Research Article

An Image Encryption Algorithm Based on the Improved Sine-Tent Map

Zijing Gao,¹ Zeyu Liu ,¹ and Lichan Wang²

¹College of Science, Northwest A&F University, Yangling 712100, China

²Department of Foreign Languages, Northwest A&F University, Yangling 712100, China

Correspondence should be addressed to Zeyu Liu; liuzeyu_90@163.com

Received 15 May 2021; Accepted 11 September 2021; Published 13 October 2021

Academic Editor: Piergiulio Tempesta

Copyright © 2021 Zijing Gao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper makes use of the characteristics of initial sensitivity and randomness of the chaotic map to design an image encryption algorithm based on the sine map and the tent map. The sine map is used to improve the tent map; then, the improved sine-tent map is proposed. The traditional tent map proposed in this paper has an expanded control parameter range and better chaos. In this algorithm, bit rearrangement is adopted to further improve the improved sine-tent map, which can reconstruct the output value and expand the chaotic characteristics of the map. In this algorithm, the image parameters are connected with the algorithm to generate the key. In the encryption step, a method of replacing the most significant bit and scrambling-diffusion algorithm is designed to encrypt the plaintext image. Finally, the algorithm is simulated with the experiment and evaluated with analysis; then, the experimental results are given. The evaluation results show that the ciphertext of the algorithm has high randomness, strong robustness, and better resistance to differential attacks after comparison. The correlation of the ciphertext image pixels is very low, and the algorithm is highly secure as a conclusion.

1. Introduction

An algorithm for image encryption is proposed in this paper. As is all known, image is one of the most widespread forms of multimedia, and it plays a really important role in people's lives. It also has an extensive application requirement in all walks of life. In people's daily lives, images can easily reveal personal privacy, and images have high confidentiality requirements in some special fields, so it is very important to encrypt images. Today, most images are stored and displayed in the form of digital images, so the encryption method of digital images has also been extensively studied in secure communication [1–6].

Digital images are stored in a matrix. Essentially, they are a group of two-dimensional sequences. Encrypting digital images is hiding the information carried in these two-dimensional sequences, so that the attackers cannot read it. However, the image encryption algorithm is different from the traditional encryption algorithm, because image encryption needs to meet high computation

efficiency and avoid information loss at the same time. Due to the inherent characteristics of the image, such as high redundancy, large amount of data, strong correlation between adjacent pixels, and real-time transmission, some classic algorithms such as the RSA algorithm will be computationally expensive when encrypting the image. They are difficult to perform image encryption work [7]. In this paper, the algorithm is designed by chaotic systems, and the evaluation results show that it can perfectly solve these problems.

Chaos refers to the determinism that appears in non-linear dynamic systems, similar to random processes. These processes are neither periodic nor convergent and have an extremely sensitive dependence on initial values. In daily life, chaos always appears in casual places. Since R. Matthews proposed an encryption algorithm by chaos in 1989 [8], these encryption algorithms have gradually come into people's field of vision nowadays. In cryptography, the randomness and initial sensitivity of chaotic maps are mainly used. Nowadays, it shines in the field of information

security, and encryption algorithms based on the chaotic map are also constantly being proposed.

Literature [9] proposed a bit embedding based on the chaotic tent map as a novel multicore implementation of the steganography algorithm. Literature [10] used the obfuscation phase to scramble the pixel position; the diffusion phase to continuously change the pixel content; the introduction of Arnold's cat map to perform the obfuscation operation; and a reasonable combination of the sine map, logistic map, and the tent map to realize the principle of diffusion. In addition, exclusive OR (XOR), exchange, and transformation operations are used to improve the efficiency of the diffusion stage. Literature [11] proposed a cellular automaton based on the tent map, which uses different key streams to encrypt a single block. In the subsequent steps, the bytes of the encrypted block thus obtained are further shuffled to make the scheme more distributed. Literature [12] proposed a two-dimensional chaotic system structure based on the sine transformation based on the good non-linear performance of the sine function, which can generate a variety of chaotic systems. When a digital chaotic system is implemented on hardware with limited computational precision, it will lead to short-period orbits. Although many existing image encryption algorithms state that the average period length of their digital chaotic system is greater than the period length required for image encryption, there are still many periodic tracks whose length is much smaller than the average period length. Literature [13] designed an improved cryptosystem based on a 2D-SCL map. It combined the confusion and diffusion process in one stage to increase the speed of operation. Based on the SHA-1 hash value and chaotic sequence of the plane graph, a pseudorandom sequence is designed, and an antidegradation method is introduced to resist the dynamic degradation of the 2D-SCL graph under limited calculation accuracy. Banu et al. [14] studied an encryption algorithm based on integer wavelet transform (IWT) combined with deoxyribonucleic acid (DNA) and chaos to secure digital medical images. The proposed work will be composed of two phases: a two-stage shuffling phase and a diffusion phase. The first step of shuffling starts with initial block confusion followed by the column and row shuffling of pixels as the second stage. Consequently, the algorithm security is greatly increased.

