Hindawi
Journal of Sensors
Volume 2019, Article ID 2768121, 12 pages
https://doi.org/10.1155/2019/2768121

Research Article

Image Encryption Algorithm Based on Adaptive Wavelet Chaos

Feng-Ping An[1,2] **and Jun-e Liu**[3]

[1]*School of Physics and Electronic Electrical Engineering, Huaiyin Normal University, Huai'an, JS 223300, China*
[2]*School of Information and Electronics, Beijing Institute of Technology, Beijing, BJ 100081, China*
[3]*School of Information, Beijing Wuzi University, Beijing, BJ 100081, China*

Correspondence should be addressed to Feng-Ping An; anfengping@163.com and Jun-e Liu; 2924175349@qq.com

Received 3 June 2019; Revised 5 October 2019; Accepted 8 October 2019; Published 20 December 2019

Academic Editor: Mohammad Haider

Images, as one of the important carriers for information exchange, play an important role in work and daily life. Image encryption technology has received a lot of attention, and varieties of encryption technologies for images have emerged. Early image encryption technologies have shortcomings such as simple algorithm structure, small key space, and poor resistance to plaintext attacks. These algorithms have been unable to meet the needs of information security at this stage. Based on the wavelet algorithm, chaos algorithm, and cyclic encryption algorithm, combined with frequency domain encryption and spatial domain encryption, a digital image encryption algorithm based on adaptive wavelet is proposed in this paper. In terms of frequency, this paper enhances the adaptive ability of the wavelet algorithm by convex optimization-particle swarm optimization (PSO). At the same time, the chaotic algorithm is used to scramble the low-frequency coefficients. In the aspect of airspace, this paper uses the block-encryption adaptive encryption algorithm to rescramble the wavelet-reconstructed image. And the SHA-1 algorithm is introduced into the plaintext image generation key sequence as a cyclic index value for cyclic encryption. The key composition of the encryption algorithm proposed in this paper is complex, and the idea of a one-time pad is used, which makes the improved algorithm increase the key space and improve the ability to resist the choice of plaintext attack. In each cyclic encryption of the airspace, mutual encryption is performed by image subblocks, and the algorithm adaptability is improved. Through the experimental test of statistical characteristics, key space, and key sensitivity, the encryption performance of the algorithm is verified, and it has strong antiattack and interference ability. It is a relatively secure encryption algorithm.

1. Introduction

As one of the important carriers of information exchange [1–4], images play an important role in work and daily life. During the transmission of digital images, some picture information may involve personal privacy, even involving trade secrets and state secrets. When such information is illegally accessed, stolen, or even tampered with, it will have serious consequences, cause huge economic losses, even endanger national security [5]. How to prevent the occurrence of these security incidents and provide security in digital image transmission is a research topic of concern [6].

At present, there are two main methods for protecting digital image information [5]: digital watermarking technology and image encryption technology [7]. The digital watermarking technology directly embeds segment identification information (digital watermark) into digital images, which does not affect the information value of the original image and is not easily noticed by the human visual system [8]. However, this technology cannot hide the visible information of digital images and reduces the security of digital images transmitted over the network. The image encryption technology uses the encryption algorithm to completely transform the plain image information into randomly arranged pixels [9], forming a disorganized image and then transmitting it. The attacker or the stealer cannot recognize the encrypted image without knowing the key, so that the image transmitted in the network is effectively protected. In 1949, the idea of "mixing some information" mentioned by Shannon in his published paper "Communication Theory of Secrecy Systems" [10] became the origin of digital image encryption technology. An image encryption algorithm based on a

