Research on Chaotic Image Encryption Based on Fibonacci-ILogistic-IHenon

Yong Yang[1], Xuan Chen[1], Jiaying Xu[1]
and Yuxia Li[2,*]

[1]*Zhejiang Industry Polytechnic College, Shaoxing, Zhejiang, 312000, China*
[2]*Beijing Union University, Beijing, 100025, China*
E-mail: bjlyx1970@sina.com
[*]*Corresponding Author*

Received 15 September 2023; Accepted 16 October 2023;
Publication 13 February 2024

Abstract

To further improve the security of image encryption, we propose an image encryption algorithm that combines Fibonacci with improved logistic and improved Henon chaotic mapping, i.e., the Fibonacci-ILogistic-IHenon algorithm. The algorithm addresses that the existing logistic chaotic algorithm is controlled by the parameter resulting in an uneven distribution, and the Henon chaotic algorithm may have the problem of periodic orbits. Using the mode-taking and sinusoidal functions for optimization, the output sequence region generated by the logistic chaotic mapping is adjusted to the input of the Henon chaotic mapping, which enables the construction of a new chaotic system (ILogistic-IHenon). In the image encryption implementation, Fibonacci is used to cure the chaos, and ILogistic-IHenon is utilized to generate chaotic sequences to complete the encryption. In the simulation experiments, we choose the improved logistic encryption algorithm, the improved Henon encryption algorithm, and the improved logistic-ent encryption algorithm

Journal of Cyber Security and Mobility, Vol. 13_2, 215–238.
doi: 10.13052/jcsm2245-1439.1322

as the comparison algorithms, and the results illustrate that the Fibonacci-ILogistic-IHenon algorithm has better performance in image encryption statistical analysis, encryption speed, pixel correlation analysis, information entropy analysis, differential attack analysis and other metrics.

Keywords: Chaos, image, encryption.

1 Introduction

Accompanied by the rapid promotion and popularization of 5G network technology and digital communication technology worldwide, digital images have become an important medium for information storage and transmission in computer networks [1]. Digital images have become an important content of data transmission in networks by virtue of their intuition and convenience. Especially in recent years, against the background of increasingly severe network security conditions, the transmission and sharing of information based on digital images often face problems such as data theft, tampering, deletion, and attacks, which cause great losses for the owner or publisher of digital images [2]. Image encryption technology is a commonly used technical means and program that plays a key role in the protection of image content. In recent years, chaotic encryption technology has received great attention from the information security community by virtue of its advantages, such as high efficiency and strong security, and it has also been promoted and applied to a certain extent in the field of digital image encryption. Many digital image protection schemes based on chaotic encryption have entered into the field of practical applications [3], but digital image protection technology based on chaotic encryption has still not been developed to maturity, and the research of digital image encryption is still of great importance. The study of chaotic encryption technology still has certain theoretical significance and practical value, and it has become the research object that scholars focus on. These encryption techniques mainly take logistic, Henon, and tent as the main chaotic systems in image encryption and have achieved better results.

In this paper, by examining and analyzing the basic theoretical and technical foundations of digital image chaos encryption technology, we propose a Fibonacci-ILogistic-IHenon-based image encryption algorithm, which first uses Fibonacci to rule the chaos and then generates chaotic sequences using the ILogistic-IHenon system composed of the improved logistic and Henon to complete the encryption of the image, and the encryption effect of this algorithm is validated by comparing the results with the other chaos algorithms in the experiments.

In this paper, we are organized as follows: Section 2 categorizes the current research on chaotic encryption; Section 3 introduces the chaotic algorithms that need to be used in this paper; Section 4 describes the improved logistic-henon chaotic mapping; Section 5 describes the process of using this paper's algorithms for image encryption; Section 6 verifies the performance and superiority of this paper's algorithms in simulation experiments from several aspects; and Section 7 summarizes.

2 Related Research

Based on the research on chaotic image encryption, scholars from various countries have carried out different degrees of research, which is roughly categorized into the following three aspects.

(1) Single chaotic mapping scheme. Most scholars used a one-dimensional chaotic algorithm for image encryption and achieved good results. For example, [4] proposed a new color image encryption algorithm based on one-dimensional logistic mapping. The algorithm uses one-dimensional chaos to make the key space of the algorithm smaller, but the robustness of the algorithm is not good due to the direct use of chaotic sequences generated by the chaotic mapping without other operational processing. Literature [5] proposes to first use the affine and substitution methods of traditional cryptosystems for encryption and then use the extended one-dimensional logistic chaotic map to enhance the encryption process, and simulation experiments illustrate the superiority of the proposed method. Literature [6] uses a dual Henon model for encryption, and experimental results show that the proposed encryption system is simple and fast with an additional random switching effect. Literature [7] proposed an image encryption system with Henon chaos with nonlinear terms, and the experiments verified the security of the encryption algorithm through secret key space analysis, anti-statistical attack analysis, anti-differential attack analysis, and anti-shear and noise attack analysis. Literature [8] proposed an image encryption scheme based on chaotic mapping and metacellular automata, which utilizes segmented linear chaotic mapping to obfuscate the original image in the replacement phase and logistic mapping and reversible metacellular automata in the diffusion phase to obtain efficient and secure cryptosystems, but the algorithm encrypts

at a slower speed. From the above research results, although the one-dimensional chaotic system has a good encryption effect, it has the disadvantages of short periodicity, small key space, low security, and the risk of encrypted information being cracked. Literature [9] proposes a novel and effective image encryption algorithm that utilizes PWLCM to generate a key image and then encodes the plaintext image and the key image line by line using DNA rules and performs DNA operations on a line-by-line basis between the plaintext encoding matrix and the key matrix. The different line encoding rules and operation rules are determined by logistic mapping.