The contributions of this paper are summarized as follows: (i) this paper proposed and improved a chaotic map based on the sine map and the tent map, called the improved sine-tent map. For the traditional tent map, the improved sine-tent map proposed in this paper has an expanded control parameter range. (ii) It designed a bit rearrangement method to improve chaotic system behavior and good properties. (iii) It designed a scrambling-diffusion algorithm, which is suitable for image encryption. The remaining parts of this paper are organized as follows. In Section 2, the prerequisite knowledge will be introduced, and the improved sine-tent map will also be proposed. Then, there is a method designed to improve the improved sine-tent map. In Section 3, the specific steps of encryption are designed for the algorithm and we implement them to realize the encryption of the image and prove the feasibility of the

technology. Then, Section 4 mainly describes how to put forward the decryption algorithm based on the encryption algorithm. We will verify the technology through experimental simulation, effectiveness, and practicality by calculating a series of indices in Section 5. The remaining section is the conclusion.

2. Preliminaries and Proposal of an Improved Chaotic Map

2.1. Lyapunov Index. Chaotic systems have many basic characteristics, which are mainly manifested as non-periodic, randomness, and extreme sensitivity of the system to initial values. The sensitivity of the initial value is mainly manifested as the trajectory produced by the change of two initial values with little difference over time, which is gradually separated exponentially with the passage of control parameters. Among them, the Lyapunov exponent is the parameter used to describe this phenomenon [15]. In other words, it can judge whether the system is chaotic. The important parameters for judging the stability of a system can be visually observed by judging the Lyapunov exponent. Its principle is to measure the state of a system by measuring the rate of convergence or separation of adjacent trajectories, which are expressed as the average rate of divergence or convergence of adjacent trajectories in phase space. The lower the exponent is, the more stable the system is. If the control parameter is at a certain point, the exponent is positive. If the system is chaotic, no matter how small the initial distance between the two trajectories is, the difference will increase exponentially over time to the point of being unpredictable and forming a chaotic phenomenon.

The calculation methods of Lyapunov exponents are usually divided into two categories. One is the solution method based on the differential equation, and the other is the calculation method based on the motion trajectory. It has two important parameters: the embedding dimension m and time lag T . Since there are m spatial dimensions, there are m Lyapunov exponents [16, 17]. The largest exponent can determine the magnitude of local stability. When studying dynamic systems in this paper, bifurcation graphs and Lyapunov exponents will be studied at the same time to analyze the chaotic phenomena of the system. The formula for calculating the Lyapunov exponent is

$$\lambda = \lim_{n \rightarrow \infty} \sum_{k=0}^{n-1} \log \left| \frac{dS}{dx} \right|_{x_k}. \quad (1)$$

Among them, S is a chaotic map. In this paper, the Jacobi matrix method is used to calculate the improved sine-tent map with

$$\begin{cases} x_{n+1} = g_1(x_n, y_n), \\ y_{n+1} = g_2(x_n, y_n). \end{cases} \quad (2)$$

Its Jacobi matrix is

$$J = \begin{bmatrix} \frac{\partial g_1}{\partial x_n} & \frac{\partial g_1}{\partial y_n} \\ \frac{\partial g_2}{\partial x_n} & \frac{\partial g_2}{\partial y_n} \end{bmatrix}. \quad (3)$$

And then, there are initial values x_0 and y_0 , and the small difference is ∂x_0 and ∂y_0 . After n iterations, it can create $(x_0, y_0), (x_1, y_1), \dots, (x_n, y_n)$. Then, these n Jacobi matrices are expressed as

$$J_n = J(x_n, y_n). \quad (4)$$

Making QR decomposition of these matrices, get $J_n, J_{n-1}, \dots, J_1$. Each entry on the diagonal of R is the product of all entries on the diagonal of R_i . In other words, the approximate value of the Lyapunov exponent can be obtained by the following formula:

$$\lambda_k = \frac{1}{n} \sum_{i=1}^n \ln |R_i(k \cdot k)|, \quad k = 1, 2. \quad (5)$$

2.2. The Sine Map. The sine map is a classic chaotic map derived from the sine function. It converts the input angle into a certain angle and then outputs it. Sine map's mathematical expression is defined as

$$x_{n+1} = S(x) = a \sin(\pi x). \quad (6)$$

In formula (6), the map is expressed as (x) , and a is the control parameter. Its bifurcation graph and Lyapunov exponent graph are shown in Figure 1.

2.3. The Tent Map. The tent map is a segmented linear map which is widely used in image encryption systems. The tent map appears as a chaotic map within the value range of the control parameters, which has a uniform distribution function and a good correlation. The mathematical model of the tent map is defined as follows:

$$x_{n+1} = S(x) = \begin{cases} \frac{x_n}{a}, & x_n = [0, a), \\ \frac{(1-x_n)}{(1-a)}, & x_n = [a, 1]. \end{cases} \quad (7)$$

The tent map's expression can be transformed into the following formula:

$$x_{n+1} = a - (1+a)|x_n|, \quad a = [0, 1], x_n = [-1, 1]. \quad (8)$$

Among them, (x) is the map, a is the control parameter, and the value range of a is $0 < a < 1$. When $a = 0.5$, the system presents a short-period state. And the initial value cannot be equal to the control parameter; otherwise, let the system present a periodic state [18]. Its bifurcation diagram and Lyapunov exponent plot are shown in Figure 2.