chaotic system is the most widely studied encryption algorithm. Chebyshev chaotic map [11], Rossler system [12], logistic chaotic map [13], three-dimensional Lorenz chaotic system [14], and tent map are common. In 2005, Luo and others [15] proposed an image encryption algorithm with certain adaptive capabilities [16]. The algorithm controls the arrangement of image pixels by using the original image data itself and performs cyclic encryption. Although it can effectively resist the known plaintext attack, the algorithm structure is simple and the security is low. In [17], an adaptive two-dimensional wavelet transform algorithm is proposed. It updates the operator with the local feature information of the image. At the same time, the regression algorithm is used to predict the corresponding operator information, so that the algorithm reduces the energy of the high-frequency coefficient to some extent. However, the feature information acquisition capability of the algorithm is weak. In [18], Chen et al. proposed a new adaptive wavelet-based image encryption algorithm, which mainly uses the particle swarm optimization algorithm to optimize the encryption process, thus improving the wavelet image encryption efficiency. Aiming at the problems of weak adaptive ability and low encryption efficiency of existing image encryption algorithms, this paper introduces optimization algorithms and heuristic algorithms to improve the traditional wavelets, so that wavelets have better adaptive ability. Therefore, this paper uses the optimized wavelet to adaptively decompose the image to obtain multiple image components, then fully utilize the characteristics of initial value sensitivity and parameter sensitivity of chaos theory and select the combination of multiple chaotic systems to encrypt the low-frequency coefficient matrix as the first module of the encryption system. At the same time, this paper also combines the cyclic adaptive encryption algorithm, proposes a cyclic encryption algorithm combining SHA-1 key sequence and adaptive encryption, and adds the process of block encryption, as the second module of the encryption system. In these two encryption modules, the optimized adaptive wavelet and the newly proposed cyclic adaptive encryption technology are used, respectively, which effectively improve the adaptive ability of the encryption algorithm and solve the problems that the traditional image encryption algorithm has low adaptive ability for the plaintext image and poor resistance to selective plaintext attack and other issues.

Section 2 of this paper will mainly explain the digital image encryption algorithm based on the adaptive wavelet chaos proposed in this paper. Section 3 analyzes the image encryption algorithm proposed and compares it with the mainstream encryption algorithm. Finally, the last section summarizes and discusses the full text.

2. Digital Image Encryption Algorithm HA Based on Adaptive Wavelet Chaos

Image encryption technology is divided into two categories according to domain: image spatial domain encryption and image frequency domain encryption. Image spatial domain encryption can achieve high-speed and efficient encryption algorithms, so it is widely used in various fields. However, with the increasing demand for encryption, the image frequency domain encryption algorithm has gradually developed due to the weak ability of the image spatial domain encryption algorithm to resist external attacks. The image frequency domain encryption algorithm transforms the image from the spatial domain to the frequency domain representation by using mathematical transformation. The ciphertext image is obtained by encrypting the coefficients in the frequency domain, and the decryption needs to obtain the plaintext image through inverse transformation. The image frequency domain encryption algorithm uses mathematical transformation to transform the image from the spatial domain to the frequency domain for representation and encrypts the coefficients in the frequency domain to obtain the ciphertext image. The decryption needs to obtain the plaintext image through inverse transformation. There are many methods for transforming an image from a spatial domain to a frequency domain. Discrete Fourier transform, discrete cosine transform, wavelet transform, and the like are widely used.

The frequency domain encryption algorithm has strong initial value sensitivity and has strong robustness against external attacks. In the wavelet transform of the frequency domain, the computational complexity of the lifted wavelet transform is low, which can effectively save the computational cost and relatively reduce the loss of image information in the decryption operation. This paper makes use of the advantages of wavelet lifting and combines the proposed optimization algorithm [19] to design a new encryption algorithm.

2.1. Encryption Scheme Design. The digital image encryption algorithm based on the adaptive wavelet proposed in this paper is mainly divided into two modules:

The encryption algorithm module 1 is shown in Figure 1. Firstly, the optimization algorithm and heuristic algorithm are used to optimize the 9/7 wavelet transform, which can further improve the adaptive ability of wavelet transform. Then, the paper uses the optimized wavelet to decompose the image to obtain a series of image components. Further, the low-frequency coefficient and the high-frequency coefficient of the image to be encrypted are obtained. A set of double chaotic sequences is obtained by using two Logistic chaotic maps with different parameters, and the low-frequency coefficients obtained by image decomposition are scrambled and made confusing. Then, the scrambled low-frequency coefficient and the high-frequency coefficient are reconstructed by the optimized wavelet algorithm. This will give you the scrambled image after the first encryption. At this point, the encryption of module 1 is completed, and the parameters and the initial values of the logistic chaotic map r, μ, x_0, and y_0 are used as the keys of the encryption module 1. In order to improve the security of the algorithm, the scrambled image is encrypted a second time.