(2) High-dimensional chaotic system scheme. Literature [10] proposed a new four-dimensional hyper chaotic system. The hyperchaotic system has good stochastic properties and can be applied to image encryption. Literature [11] proposed combining DNA coding and a new four-dimensional chaotic system to control the dislocation to exchange the position, and the dislocation is diffused using DNA operations. Literature [12] proposed a novel approach to design a high-dimensional digital chaotic system, which is based on random sequence control, making a multidimensional system to encrypt images, but the complex structure makes it difficult to implement and inefficient. Literature [13] proposed a new two-dimensional improved coupled mapping (2D-ILCM) to encrypt images with multidimensional chaotic systems. The algorithm is robust, but the structure is complex and not easy to implement, and the time consumed is correspondingly longer. Literature [14] designed a two-dimensional logistic-Gaussian hyperchaotic map (2D-LGHM) with a wide hyperchaotic range, which is modeled with substitution and multidirectional pixel substitution processes, and the results show that the scheme has high robustness and effectiveness against different security attacks and data loss. From the results of the above scholars, although high-dimensional chaos achieves better encryption than low-dimensional chaos, the complexity of the structure makes it more difficult to realize, and the time cost is higher. Literature [15] proposes an encryption scheme that utilizes three-dimensional (3D) logistic and S-boxes for obfuscation. Simulation results illustrate the advantages of this proposal in the design of encryption schemes.

(3) Fusion of multiple simple chaotic systems. Literature [16] proposed a new image encryption algorithm based on dual chaotic systems, which uses a two-dimensional Baker chaotic mapping to control the system parameters and state variables of the logistic chaotic mapping so that

the generated sequences will also be more random and unpredictable. Literature [17] proposed three chaotic systems, the logistic-tent system, logistic-sine system and tent-sine system, for image encryption, and simulation experiments verified the superiority of this chaotic system in encryption. Literature [18] proposed a new piecewise logistic sine encryption model (PLSM), and the simulation results show that the model has better chaotic behavior and lower time complexity. Literature [19] proposed an encryption scheme based on logistic-tent fusion, and simulation experiments and security evaluation showed that the model has a good encryption effect. Literature [20] proposed a chaotic image encryption algorithm based on extended sawtooth obfuscation and RNA operations, which improves the problem of uneven distribution of chaotic sequences of logistic and sine mapping and combines the two. The algorithm improves the problem of uneven distribution of logistic and sine mapping chaotic sequences and combines the two chaotic systems to obtain a good encryption effect. Literature [21] proposed a color image encryption technique based on bit-level chaos using Logistic-Sine-Tent-Chebyshev (LSTC) map. The experimental results show that the encryption is well protected against statistical attacks, differential attacks and brute force decryption attacks after only 1 round of encryption. Literature [22] proposed a chaotic image encryption model based on fuzzy concepts, and experiments illustrated that the encryption scheme is fast, secure and efficient in various security and statistical analyses. Literature [23] proposed a Henon-Logistic-Tent-based chaotic encryption model, and experiments illustrated that the model is able to withstand different security attacks and is more efficient, especially in terms of encryption time. Literature [24] proposed an Arcsine-Sine-Logistic image encryption model based on Arcsine, and the simulation experimental results illustrate the effectiveness of the proposed algorithm from different aspects. From the above scholars' research results, the fusion of multiple chaotic systems can improve the encryption effect, and the space complexity is lower than that of high-dimensional chaotic systems, so it is welcomed by the majority of scholars.

Through the above research, we found that chaos-based schemes play an important role in image encryption, especially new chaotic encryption schemes, and the fusion of multiple single chaotic algorithms has become a new research direction at present. Based on this, this paper carries out research on this topic. The study of the fusion of improved logistic and improved Henon models is proposed.

3 Introduction to the Algorithm

(1) Logistic chaos mapping

Logistic chaos is a common one-dimensional dynamical system that is widely used to study chaotic phenomena. It has the advantages of a simple structure and easy-to-implement platform, and its mathematical expression is as follows:

$$x_{n+1} = \mu x_n (1 - x_n)(n = 1, 2, 3) \tag{1}$$

where x_n denotes the mapping function and μ denotes the parameters.

(2) Henan mapping

Henon mapping is a two-dimensional nonlinear dynamical system often applied to study chaotic phenomena that is able to produce complex trajectories through a simple iterative formulation, allowing different system behaviors to be observed. The expression is as follows:

$$\begin{cases} x_{n+1} = 1 + y_n - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \tag{2}$$

where a and b are the system control parameters.

(3) Fibonacci disruption

Disambiguation is a fundamental encryption technique in image encryption that reduces the image pixel correlation by processing the image. The nonlinear Fibonacci series is a two-dimensional chaotic mapping that can realize a better pixel disruption effect in the image encryption algorithm. The specific operation process is as follows: For the original image of size $M \times N$, use formula (3) to realize the disambiguation operation, set the iteration number, and obtain the Fibonacci disambiguation matrix F by formula (4). The Fibonacci series disambiguation has a periodicity, and the set iteration factor should be kept secretly. The key factor is applied in image preprocessing to expand the space of the key.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod M \tag{3}$$

$$Q^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n+1} \end{bmatrix} \tag{4}$$

where (x', y') denotes the pixel point in the original image matrix, (x, y) is the pixel matrix coordinate, and M is the order of the pixel matrix.

4 Improved Logistic-Henon Chaos

To better enhance the effect of image encryption, we use logistic and Henon chaotic mapping as the model for modeling chaotic systems in this paper, but due to the simple structure of these two chaotic systems, the computational cost is low and can be widely used, but because they can only show good chaotic effects only in a small parameter range, they are easily affected by the parameter and lead to chaotic performance degradation. In this paper, we integrate logistic chaos and Henon chaos mapping in depth. The main idea is to use the output sequence area generated by logistic chaos mapping to adjust the input of Henon chaos mapping and then use the modal operation to obtain the result fixed to a certain range of values to construct a new kind of two-dimensional chaotic system. However, since logistic chaos and Henon chaos have certain shortcomings, in this paper, we first optimize the two chaotic systems and then generate the improved logistic-improved Henon (ILogistic-IHenon) mapping by fusion.