2.4. The Improved Sine-Tent Map. Through the study of the tent map and the sine map, this paper found that the tent map only produces chaos within the parameter value range, and the control parameter a only has a value range of $0 < a < 1$, so this paper uses the sine map to perform the tent map. We use the sine map to replace x on the right side of the equation in the tent map to get the following formula:

$$x_{n+1} = a - (1+a)|\sin(\pi x_n)|. \quad (9)$$

As shown in Figure 3, analyzing its dynamic behavior, it is obvious that the map has a large range of chaos, and it can be seen that when the bifurcation phenomenon occurs, the Lyapunov exponent is at the same time. If it is positive, it indicates that the system is indeed chaotic. From the above analysis, it can be known that the map can be used for image encryption, but as can be seen in Figure 3, the map sometimes does not appear chaotic. Therefore, the map needs to be improved.

Adjust the map slightly, and multiply π by the map:

$$y_{n+1} = b - (-1)^n (1+b)x_n. \quad (10)$$

The improved sine-tent map is as follows:

$$\begin{cases} x_{n+1} = a - (1+a)|\sin y_n|, \\ y_{n+1} = \pi(b - (-1)^n (1+b)x_n). \end{cases} \quad (11)$$

In this formula, a, b are the control parameters. Compared with the original map, the control parameter b and the initial value y_0 are added, which effectively expands the key space. The following gives the control parameter $-2 < a < 2$, $b = 3.21$, its bifurcation graph, and Lyapunov exponent graph.

As we can see from Figure 4, only when the value of a is around -1 , the mapped system is relatively stable and does not appear chaotic, compared to the previous map. The value ranges of the control parameter a is further expanded.

Then, we will operate on bits in order to further improve the improved sine-tent map. Bit rearrangement has the advantage of being able to improve the chaos of the system and make unpredictable changes to the chaotic value of the output. When there are two points with small differences in the chaotic system, rearranging their bits will make the difference between the two updated points after the rearrangement become more random. After this operation, the rearranged chaotic system has better sensitivity chaotic characteristics, such as dependence and ergodicity, and enhanced chaotic characteristics of chaotic systems.

The bit rearrangement method used in this article is to take out the decimals separately. The specific operation steps are as follows: firstly, we convert the decimals into hexadecimal, then scramble each bit of it, and restore it to decimal at last. The operational diagram is as follows.

The bit rearrangement used in this article is to convert decimals into 16-bit binary. In the next steps, we will insert the first eight digits into odd digits back to front and insert the last eight digits into even digits from back to forward. Finally, it will be converted into decimal decimals. As shown in Figure 5, 0.4321 is converted to binary, and after bit

FIGURE 1: Dynamic behavior of the sine map: bifurcation diagram (a) and Lyapunov exponent graph (b) of the sine map.

FIGURE 2: Dynamic behavior of the tent map: bifurcation diagram (a) and Lyapunov exponent graph (b) of the tent map.

FIGURE 3: Dynamic behavior of the map: bifurcation diagram (a) and Lyapunov exponent graph (b).

FIGURE 4: Dynamic behavior of the improved sine-tent map: bifurcation diagram (a) and Lyapunov exponent graph (b) of the improved sine-tent map.

FIGURE 5: Schematic diagram of bit rearrangement.

rearrangement, it becomes 0.2477. Bit rearrangement of the improved sine-tent map makes it show better chaos. The dynamic behavior is shown in Figure 6.

3. Encryption Method

The algorithm designed in this paper uses XOR of high-order bits, scrambling, and diffusion to realize image encryption. The specific steps are as follows: we will input a plaintext image I_{MN} with a size of $M \times N$ pixels, record the pixel value of row i and column j as $I_{i,j}$, extract the average number of plaintext images $\bar{x}$, and process to get x_0 as the key. The control parameters a, b and the initial value of y_0 are also the keys. x_0, y_0 will be taken as the initial value of the iteration, $y_0 = 0.01$, the control parameters value for $a = 1.12345, b = 3.21$, substituted into the improved sine-tent map. Firstly, we will iterate M times to make the chaotic system skip the chaotic transition state and then output a sequence of length $M \times N$, denoted as e_0 . Because it is in chaos, we can know that each element in e_0 is different. There are formulas for processing e_0 to get three sets of sequences:

$$\begin{aligned} e_1 &= \text{round}[(e_0 + 1) * 1000] \bmod 2, \\ e_2 &= \text{round}[(e_0 + 1) * 1000] * (M - 1) \bmod M, \\ e_3 &= \text{round}[(e_0 + 1) * 1000] * 255 \bmod 256. \end{aligned} \quad (12)$$

Sequence e_0 and sequence e_2 will be used for the scrambling algorithm, sequence e_1 will be used for high-

order bit masking, and sequence e_3 will be used for the diffusion algorithm.