The encryption algorithm module 2 is shown in Figure 2. After the scrambled image encrypted by module 1 is obtained, the scrambled image is filled and divided, and the scrambled image is equally divided into 4 subimages. And the SHA-1 key is generated by the SHA-1 algorithm

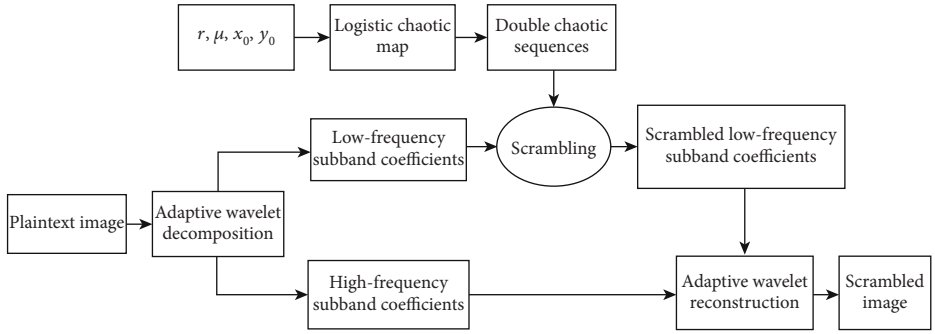


Figure 1: Encryption algorithm module 1.

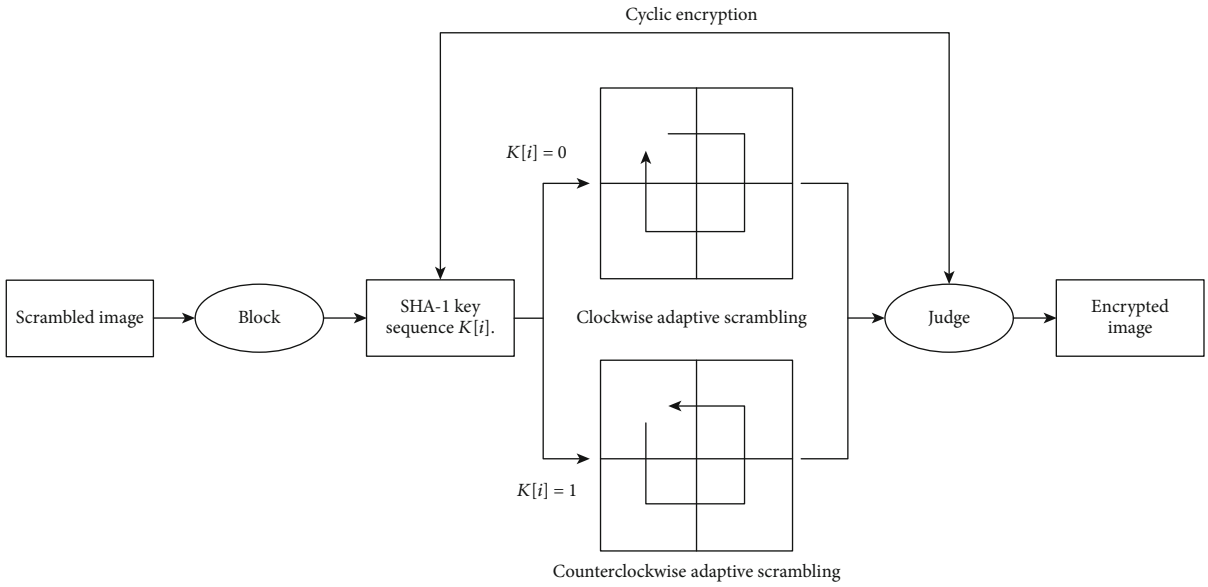


Figure 2: Encryption algorithm module 2.

according to the plaintext image, and finally, two different modes of adaptive cyclic encryption are performed according to the value of the SHA-1 key.