(1) Improved logistic chaotic systems

To address the problem that the logistic is controlled by the parameter that leads to uneven distribution, we improve the logistic, and the expression is as follows:

$$X_{n+1} = \mathrm{mod}((r \times x_n), 1) \tag{5}$$

where $r \neq 0$ is a control parameter, x_n is between [0,1], and the modulus function $\mathrm{mod}(w, z)$ represents the remainder returned after taking the modulus. Although Equation (5) will increase the computational workload and the time consumption of the encryption system by adding the modulus operation, it can make the parameter range in Equation (5) break through the traditional limit of (0, 4], thus expanding the chaotic region of the system as well as the encrypted key space of the system.

(2) Improved Henon chaotic system

To avoid the problem that the Henon chaotic algorithm may produce obvious periodic orbits rather than a lack of true chaotic behavior, we improve the Henon chaotic system according to the following expression.

$$\begin{cases} x_{n+1} = 1 + \sin y_n - a x_n^2 \\ y_{n+1} = \sin b x_n \end{cases} \tag{6}$$

Figures 1(a) and 1(b) show the original Henon chaotic orbits and the improved chaotic orbits, respectively. When a is 2.1 and $b \in (-\infty, -0.74) \cup$

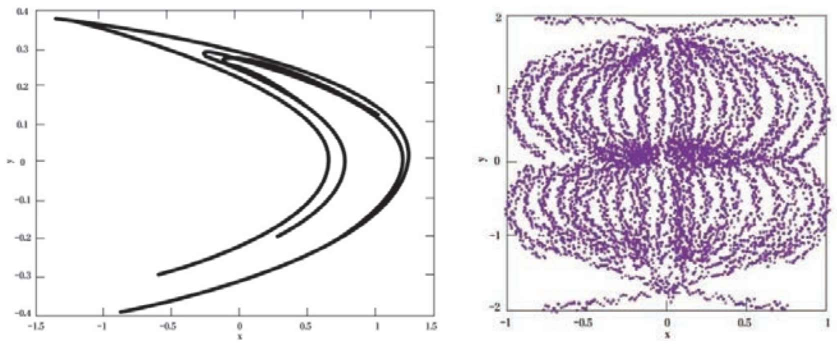

Figure 1(a) Henon motion track before improvements

Figure 1(b) Henon motion track after improvements

Figure 1 Henon motion track before and after improvement.

$[0.74, +\infty)$, the improved Henon mapping is in a chaotic state, and the chaotic output traverses better.

(3) Improved Logistic- Improved Henon Mapping

Based on the above two improvements, we construct the improved 2D logistic-Henon mapping, namely, ILogistic-IHenon, which integrates the optimized properties of both the improved logistic and Henon mappings and improves the encryption performance with the following expression:

$$\begin{cases} x_{n+1} = a_1 + \sin(\mathrm{mod}((r \times x_n), 2)) - a_2 x_n^2 \\ y_{n+1} = \sin(a_3 \times \mathrm{mod}((r \times x_n), 1)) \end{cases} \tag{7}$$

where a_1, a_2 and a_3 denote unknown parameters, and r denotes control parameters.

5 Image Encryption Algorithm

5.1 Algorithm Flow

In this paper's algorithm, we use the random sequence generated by ILogistic-IHenon to increase the security characteristics of the system, and the encryption process of the algorithm is divided into 2 processes, namely, the Fibonacci series is mainly used to realize pixel disruption of the image, and the ILogistic-IHenon mapping is used to generate chaotic sequences. In the diffusion operation, multiple initial parameters are added to control

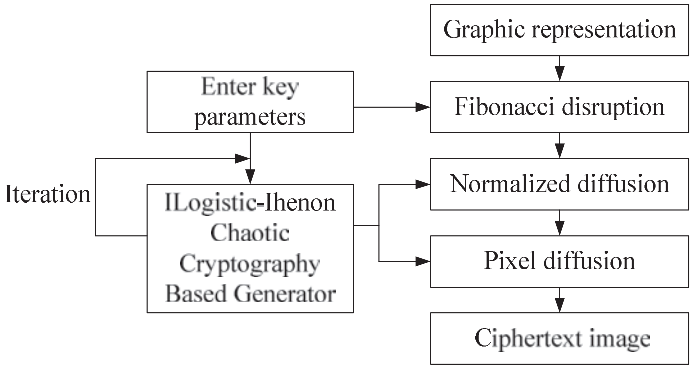

Figure 2 Flowchart of the encryption algorithm.

the generation of the key sequence to improve the security of the algorithm. The encryption process is shown in Figure 2.

5.2 Algorithmic Steps

(1) Key Generator

In the algorithm of this paper, the relevant parameters X_0, a_1, a_2, a_3, r and other parameters are set as the initial key, the image P is set as the original image of size (M, N), and (i, j) is the pixel point of the ith row and the jth column on the corresponding image. Iterate $M \times N$ over the initial value X_0 and take the iterated data to generate a chaotic stream cipher sequence of length $M \times N$.

(2) Encryption process

Step 1: Encryption Preprocessing. The original image is used as input for the separation of three channels, which are stored in different $P_{M \times N}$ arrays, and then each step of the operation is carried out on the $P_{M \times N}$ groups of the three channels. The size of the original image P obtained, which is saved by using (M, N), the setting $n = M \times N$, the setting of the key sequence X_n, the input of the initialization of the unknown parameter and the control parameter, and the use of the chaotic cipher with the ILogistic-IHenon X_0 is iterated $M_1 \times N_1 + M_2 \times N_2$ using ILogistic-IHenon's chaotic cryptography generator, in which the chaotic state X_1 is obtained by iterating $M_1 \times N_1$ times, and then the chaotic key sequence X_n is obtained by iterating $M_2 \times N_2$ according to the chaotic state X_1.