3.1. Shielding of High Bit. Bit is the smallest storage unit in the computer. It usually stores as 0 or 1. The experimental image used in this article is a grayscale image. The 8-bit grayscale is used when converted to decimal. The pixel value is between 0 and 255, and the larger the pixel value, the darker the color when represented in the image. In other words, when the pixel value is 0, it is shown as pure black, and when the pixel value is 255, it is shown as pure white.

Many information hiding algorithms are also implemented based on bit manipulation, such as the LSB algorithm. The LSB algorithm is a relatively classic information hiding technology, which realizes information hiding by hiding information in the lowest bits of the image [19]. It is based on the principle that the lower the image bit is, the less the impact on the image information after the bit is changed. Therefore, after the ciphertext information is embedded in the lowest bit of the carrier image, although the pixel value has changed, the impact of the carrier image is minimal. It shows that the higher the effective bit changes, the greater the impact of the change on the image information in an image is. So, we will operate on the high-order bits of the plaintext image pixels based on this. This method can effectively change the pixel value of the image according to the chaotic sequence, so the algorithm can also encrypt the solid color image well.

FIGURE 6: Dynamic behavior of the improved sine-tent map after further improvement: bifurcation diagram (a) and Lyapunov exponent graph (b).

In this paper, the plaintext image is converted into an 8-bit binary array, and the highest bit and the second-highest bit are XORed with e_1 to shield the high bit and hide the plaintext information. This method can make every pixel value of the plaintext image change unpredictably, which is a preprocessing of the pixel value.

3.2. Scrambling Algorithm. Scrambling refers to scramble the information order of the image to transform it into a chaotic image where information cannot be read. If we use the scrambling method to hide the information, the scrambled image is scrambled only at the pixel position, so the value of the pixel has not changed. Generally speaking, after the image scrambling, the result is an image with disordered pixel order. Even if the ciphertext image is obtained, no information can be obtained, which can effectively resist the attack. This technique can greatly improve the robustness of the encryption system [20–22].

3.2.1. Random Emission of Pixels. The way to implement the algorithm in this paper is as follows: at first, the plaintext image I is transformed into a set of one-dimensional sequence I' . e_0 will be sorted in ascending order to generate e'_0 . When e_0 is sorting, the plaintext image I' sorts synchronously. Since e_0 is a chaotic sequence without the same number, there will be no repetition and it is difficult to crack. However, because the amount of pixels is too large, if this scrambling method is used, it will cause too much calculation. So, we have to reduce the calculation efficiency and reduce the time cost. Therefore, e_0 is transformed into a two-dimensional number sequence of $M \times N$, denoting it as e''_0 . The M column of e''_0 is denoted as e_{0M} , the N row of e''_0 is denoted as e_{0N} . e_{0M}, e_{0N} are arranged in ascending order and scrambled to get the image E ; the sorted scrambling index of e_0 is recorded to form a two-dimensional array, denoted as D .

3.2.2. Cyclic Shift. This method is also a scrambling algorithm. Random horizontal displacement is performed on each row of pixels to achieve the scrambling effect. The processed e_1 sequence is a sequence of positive integers with a value range of $0 - M$. The i row of the scrambling matrix is denoted as $E(i)$, and the i position of e_1 is denoted as $e_1(i)$; shift the pixel in row i of the scrambled image E by $e_1(i)$ to the left to get the scrambled image E' . The schematic diagram is shown in Figure 7.

3.3. Diffusion Algorithm. Diffusion algorithm is a processing method that allows data and data to interact with each other. The purpose is to make the elements interact with each other through diffusion processing, causing an avalanche effect. When small changes are made to different data or input values, there will be huge differences in the output results finally.

Diffusion algorithms have many characteristics, such as rich diffusion establishment methods, natural parallel computing support, abundant diffusion calculation, and elementary organization methods [23]. When the diffusion algorithm is used in image encryption, the diffusion rate needs to reach 100%. The diffusion algorithm with a perfect diffusion rate can better encrypt the image. Parallel computing can also greatly improve computing efficiency, so it has good computing performance. The diffusion algorithm hides the pixel value without changing the pixel position.

This paper adopts the addition and subtraction operation for diffusion encryption. The diffusion algorithm used in this paper is as follows:

$$\begin{aligned} E''(n) &= E''(n-1) + E'(n)^2 + e_2 \bmod 256, \\ E''(n) &= E''(n+1) + E'(n)^2 + e_2 \bmod 256. \end{aligned} \quad (13)$$

Firstly, the scrambled image E' will be converted into a one-dimensional number sequence, and the data type has to

FIGURE 7: Schematic diagram of cyclic shift operation.

be converted to a floating-point type. And then spread backward and forward twice, where $E''(n)$ is the n th ciphertext image after diffusion pixels, $E'(n)$ is the pixel of the n th scrambled image sequence, and e_2 is the chaotic sequence after processing. At last, we will output E'' , convert it into a two-dimensional sequence of $M \times N$, convert its data type to uint 8, and output the ciphertext image C , completing the encryption.