2.2. 9/7 Wavelet Transform Based on Lifting Algorithm. The finite-length filter is represented by equations (1) and (2) to represent the low-pass filter functions at the decomposition end and the reconstruction end:

$$H(\omega) = \sum_{n=-N_1}^{N_2} h_n e^{-in\omega}, \tag{1}$$

$$G(\omega) = \sum_{n=-M_1}^{M_2} g_n e^{-in\omega}. \tag{2}$$

The biorthogonal wavelet construction theorem is as follows.

Suppose $H(\omega) = \sqrt{2}[(1+e^{-i\omega})/2]^N P(\omega)$, $G(\omega) = \sqrt{2}[(1+e^{-i\omega})/2]^{\tilde{N}} \tilde{P}(\omega)$, and $P(\omega)$ and $\tilde{P}(\omega)$ are polynomials for $e^{-i\omega}$, if the following conditions are met:

(1) Normalization: $H(0) = \sqrt{2}$ and $G(0) = \sqrt{2}$

(2) $\sup_{\omega\in[0.2\pi)} |P(\omega)| < 2^{N-1}$ and $\sup_{\omega\in[0.2\pi)} |\tilde{P}(\omega)| < 2^{\tilde{N}-1}$

(3) $H(\omega)\overline{G(\omega)} + H(\omega+\pi)\overline{G(\omega+\pi)} = 2$ is established everywhere

So far, a pair of biorthogonal wavelet filters can be constructed according to the $H(\omega)$ and $G(\omega)$ above.

In the 9/7 optimized wavelet algorithm, 9 and 7 represent low pass filter coefficients and high pass filter coefficients, respectively. The two filter coefficients $h[n]$ and $g[n]$ are divided into odd and even terms, and they are Z-transformed to obtain the following formula:

$$\begin{aligned} H_e(z) &= h_0 + h_2\left(z + z^{-1}\right) + h_4\left(z^2 + z^{-2}\right), \\ H_o(z) &= h_1(z+1) + h_3\left(z^2 + z^{-1}\right), \\ G_e(z) &= g_1\left(1 + z^{-1}\right) + g_3\left(z + z^{-2}\right), \\ G_o(z) &= -g_0 - g_2\left(z + z^{-1}\right). \end{aligned} \tag{3}$$

Bringing equation (3) into the multinomial matrix $P_a(z)$ at the 9/7 wavelet decomposition end, the following formula can be obtained:

$$P_a(z) = \begin{bmatrix} H_e(z) & G_e(z) \\ H_o(z) & G_o(z) \end{bmatrix}. \tag{4}$$

Using the notation in [20, 21], the multinomial matrix $P_a(z)$ is expressed as

$$P_a(z) = P_1 P_2 P_3 P_4 P_5. \tag{5}$$

Among them,

$$\begin{aligned} P_1 &= \begin{bmatrix} \zeta & 0 \\ 0 & -\dfrac{1}{\zeta} \end{bmatrix}, \\ P_2 &= \begin{bmatrix} 1 & \delta(1+z) \\ 0 & 1 \end{bmatrix}, \\ P_3 &= \begin{bmatrix} 1 & 0 \\ \gamma\left(1+z^{-1}\right) & 1 \end{bmatrix}, \\ P_4 &= \begin{bmatrix} 1 & \beta(1+z) \\ 0 & 1 \end{bmatrix}, \\ P_5 &= \begin{bmatrix} 1 & 0 \\ \alpha\left(1+z^{-1}\right) & 1 \end{bmatrix}. \end{aligned} \tag{6}$$

From the above formulas (4) and (5), we can get

$$\begin{cases} h_0 = (1 + 2\alpha\beta + 2\alpha\delta + 2\gamma\delta + 6\alpha\beta\gamma\delta)\zeta, \\ h_1 = (3\beta\gamma\delta + \beta + \delta)\zeta, \\ h_2 = (\alpha\beta + \alpha\delta + \gamma\delta + 4\alpha\beta\gamma\delta)\zeta, \\ h_3 = \beta\gamma\delta\zeta, \\ h_4 = \alpha\beta\gamma\delta\zeta, \\ g_0 = \dfrac{2\beta\gamma + 1}{\zeta}, \\ g_1 = -\dfrac{3\alpha\beta\gamma + \alpha + \gamma}{\zeta}, \\ g_2 = \dfrac{\beta\gamma}{\zeta}, \\ g_3 = -\dfrac{\alpha\beta\gamma}{\zeta}. \end{cases} \tag{7}$$

2.3. Adaptive Optimization of Lifting Wavelet Transform. The traditional wavelet structure has many limitations such as low precision and weak adaptive ability in practical applications. At the same time, in the traditional wavelet framework, its updated algorithm method and prediction algorithm are fixed. In this paper, the optimization algorithm and the heuristic algorithm are used to optimize the two algorithms and adjust them continuously to obtain the optimal operation steps and processes, so as to obtain the encryption algorithm with the least error [22, 23].