Step 2: Fibonacci disambiguation. Select parameter l as the key of the Fibonacci disambiguation algorithm, disambiguate the plaintext image array $P_{M \times N}$ to be encrypted, and then obtain the disambiguation matrix $A_{M \times N}$.

Step 3: Normalized diffusion. The chaotic key sequence X_n generated by the ILogistic-IHenon chaotic key generator is normalized, and its range is encrypted by diffusion through the parameters a_1, a_2, a_3, r, etc., to enhance the security and complexity of the algorithm, i.e., according to the following equation:

$$Y_i = \bmod\left(\left\lceil \frac{b+1}{(b+c+2)} \times x \times M \times N \right\rceil, 255\right) \tag{8}$$

Expand each element of the key sequence X_n to between (0.255) and convert the sequence to an $M \times N$ matrix to obtain the diffusion key matrix $Y_{M \times N}$.

Step 4: Pixel diffusion. The diffusion key sequence $Y_{M \times N}$, obtained after normalized diffusion through the above, is based on the following equation:

$$Z(i,j) = Y(i,j) \otimes A(i,j) \tag{9}$$

The encrypted ciphertext image $Z_{M \times N}$ is obtained by diffusion encryption of pixels with the scrambled pixel matrix $A_{M \times N}$ of the waiting encrypted plaintext.

Step 5: Channel merging. The encrypted ciphertexts $Z_{M \times N}$ of different channels obtained after the above steps are merged to obtain the final ciphertext image.

The combination of the above five steps is the Fibonacci-ILogistic-IHenon-based image encryption scheme proposed in this paper, and the decryption process is the inverse of the encryption process.

5.3 Key Space Analysis

Key space analysis refers to the analysis of the size of the key's valueable space. In an encryption system, the size of the key space is determined by all the relevant parameters that are used in the encryption process. Within the range of existing computational capabilities, a key space larger than 264 bits can be considered a secure system key space, which is resistant to the existing means of brute force decryption. The image encryption scheme proposed in this paper contains a total of six security keys, and the encryption scheme

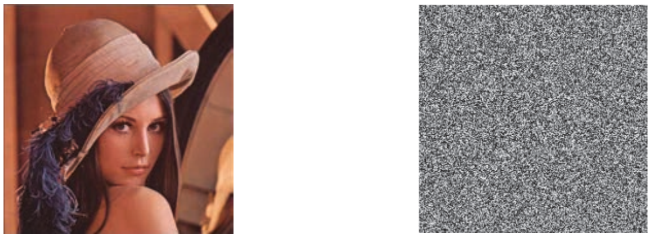

Figure 3(a) Original Lena image

Figure. 3(b) Encrypted Lena image

Figure 3 Comparison of images before and after Lena encryption.

using Fibonacci transform and logistic-Henon mapping has an accuracy of 10^{-16} under the condition of double precision of the computer. Then, the key space proposed in this paper is at least 1096 bits. Therefore, the key space of the image encryption scheme based on the Fibonacci transform and logistic-Tent chaotic mapping is large enough to effectively defend against brute-force cracking and achieve a high level of security.

6 Simulation Experiments

To further practice the effect of our proposed algorithm, we divide the experiment into two parts. The first part tests the performance of the algorithm in this paper, and the second part compares other algorithms to verify the effect of the encryption index. We choose CPU as Core I7, memory as 16GDDR3, hard disk capacity as 1T, software system as Windows, and simulation software as MATLAB 2010. We chose the Improved Logistic Encryption Algorithm (ILogistic) [5], the Improved Henon Encryption Algorithm (IHenon) [7], and the Improved Logistic-Tent fusion encryption algorithm (ILogistic-Tent) [19] as comparison algorithms in this paper (ILogistic-IHenon).

6.1 Performance of the Algorithm in This Paper

We chose the classic 256 × 256 Lena shown in Figure 3 as the performance test object and selected only representative indicators in terms of statistical analysis and correlation of neighboring elements for comparison.

(1) Statistical analysis

Figure 2 shows the comparison of the histogram effect of this algorithm before and after encryption, of which Figure 1(a) shows the statistical analysis

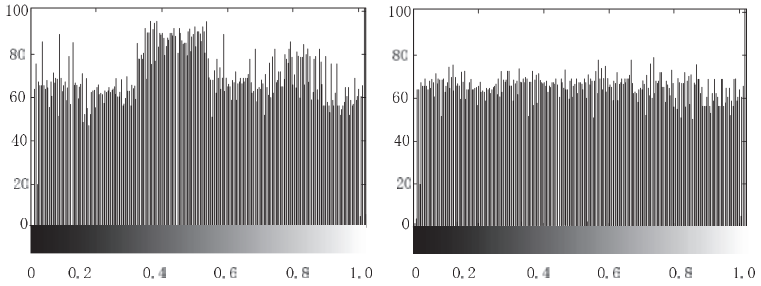

Figure. 4(a) Histogram of original Lena image Figure. 4(b) Histogram of encrypted Lena image

Figure 4 Histogram of the Lena image before and after encryption.

of the Lena image before encryption. Figure 2(b) shows the statistical analysis of the Lena image after encryption. It can be found that in the figure without encryption before the distribution of the image's grayscale histogram is not very uniform, the overall amplitude of the overall distribution of encrypted image is very uniform, which indicates that the effect of the statistical analysis using the algorithm in this paper is good.