3.4. Decryption Algorithm and Result. The algorithm is written and implemented based on MATLAB. The images of 512×512 pixels are encrypted as plaintext images. The plaintext image I and the encrypted output ciphertext image C are shown in Figure 8.

The encrypted ciphertext image cannot read any information.

When the pure white and pure black images are encrypted, the results are shown in Figure 9.

The results show that the algorithm can also encrypt solid color images.

4. Decryption Method

In terms of the design of the decryption algorithm, actually we do the inverse process of the above steps. The following is the specific operation process of decryption:

- (1) Perform diffusion algorithm decryption, once for the forward diffusion and once for the reverse diffusion. The step of diffusion is opposite to that of encryption. The formula used in this step of the decryption algorithm is as follows:

$$\begin{aligned} E'(n) &= \sqrt{256 * 2 + C(n) - C(n-1) - e_2} \bmod 256, \\ E'(n) &= \sqrt{256 * 2 + C(n) - C(n+1) - e_2} \bmod 256, \end{aligned} \quad (14)$$

where E' is the image after diffusion and decryption, C is the ciphertext image, and e_2 is a sequence value for 1–255, generated by e_0 . The ciphertext image C and e_2 will be inversely diffused based on the above two formulas twice to get the decrypted image C' .

- (2) The cyclic shift encryption algorithm decrypts the ciphertext image C' . Since the image is cyclically shifted to the left according to the sequence e_1 during encryption, in decryption, the ciphertext image C' is cyclically shifted to the right to obtain the ciphertext image C'' .

- (3) These pixels will be restored. When performing image pixel scrambling, we can record the index D . D is a two-dimensional sequence from 1 to $M \times N$. When it is scrambling, D and the plaintext image synchronously scramble, so that the plaintext image can be scrambled and the index of the pixel change is recorded. The index D can restore the image. We will sort D from small to large, and perform the same operation on C'' to restore the pixels of the ciphertext image C'' to the position of the plaintext image.
- (4) Bit restoration. There is a XOR operation on the highest and second-highest bits with e_1 to restore them. And finally, we restore the restored image to a decimal two-dimensional array of $M \times N$ and convert it to the uint 8 type. The decrypted image has been obtained.

The decryption result is shown in Figure 10.

5. Analysis of the Algorithm

5.1. Key Space Analysis. The keys for this article are x_0, y_0, a, b . x_0, y_0 are the initial values of the iteration, x_0 is related to the plaintext image. They are used with the parameters a, b to control the generation of the chaotic sequence e_0 and the sequence e_1, e_2, e_3 . The control parameter range of the two-dimensional improved sine-tent map is not limited to $[0 \sim 1]$. Experimenting $x_0 = 0.12345678901234567$, $y_0 = 0.1234567890123456$, $a = 1.1234567890123456$, $b = 0.123456789012345678$, at this time, when the last decimal place changes, the decryption still fails. We can easily know that the key space of this algorithm is $10^{17} \times 10^{16} \times 10^{16} \times 10^{18} = 10^{66}$, which is very large. Table 1 shows the comparing results with other documents.

5.2. Key Sensitivity Analysis. In an encryption algorithm, the key sensitivity is an important index to measure the security of the encryption system. After the ciphertext image and encryption algorithm are obtained, though the key has undergone very slight changes, it still cannot be decrypted correctly. Security is relatively high. The following is to test the key sensitivity.

Setting the control parameter $a = 1.234567890123451$, we substitute it into the algorithm for testing before decryption. The experimental results of the test are as follows.

As shown in Figure 11, it can be seen that when the 16 digits after the decimal point of the parameter are changed, it still cannot be decrypted correctly. So, the key sensitivity of this algorithm achieves the expected effect.

5.3. Classic Attack Analysis. When cracking and analyzing a cryptographic system, it is generally believed that the design and working information of the cryptographic system can be obtained. There are four classic attack methods [24]:

- (1) In a pure ciphertext attack: the attacker only has ciphertext information

(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 8: Continued.

FIGURE 8: Comparison of the original images ((a), (c), (e), (g), and (i)) before encryption and the images ((b), (d), (f), (h), and (j)) after encryption.

FIGURE 9: Ciphertext image of the pure white image (a) and ciphertext image of the pure black image (b).

(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 10: Continued.

FIGURE 10: Comparison of ciphertext images ((a), (c), (e), (g), and (i)) and correctly decrypted images ((b), (d), (f), (h), and (j)).

TABLE 1: Comparison of the key space with other documents.

Algorithm	Key space
Lina	10^{66}
[8]	10^{64}
[9]	10^{34}
[24]	10^{60}
[25]	10^{42}

- (2) Attacks with known plaintext: the attacker possesses plaintext and its corresponding ciphertext information
- (3) Select plaintext attack: the attacker can construct a part of the ciphertext attack based on the plaintext
- (4) Select ciphertext attack: the attacker can construct the corresponding plaintext based on the ciphertext

It can be seen that the selected plaintext attack is the most difficult attack to defend. Therefore, if an encryption system is constructed to completely resist the selected plaintext attack, we can say that this algorithm can resist all the above attacks. In the encryption algorithm

constructed in this paper, the modular arithmetic diffusion algorithm uses a combination of scrambled image information and a key to encrypt. The scrambled images produced by different plaintext images are different, and the key stream they generate in the modular arithmetic diffusion algorithm is also different. It can resist selected plaintext attacks; that is, it can resist all the aforementioned attacks.

