo-random sequence generation algorithm design for digital chaotic systems[D]. Harbin:Heilongjiang University.2020:1-13.

[6] Liu F, Ji XY, Wang YQ, et al. Design of FPGA-based CPRS chaotic encryption and decryption chip algorithm [J]. Computer Engineering and Design, 2010,(11):2419-2422.

[7] FethiD,SafwanAE,HadjEWY,etal.Design,FPGA-based Implementation and Performance of a PseudoRandom Number Generator of Chaotic Sequences [J]. ADVANCESINEL ECTRICALANDCOMPUTERENGINEERING,2021,21(2):4 1-48.

[8] DING Wei. Design and application research of four-dimensional discrete chaotic system based on FPGA[D]. Heilongjiang University,2022.

[9] Chen F, Liu JD, Hu HH, et al. Two-dimensional integer tent mapping model design and security simulation analysis[J]. Computer Engineering and Applications, 2019, 55(1):103-108, 173.

[10] Tian Ruyi,Gu Fengjun,Peng Kun et al. Network information encryption based on one-dimensional Logistic mapping and two-dimensional Tent mapping dual chaos idea[J]. Computerized Measurement and Control,2023,31(06):280-286.

[11] WangL,RanQ,DingJ.ImageEncryptionUsingQuantum3DMobi usScramblingand3DHyper-Chaotic HenonMap [J]. Entropy, 2023, 25(12).

[12] AndrewR.,JuanS.,JamesN.,Astatisticaltestsuiteforrandomandp seudorandomnumbergeneratorsforcryptographicapplications[M]. NISTSpecialPublication,800-22,2001.

[13] Y. Q. Hu. FPGA implementation of pseudo-random sequence generator based on hyper chaos[D]. Tianjin University of Technology, 2018.

[14] Qiu Jin. Research on chaotic pseudo-random sequence and its application in digital image encryption[D]. Chongqing University, 2011.

[15] P.C. Wei. Chaotic pseudorandom sequences and their applications [D]. Chongqing University, 2008.

[16] YUAN Zeshi, ZANG Fei. Cascading of Chen systems with cubic terms and design of random number generators[J]. Journal of Anhui University of Technology (Natural Science Edition), 2020,37(04):379-384.

[17] SaadMF,KadhimAF,NatiqMF.Designing Substitution Box Based on the 1Dlogistic MapChaotic System [J]. IOP Conference Series. Materials Science and Engineering, 2021, 1076 (1):012041-.

[18] Tao H. Design of image encryption based on logistic chaotic sequences [D]. [Master's thesis],Southeast University,2018.

[19] Jun Lang, Zhengchao Hao. Novel image fusion method based on adaptive pulse coupledneural network and discretemulti-parameter fractional randomtransform [J]. Optics and Lasersin Engineering, 2014,52(15):91-98.

[20] Yang Chao.Liapunov stability analysis of aircraft magnetorh eological landing gear system[J]. Foreign Electronic Measurement Technology, 2020, 39(12): 34-37. DOI:10. 19652 /j. cnki. femt. 2002290.

[21] Zhenzhen Lu. Analysis and design of image encryption algorithm based on discrete chaotic system[D]. PLA Information Engineering University,2012.

[22] WANG Yong,JIANG Gongkun,YIN Enmin. Image encryption based on two-dimensional coupled image lattice model[J]. Journal of Southwest Jiaotong University,2020,6:1048-1057. WANGYong, JIANGGongkun,YINE.

[23] DiscreteandContinuousDynamicalSystems;Researchers from NewYork University (NYU) Report Recent Findings in Discrete and Continuous Dynamical Systems (Nonuniformly Hyperbolic Systems Arising From Coupling of Chaotic and Gradient-likeSstems)[J].JournalofMathematics,2020,1273-.

[24] C.F.Wang,C.L.Fan,Q.Ding.Constructing Discrete Chaotic Systems with Positive Lyapunov Exponents [J]. International Journal of Bifurcation and Chaos, 2018,28(7):1850084.

[25] Zhou X. Research on some problems of chaos theory and applications[D]. Nankai University, 2010.

[26] Yan Fuping. DSP implementation of double-precision floating-point chaotic pseudo-random sequence generator[D]. Central South University,2009.

[27] Wang Yudong, Liu Chunlei. New proof of Gold sequence mutual correlation and the study of non-maximal Gold sequence properties [J]. Communication Technology, 2014 (3): 241-246.

[28] Lei Liping. Design of Chaos-based Random Sequence Generator and Its Application[D]. Nanjing University of Aeronautics and Astronautics, 2007.

[29] SUN Kehui, YE Zhengwei, HE Shaobo. FPGA design and implementation of chaotic pseudorandom sequence generator [J]. Computer Application and Software, 2014, 31 (12): 7-11+20.

[30] WEI Yanwen, LI Zhen, LI Liangrong. Design of pseudo-random number generator based on chaotic system[J]. Electronic Technology Applications, 2020, 46(10): 114-117+ 122. DOI:10.16157/j.issn.0258-7998.200596.

[31] NISTspecialpublicationSP800-22Rev[EB/OL].(2010-04-15). http:// csrc. nist. gov/ publications/ nist-pubs/ 800-22-rev1a/ SP800-22rev1a.Pdf.