(2) Neighboring pixel correlation

Neighboring pixel correlation in an image relates to the encryption effect of the image. To illustrate the effect of this paper's algorithm on its encryption, we select 100 groups of pixels adjacent to the image of Figure 1, according to formulas (10)–(13), to calculate the encrypted image in the horizontal, vertical, diagonal direction pixel correlation and the pixel correlation in the horizontal, vertical, and diagonal directions, and the pixel correlation in the diagonal direction is calculated according to formulas (11)–(13).

$$E(x) = \frac{1}{N}\sum_{k=1}^{N} x_k \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{k=1}^{N} (x_k - E(x)) \tag{11}$$

$$Cov(x, y) = \frac{1}{N}\sum_{k=1}^{N} (x_k - E(x))(y_k - E(y)) \tag{12}$$

$$r(x, y) = \frac{|Cov(x, y)|}{\sqrt{D(x)\sqrt{D(y)}}} \tag{13}$$

Table 1 Correlation of two neighboring pixels of three images

Direction	Figure 1(a)	Figure 1(b)
Horizontal	0.8942	0.0079
Vertical	0.8723	0.0085
Diagonal	0.8816	0.0081

Table 2 Time complexity of the three images (%)

Direction	Figure 1(a)	Figure 1(b)
Horizontal	83.21	53.27
Vertical	81.42	61.35
Diagonal	94.35	63.32

where Cov in Equation (12) denotes the covariance, (x, y) denotes the gray value of the neighboring pixel points in the image, and N is the number of pixels picked. Table 1 shows the results of the correlation of neighboring elements of the Lena image in three directions before and after encryption. From the data results, the image in the three directions of the comparison of the data results are very different, which shows that the encrypted image retains the main pixel characteristics of the original image. Through the results of the comparison of the time complexity of Table 2, after encryption, the complexity of the image has been reduced, although the magnitude of the reduction of the time is not very large. The time complexity of the encrypted image is reduced, although the reduction in time is not very large, the encrypted information of the image is still well preserved, which is mainly due to the increase in the complexity of the encryption algorithm affecting the encryption time. Figure 3 shows the comparison results of the image in three directions: diagonal, horizontal and vertical. From the comparison in the figure, the neighboring pixel values of the original image in each direction are roughly concentrated near the center region, but the overall distribution of pixels in the encrypted three images shows a random distribution, which shows a better encryption effect.

The comparison of the above two aspects of the index data shows that the algorithm in this paper does have a certain effect in terms of encryption performance and has a certain role in promoting the enhancement of the encryption effect.

(3) NIST test

In this paper, we introduce the random test suite NIST SP800-22 to carry out a random test on the key generated by this paper's algorithm. The test is

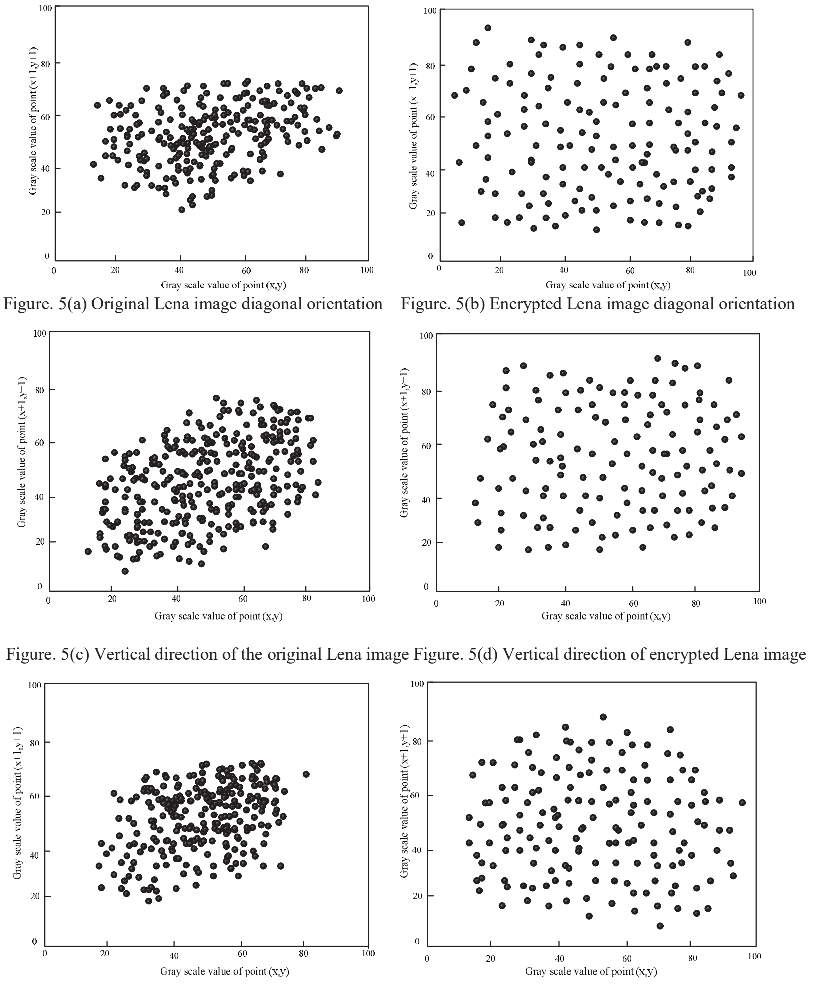

Figure. 5(a) Original Lena image diagonal orientation Figure. 5(b) Encrypted Lena image diagonal orientation

Figure. 5(c) Vertical direction of the original Lena image Figure. 5(d) Vertical direction of encrypted Lena image

Figure 5(e) Horizontal direction of the original Lena image Figure 5(f) Horizontal direction of the encrypted Lena image

Figure 5 Lena image neighboring element correlation.

to determine the degree of randomness of the encrypted image pixel points. If we obtain 15 test results greater than 1%, then the overall randomness of the cipher image pixel points is better, and the complexity is higher [25]. The results of the NIST test for the ciphertext of the image of lena are shown in Table 3. From the results in the table, all the chaotic encryption algorithms proposed in this paper have good results for image encryption.