5.4. Antidifferential Attack. The important indicators for evaluating the resistance of an image encryption algorithm to differential attacks are as follows: image pixel change rate (Number of Changing Pixel Rate, NPCR) and normalized average intensity change (Unified Averaged Changed Intensity, UACI) [26]. Among them, the image pixel change rate is an indicator to judge the distortion of the image after decryption, and the normalized average intensity change is an indicator to evaluate the severity of the change in the entire ciphertext image after the pixel changes. The calculation method of image pixel change rate is shown in the following equation:

FIGURE 11: Comparison of correctly decrypted images (a) and incorrectly decrypted images (b).

$$P_{\text{NPCR}} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\%,$$

$$D(i, j) = \begin{cases} 1, & C_1(i, j) \neq C_2(i, j), \\ 0, & C_1(i, j) = C_2(i, j). \end{cases} \quad (15)$$

The calculation method of normalized average intensity change is as follows:

$$P_{\text{UACI}} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{C_1(i, j) - C_2(i, j)}{255} \times 100\%. \quad (16)$$

The image is a grayscale image of pixels $M \times N$, C_1 is the ciphertext image gained by encrypting the image, C_2 is the image encrypted by changing the pixel value of a certain point in the original image. This article will focus on the central pixel of the plaintext image (add 1 to the value of $I(256, 256)$) to test. After calculating $P_{\text{NPCR}} = 99.5979\%$, $P_{\text{UACI}} = 33.3695\%$. Their ideal values are, respectively, 99.6094% and 33.4635%. It can be seen that, in the image, when a very small change occurs at a pixel value, there is a huge change. The above data show that the algorithm can well defend against differential attacks. There is a comparison with other documents in Table 2.

5.5. Histogram Analysis. It can be known that when the number of pixels at each gray level is closer, the histogram is more stable. It indicates that each pixel value tends to be the same, which indicates higher security. The histogram analysis result is as follows.

Figure 12 shows that the uneven pixel distribution becomes relatively smooth and even pixel distribution after encryption, which proves that the algorithm is more secure.

5.6. Correlation Analysis of Adjacent Pixels. The correlation of adjacent pixels is expressed as the degree of correlation between pixels. Normally, the pixels of a plaintext image

TABLE 2: NPCR and UACI and other literature comparison.

Figure or algorithm	NPCR (%)	UACI (%)
Lina	99.5979	33.3695
AirplaneGray	99.5956	33.4827
Peppers	99.5945	33.4666
Milkdrop	99.6082	33.5004
Baboon	99.6113	33.4692
[8]	99.6567	33.5543
[9]	99.62	33.39
[27]	99.5893	33.3730

are strongly correlated with its neighboring pixels. An ideal encryption algorithm can cut down the correlation of the pixels of the image as much as possible and try to be zero correlation [25, 28]. The lower the correlation is, the less likely it is to carry effective information. The following text will use simulation experiments on the pixels of the encrypted image. For the correlation coefficient calculation in three directions, the calculation formula is

$$\sigma_{xy} = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \sum_{i=1}^n (y_i - \bar{y})^2}}, \quad (17)$$

where y_i is the value of the next pixel in a certain direction of x_i , $\bar{x}$ is the average of all the points that can be taken by the previous pixel, and $\bar{y}$ is the average of all the points that can be taken by the next pixel value. For example, when calculating the correlation between the horizontally adjacent pixels, $x_i = C(i, j)$, $y_i = C(i, j + 1)$, where C is the ciphertext image and i and j are the value ranges of $1 < i < N$, $1 < j < M - 1$.

Table 3 shows the comparison between the pixel correlation coefficient of plaintext image and ciphertext image in three directions.

The scatter plot of the correlation between the plaintext image and the ciphertext image of a selected row is shown in Figures 13 and 14.

FIGURE 12: Pixel histogram of original image Lina (a) and encrypted image (b).

TABLE 3: Correlation coefficients of plaintext image and ciphertext image pixels in three directions and comparison with other papers.

Figure or algorithm	Horizontal direction	Vertical direction	Diagonal direction
Plaintext Lina	0.9896	0.9797	0.9683
Ciphertext Lina	0.0012	-0.00004	-0.0004
Ciphertext AirplaneGray	-0.00044	-0.0011	-0.0041
Ciphertext Peppers	0.0031	0.0014	-0.0035
Ciphertext Milkdrop	-0.00097	0.00078	-0.0012
Ciphertext Baboon	0.00097	0.00078	-0.0012
[8]	0.0241	0.0222	0.0169
[20]	0.0064	0.0001	-0.0029
[25]	-0.0304	-0.0056	0.0058
[29]	-0.0003	0.0011	0.0013
[27]	0.0003	-0.0011	-0.0010

FIGURE 13: The horizontal (a), vertical (b), and diagonal (c) pixel correlation scatter plots of the original image Lina.