Table 3 NIST tests

Subtest	P Value(>0.01)	Passing Rate (>=248/256)	PASS/NOT
Frequency	0.440897	256/256	PASS
Block frequency	0.795129	252/256	PASS
Cumulative Sums	0.426271	251/256	PASS
Runs	0.363284	254/256	PASS
Longest runs	0.213309	252/256	PASS
Rank	0.666245	251/256	PASS
FFT	0.518106	251/256	PASS
Nonoverlapping template	0.763673	250/256	PASS
Overlapping template	0.284026	253/256	PASS
Universal	0.816537	251/256	PASS
Approximate Entropy	0.794231	252/256	PASS
Random Excursions	0.021505	253/256	PASS
Random Excursions Variant'	0.096578	254/256	PASS
Serial 1	0.463781	253/256	PASS
Serial 2	0.083809	253/256	PASS
Linear Complexity	0.364387	254/256	PASS

6.2 Performance Comparison with Other Algorithms

To better verify the encryption effect of the algorithms in this paper, we chose two images of Lena, 256 × 256 and 512 × 512, as the comparison objects of the four algorithms.

(1) Statistical analysis comparison

Figure 6 shows the comparison results of the four algorithms for the 256 × 256 image of Lena, and Figure 6(a–d) shows the histograms of the four algorithm images. Figure 7 shows the comparison results of the four algorithms for the 512 × 512 image of Lena. Figure 7(a–d) shows the image histograms of the four algorithms. From the results in the figure, the histograms of ILogistic and IHenon show a more obvious wave trend, while the ILogistic-Tent algorithm, although compared to the previous two algorithms, is gentler, and the algorithm of this paper phase has an obviously more obvious effect.

(2) Encryption speed comparison

Table 4 shows the encryption speed comparison of the four algorithms. From the results of the data in the table, it is found that the algorithm in this paper has an advantage in encryption time compared to ILogistic, IHenon and

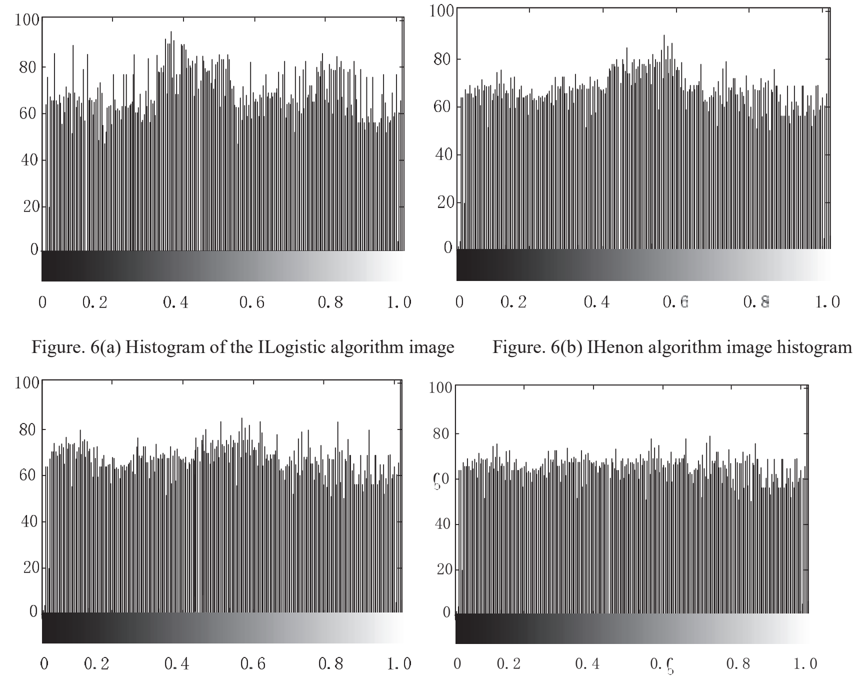

Figure. 6(a) Histogram of the ILogistic algorithm image Figure. 6(b) IHenon algorithm image histogram

Figure. 6(c) Histogram of the ILogistic-Tent algorithm image Figure. 6(d) Image histogram of this paper's algorithm

Figure 6 256 × 256 histogram of the four algorithms.

ILogistic-Tent because the image encryption algorithm proposed in this paper needs to go through the traversal of the image only once, which improves the speed of the operation, whereas the ILogistic encryption algorithm, although improved, still appears to have an encryption time that is slightly longer. The same situation also occurs in the case of the IHenon encryption algorithm. It is clear that these two single encryption algorithms do not have much advantage in time compared to ILogistic-Tent, although this paper's algorithm is the depth of the fusion of the two chaotic algorithms, but due to the lack of improvement, the algorithm's performance is not as good as this paper's algorithm.

(3) Pixel correlation analysis

Table 5 shows the pixel correlation comparison results of the four algorithms in Lena's 256 × 256 and 512 × 512 images. From the data in the table, this paper's algorithm has a more obvious advantage both in 256 × 256

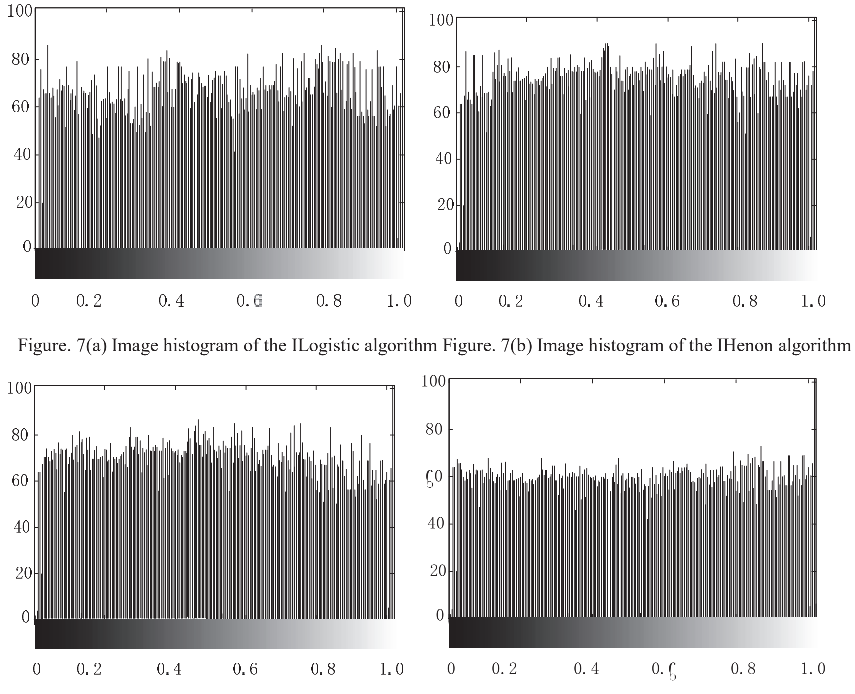

Figure. 7(a) Image histogram of the ILogistic algorithm Figure. 7(b) Image histogram of the IHenon algorithm

Figure. 7(c) Image histogram of the ILogistic-Tent algorithm Figure. 7(d) Image histogram of this paper's algorithm

Figure 7 512 × 512 histogram of the four algorithms.

Table 4 Comparison of encryption algorithm efficiency

	Encryption Time/S			
Image Size	ILogistic	IHenon	ILogistic-Tent	ILogistic-IHenon
256 × 256	0.0095	0.0089	0.0042	0.0023
512 × 512	0.1081	0.0096	0.0072	0.0048

and 512 × 512 conditions. In 256 × 256 conditions, this paper's algorithm improves 11.39%, 10.12% and 7.59% in the horizontal, vertical and diagonal directions, respectively, compared to ILogistic, and 9.41%, 8.23% and 2.35% in the horizontal, vertical and diagonal directions, respectively, compared to IHenon, compared to ILogistic-Tent improves 9.87%, 8.64% and 2.47% in the horizontal, vertical and diagonal directions, respectively. In the 512 × 512 condition, the algorithm in this paper improves 14.28%, 11.22% and 5.10% in the horizontal, vertical and diagonal directions, respectively, compared to the ILogistic algorithm, improves 18.56%, 16.49% and 10.31%

Table 5 Analysis of the four algorithms' relationships

Lena Image	Method	Horizontal	Vertical	Diagonal
256 × 256	ILogistic-IHenon	0.0079	0.0085	0.0081
	ILogistic	0.0088	0.0093	0.0089
	IHenon	0.0087	0.0092	0.0088
	ILogistic-Tent	0.0085	0.0087	0.0083
512 × 512	ILogistic-IHenon	0.0098	0.0097	0.0096
	ILogistic	0.0112	0.0115	0.0113
	IHenon	0.0109	0.0113	0.0109
	ILogistic-Tent	0.0103	0.0107	0.0105

in the horizontal, vertical and diagonal directions, respectively, compared to IHenon, and improves 10.31% in the horizontal, vertical and diagonal directions, respectively, compared to ILogistic-Tent by 17.71%, 13.54% and 9.37% in the horizontal, vertical and diagonal directions, respectively. The comparison of these two sets of data results shows that the algorithm in this paper has a better encryption effect in all three directions and generates ciphertext images with lower pixel correlation coefficients and better security.

(4) Information Entropy Analysis

The information entropy in a ciphertext image can measure whether the distribution of gray values in a ciphertext image is uniform or not. The larger the information entropy is, the more uniform its distribution is, and the higher the randomness of the pixel value is, the stronger the representative's ability to resist the entropy attack is. Each gray value consists of 8 bits of binary, so the ideal information entropy should be wirelessly close to 8. The results are shown in Table 6. From the data in the table, it is found that this paper's algorithm is close to 8 in terms of all three channels, which indicates that this paper's algorithm is able to adapt to different sizes of images and is able to obfuscate the image to a high degree and has the ability to resist the entropy attack.

(5) Differential Attack Analysis

Differential attack is an important means to test the sensitivity of encryption algorithms to plaintext, and we use two indexes, the relevant parameter number of pixel change rate (NPCR) and the overall average change density (UACI), to test the ability of the image encryption system to resist differential attack. The ideal value of the former is 99.6093%, and the ideal value of the latter is 33.4635%. The comparison results of the four algorithms for two

Table 6 Shows the comparison of the information entropy analysis of the four algorithms

Lena Image	Algorithm	R-channel	G-channel	B-channel
256 × 256	ILogistic-IHenon	7.9913	7.9916	7.9928
	ILogistic	7.9900	7.8997	7.8998
	IHenon	7.9901	7.9901	7.9914
	ILogistic-Tent	7.9908	7.9903	7.9905
512 × 512	ILogistic-IHenon	7.9938	7.9972	7.9976
	ILogistic	7.9902	7.9913	7.9908
	IHenon	7.9903	7.9915	7.9909
	ILogistic-Tent	7.9932	7.9935	7.9936

Table 7 Analysis of four algorithmic differential attacks

Lena Image	Algorithm	NPCR	UACI
256 × 256	ILogistic-IHenon	99.5821%	33.4617%
	ILogistic	99.5794%	33.4519%
	IHenon	99.5801%	33.4524%
	ILogistic-Tent	99.5803%	33.4601%
512 × 512	ILogistic-IHenon	99.5938%	33.4619%
	ILogistic	99.5819%	33.4559%
	IHenon	99.5833%	33.4563%
	ILogistic-Tent	99.5901%	33.4609%

images 256 × 256 and 512 × 512 are shown in Table 7. From the results in Table 6, it is found that compared to the other three algorithms, the image encryption algorithm proposed in this paper has better pixel sensitivity and more ideal resistance to differential attacks.

7 Conclusions

To further improve the performance of image encryption algorithms, this paper proposes an image encryption scheme based on the Fibonacci-ILogistic-IHenon image encryption scheme, which improves the security of image encryption through Fibonacci disruption and the use of the ILogistic-IHenon encryption model, and simulation experiments to verify that the scheme has obvious advantages over the improved chaotic encryption algorithms in the comparison of the encryption indexes. The simulation experiment verifies that this scheme and the improved chaotic encryption algorithm have obvious advantages in the comparison of encryption indexes. In the future, the direction of image encryption will focus on blockchain, deep learning, etc. In the next step, we will continue to consider how to deeply optimize the structure of the current chaotic model and reduce the time complexity.