5.7. Information Entropy Analysis. Entropy is an important indicator used to describe the complexity of things, and the randomness of information is usually used to measure by information entropy. Generally, we use information entropy to measure the randomness of text or image information. In the criteria for judging the randomness of image encryption algorithms, the ideal grayscale ciphertext image information entropy should be equal to 8. That is to say, in the algorithm of this article, the closer to 8 the information entropy is, the

better the ciphertext image randomness is [30, 31]. The calculation method of information entropy used in this paper is as follows:

$$H(S) = - \sum_{i=0}^n P(S_i) \log_2 P(S_i), \quad (18)$$

where (S_i) is the probability of a certain pixel and S_i is the value of the pixel. The calculation result is $(S) = 7.9993$,

FIGURE 14: The horizontal (a), vertical (b), and diagonal (c) pixel correlation scatter plots of the ciphertext image.

TABLE 4: Comparison of information entropy.

Figure or algorithm	Information entropy
Lina	7.9993
AirplaneGray	7.9993
Peppers	7.9993
Milkdrop	7.9993
Baboon	7.9993
[8]	7.9993
[20]	7.9971
[25]	7.9867
[27]	7.9025
[32]	7.9500

TABLE 5: Comparison of information entropy.

Figure or algorithm	Time (s)
Lina	0.1035
AirplaneGray	0.0979
[8]	0.0259
[20]	0.0501
[27]	0.0300

which proves that the randomness of the algorithm after encryption is close to the ideal state. Table 4 shows the comparison of information entropy.

5.8. Time Analysis. Encryption speed is also an important index to measure the encryption algorithm. Table 5 shows the comparison between the encryption time required by the algorithm in this paper and the literature.

5.9. Randomness Test. In order to test the randomness of ciphertext image pixels, the test is carried out based on NIST-SP-800-22 standard [33].

For a sample size equaling 10 binary sequences, the minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately equaling 8. The minimum pass rate for the random excursion (variant) test is approximately equaling 0 for a sample size equaling 1 binary sequences. Fifteen test results are shown in Table 6.

TABLE 6: Result of NIST-SP-800-22 test.

The test item	<i>P</i> value
Frequency	0.911413
BlockFrequency	0.739918
CumulativeSums	0.534146
Runs	0.350485
LongestRun	0.911413
Rank	0.035174
FFT	0.122325
NonOverlappingTemplate	0.911413
OverlappingTemplate	0.534146
Universal	0
ApproximateEntropy	0.739918
RandomExcursions	—
RandomExcursionsVariant	—
LinearComplexity	0.122325
Serial	0.534146

The randomness of ciphertext images passed the test.

6. Conclusions

This paper introduces an image encryption algorithm designed around the improved sine-tent map based on the tent map and the sine map. The algorithm skips the chaotic transition state through the improved sine-tent map and iterates out a set of chaotic sequences. This paper uses scrambling and diffusion to encrypt the plaintext image based on the sequence, and the decryption of the image is the inverse steps of the encryption. Finally, the algorithm is performed on the histogram, key space, key sensitivity, anti-differential attack, anticlaccal attack, pixel correlation coefficient, information entropy, and so on.

The evaluation result shows that, for today's computers, the key space of this algorithm is large enough, the key space of this algorithm is large enough, the antiattack ability is strong, and the robustness is strong. The diffusion algorithm makes use of the pixels in the scrambled image to perform mutual diffusion and greatly improves the ability of anti-attack. However, it weakens the algorithm's ability to perform occlusion attacks. The proposed algorithm meets the requirements of image encryption, achieves the expected goal, and can be used in image encryption.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the Natural Science Foundation of Shaanxi Province of China under Grant No. 2021JQ-131 and the Scientific Research Funding Project of Northwest A&F University under Grant no. 2452019153.