References

[1] Porter T, Duff T. Compositing digital images[C]//Proceedings of the 11th annual conference on Computer graphics and interactive techniques. 1984: 253–259.

[2] Madhu B, Holi G, Murthy K S. An overview of image security techiques[J]. International Journal of Computer Applications, 2016, 154(6): 37-46.

[3] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map[J]. Image and vision computing, 2006, 24(9): 926–934.

[4] Wang X, Teng L, Qin X. A novel color image encryption algorithm based on chaos[J]. Signal Processing, 2012, 92(4): 1101–1108.

[5] X̧elik H, Doğan N. A hybrid color image encryption method based on extended logistic map[J]. Multimedia Tools and Applications, 2023: 1–24.

[6] Al-Hazaimeh O M. A new speech encryption algorithm based on dual shuffling Hénon chaotic map[J]. International Journal of Electrical and Computer Engineering, 2021, 11(3): 2203–2210.

[7] Luo H, Ge B. Image encryption based on Henon chaotic system with nonlinear term[J]. Multimedia Tools and Applications, 2019, 78: 34323–34352.

[8] Bakhshandeh A, Eslami Z. An authenticated image encryption scheme based on chaotic maps and memory cellular automata[J]. Optics and Lasers in Engineering, 2013, 51(6):665–673.

[9] Wang X, Liu C. A novel and effective image encryption algorithm based on chaos and DNA encoding[J]. Multimedia Tools and Applications, 2017, 76: 6229–6245.

[10] Ding L, Ding Q. The establishment and dynamic properties of a new 4D hyperchaotic system with its application and statistical tests in gray images[J]. Entropy, 2020, 22(3):310–328.

[11] Zhou H L, Liu H Q. Fast Chaotic Image Encryption Algorithm Combined with DNA Encoding[J]. Journal of Northeastern University (Natural Science), 2021, 42(10): 1391–1399.

[12] Wang Q, Yu S, Li C, et al. Theoretical Design and FPGA-Based Implementation of Higher-Dimensional Digital Chaotic Systems[J]. Circuits

and Systems I: Regular Papers, IEEE Transactions on, 2016, 63(3): 1–12.

[13] Pak C, Kim J, Pang R, et al. A new color image encryption using 2D improved logistic coupling map[J]. Multimedia Tools and Applications, 2021, 80: 25367–25387.

[14] Lai Q, Hu G, Erkan U, et al. High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map[J]. Applied Mathematics and Computation, 2023, 442: 127738.

[15] Khan H, Hazzazi M M, Jamal S S, et al. New color image encryption technique based on three-dimensional logistic map and Gray wolf optimization based generated substitution boxes[J]. Multimedia Tools and Applications, 2023, 82(5): 6943–6964.

[16] Luo Y, Yu J, Lai W, et al. A novel chaotic image encryption algorithm based on improved baker map and logistic map[J]. Multimedia Tools and Applications, 2019, 78: 22023–22043.

[17] Zhou Y C, Bao L, Chen C L. A new 1D chaotic system for image encryption [J]. Signal Processing, 2014, 97: 172–182.

[18] Shao S, Li J, Shao P, et al. Chaotic Image Encryption Using Piecewise-Logistic-Sine Map[J]. IEEE Access, 2023, 11: 27477–27488.

[19] Hua Z, Zhu Z, Yi S, et al. Cross-plane color image encryption using a two-dimensional logistic tent modular map[J]. Information Sciences, 2021, 546: 1063–1083.

[20] Wang X, Guan N. A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation[J]. Optics&Laser Technology, 2020, 131: 106366.

[21] Basha S M, Mathivanan P, Ganesh A B. Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map[J]. Optik, 2022, 259: 168956.

[22] Akraam M, Rashid T, Zafar S. An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers[J]. Multimedia Tools and Applications, 2023, 82(11): 16861–16879.

[23] Adhikari S, Karforma S. An Efficient Image Encryption Method Using Henon-Logistic-Tent Chaotic Pseudo Random Number Sequence[J]. Wireless Personal Communications, 2023, 129(4): 2843–2859.

[24] Ding Y, Duan Z, Li S. 2D arcsine and sine combined logistic map for image encryption[J]. The Visual Computer, 2023, 39(4): 1517–1532.

[25] Rukhin A, Soto J, Nechvatal J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[J]. NIST Special Publication 800-22, Gaithersburg, MD, US, 2001, 800: 163.

Biographies

Yong Yang received her bachelor's degree in Inorganic nonmetallic materials from Chengdu University of Technology in 2001 and his master's degree in computer science and technology from Hangzhou Dianzi University in 2009. He is currently an associate professor of Zhejiang Industry Polytechnic College, and his research interests are edge cloud computing, wireless sensing, image encryption.

Xuan Chen received her bachelor's degree in Information Management and Information Systems from Zhengzhou University of Aeronauticsin in 2013 and a Master's degree in software engineering from University of Electronic Science and Technology of China in 2016. He is an associate professor at Zhejiang Industry Polytechnic College. His research interests include cloud computing, image encryption and algorithm design.

Jiaying Xu received her bachelor's degree in Visual Communication Design from Hubei Academy of Fine Arts in 2015 and a Master's degree in Visual Communication Design from Hubei Academy of Fine Arts in 2018. She is currently a teacher at the School of Design and Art at Zhejiang Industry Polytechnic College, and her research interests in graphic comprehensive project design, illustration design, packaging design.

Yuxia Li received her bachelor's degree in Physics from Inner Mongolia Normal University in 1994 and a Master's degree in Computer Technology and Applications from Beijing Institute of Technology in 2003. She is currently an associate professor in Beijing United University, and her research interests are computer algorithms, big data, and cloud computing.