References

- [1] G. Veena and M. Ramakrishna, "A survey on image encryption using chaos-based techniques," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, 2021.
- [2] N. Chidambaram, P. Raj, T. Karruppuswamy et al., "An Advanced Framework for highly secure and cloud-based storage of colour Images," *IET Image Processing*, 2020.
- [3] R. Sundararaman, P. Siva, N. Mukund et al., "Chua's diode and strange attractor: a three layer hardware—software co-design for medical image confidentiality," *IET Image Processing*, vol. 14, no. 7, 2020.
- [4] Z. Liu, T. Xia, and Y. Wang, "Image encryption technology based on fractional two-dimensional discrete chaotic map accompanied with Menezes-Vanstone elliptic curve cryptosystem," *Fractals*, vol. 29, Article ID 2150064, 2021.
- [5] Z. Liu, T. Xia, and Y. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem," *Chinese Phys. B*, vol. 27, Article ID 030502, 2018.
- [6] Z. Liu, T. Xia, and Y. Wang, "Fractional two-dimensional discrete chaotic map and its applications to the information security with elliptic-curve public key cryptography," *Journal of Vibration and Control*, vol. 24, pp. 4797–4824, 2018.
- [7] G. Ghosh, Kavita, S. Verma, N. Z. Jhanchi, and M. N. Talib, "Secure surveillance system using chaotic image encryption technique," in *Proceedings of the IOP Conference Series: Materials Science and Engineering*, vol. 993, Chennai, India, September 2020.
- [8] J. Zheng and L. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic the sine map," *IET Image Processing*, vol. 14, no. 11, 2020.
- [9] J. Liu, M. Zhong, B. Liu, Y. Liu, and B. Li, "Design of three-dimensional dynamic integer tent map and its image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, pp. 19219–19236, 2021.
- [10] P. K. Ahmad, H. N. Ahmad, and M. B. Amir, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, Article ID 9597619, 23 pages, 2020.
- [11] P. Kumar Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, pp. 2877–2898, 2020.
- [12] Q. Li, *Research on Image Encryption Algorithm Based on Chaotic System*, Shenzhen University, Shenzhen, China, 2018.
- [13] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Processing*, vol. 168, 2020.
- [14] A. Banu, R. Amirtharajan, and D. Ravichandran, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Medical, & Biological Engineering & Computing*, 2021.
- [15] R. Kumar and S. Srivastava, "A novel dynamic recurrent functional link neural network-based identification of non-linear systems using Lyapunov stability analysis," *Neural Computing & Applications*, vol. 33, no. 4, pp. 1–18, 2020.
- [16] Y. Gao and Y. Sun, "Fuzzy C-means clustering small data volume method for calculating Lyapunov exponent," *Journal of Northeast Normal University*, vol. 53, no. 1, pp. 38–42, 2021.
- [17] "A new 4D chaotic system with coexisting hidden chaotic attractors," *International Journal of Bifurcation and Chaos*, vol. 30, no. 10, Article ID 2050142, 2020.
- [18] H. Zhu, B. Pu, Z. Zhu, and Y. Zhao, "Two-dimensional the sine-tent hyperchaotic map and its application in image encryption," *Small Microcomputer System*, vol. 40, no. 7, pp. 1510–1518, 2019.
- [19] N. Rusul, J. Abed, and A. Elaf, "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, 2020.
- [20] S. Jing, Y. Guo, and W. Chen, "Meaningful ciphertext encryption algorithm based on bit scrambling, discrete wavelet transform, and improved chaos[J]," *IET Image Processing*, vol. 15, no. 5, 2020.
- [21] N. R. Zhou, L. X. Huang, L. H. Gong et al., "Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map," *Quantum Information Processing*, vol. 19, no. 9, 2020.
- [22] H. S. Ye, N. R. Zhou, and L. H. Gong, "Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion," *Signal Processing*, vol. 175, Article ID 107652, 2020.
- [23] M.L. Josep, M. Sarah, P.L. Alexandre, H.A. Martin, S. Picart Armada, and D.F. Daniel, "MultiPaths: a python framework for analyzing multi-layer biological networks using diffusion algorithms," *Bioinformatics*, vol. 37, no. 1, pp. 137–139, 2020.
- [24] R. Vidhya and M. Brindha, "A novel dynamic chaotic image encryption using butterfly network topology based diffusion and decision based permutation," *Multimedia Tools and Applications*, vol. 79, no. 41–42, 2020.
- [25] P. Fang, L. Huang, M. Lou, and K. Jiang, "Image encryption algorithm based on two-dimensional Logistic chaotic mapping and DNA sequence operations," *Chinese Science and Technology Papers*, vol. 16, no. 03, pp. 247–252, 2021.
- [26] K. U. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Applied Soft Computing Journal*, vol. 90, 2020.
- [27] M. Ali and X. Wang, "A novel block-based image encryption scheme using a new the sine powered chaotic map generator," *Multimedia Tools and Applications*, vol. 80, pp. 21955–21978, 2021.
- [28] N. Zhou, H. Jiang, L. Gong, and X. Xie, "Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging," *Optics and Lasers in Engineering*, vol. 110, pp. 72–79, 2018.

- [29] X. Zhang and Y. Hu, "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding," *Optics & Laser Technology*, p. 141, 2021.
- [30] X. Shi, Y. Lin, D. He, and J. Mo, "An improved algorithm based on LSB gray-scale image information steganography," *Information and Computer (Theoretical Edition)*, vol. 31, no. 21, pp. 62–64, 2019.
- [31] R. Sivaraman, R. Sundararaman, J. Rayappan et al., "Ring oscillator as confusion- diffusion agent: a complete TRNG drove image security," *IET Image Processing*, 2020.
- [32] H. Pan, Y. Lei, and J. Chen, "Research on digital image encryption algorithm based on double logistic chaotic map," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, 2018.
- [33] S. Aashiq Banu and R. Amirtharajan, "Bio-inspired cryptosystem on the reciprocal domain: DNA strands mutate to secure health data," *Frontiers of Information Technology & Electronic Engineering*, vol. 22, no. 7, pp. 940–956, 2021.