Decompose the original signal using the optimized wavelet method proposed in Section 2.2 of this paper. The original signal $x(n)$ is subjected to lifting wavelet decomposition, and α, β, γ, δ, and ζ are used to represent the coefficients generated by the functions P and U in the lifting algorithm, and the 9/7 wavelet transform process based on the lifting algorithm is as follows:

(1) Parity decomposition:

$$\begin{aligned} s_i^{(0)} &= x_{2i}, \\ d_i^{(0)} &= x_{2i+1} \end{aligned} \tag{8}$$

(2) Two liftings:

$$\begin{aligned} d_i^{(1)} &= d_i^{(0)} + \alpha\left(s_i^{(0)} + s_{i+1}^{(0)}\right), \\ s_i^{(1)} &= s_i^{(0)} + \beta\left(d_i^{(1)} + d_{i-1}^{(1)}\right), \\ d_i^{(2)} &= d_i^{(1)} + \gamma\left(s_i^{(1)} + s_{i+1}^{(1)}\right), \\ s_i^{(2)} &= s_i^{(1)} + \delta\left(d_i^{(2)} + d_{i-1}^{(2)}\right) \end{aligned} \tag{9}$$

(3) Numerical change:

$$\begin{aligned} s_i &= \zeta s_i^{(2)}, \\ d_i &= \frac{d_i^{(2)}}{\zeta} \end{aligned} \tag{10}$$

The adaptive matching lifting wavelet for the original image is equivalent to adaptively select the values of the parameters a, b, c, d, and e. In order to facilitate the optimization calculation, let the vector $t = (\alpha, \beta, \gamma, \delta, \zeta)$, f denotes the original image, and $W(t)$ denotes the lifting wavelet transform. After the values of α, β, γ, δ, and ζ are determined by the optimization algorithm, the adaptive decomposition of the 9/7 wavelet can be determined.

According to the selection criterion of [24], optimize the lifting wavelet transform, so that the sparsity of wavelet coefficients after wavelet transform is improved. The best parameters are obtained by optimizing

$$\left(\hat{t}, \hat{v}\right) = \arg\min_{t,v} \|v - W(t)f\|_2^2 + \lambda\|v\|_1. \tag{11}$$

The vector t in equation (11) is a parameter vector, and the coefficient after the coefficient $W(t)f$ is subjected to the sparse approximation and is represented by an unknown vector v. Among them, formula (11) contains two unknown models, and the above formula is decomposed into formulas

(12) and (13) by the alternating direction method proposed in [24]:

$$v^{(k+1)} = \arg\min_{v} \left\| v - W\left(t^{(k)}\right) f \right\|_2^2 + \lambda \|v\|_1, \tag{12}$$

$$t^{(k+1)} = \arg\min_{t} \left\| v^{(k+1)} - W(t) f \right\|_2^2 + \lambda \left\| v^{(k+1)} \right\|_1. \tag{13}$$

2.3.1. Convex Quadratic Optimization. Formula (12) is optimized in this section to improve the sparsity of the optimized wavelet decomposition. In view of formula (12), the problem of convex quadratic optimization is reflected. Therefore, this paper uses the soft threshold method proposed in [25] to optimize the formula (12).

Let T_λ be the soft threshold operator; T_λ is defined as follows:

$$T_\lambda = \begin{cases} \operatorname{sgn}(v - \lambda), & |v| \geq \lambda, \\ 0, & |v| < \lambda. \end{cases} \tag{14}$$

We can get

$$v^{(k)} = T_\lambda\left(W\left(t^{(k)}\right) f\right). \tag{15}$$

2.3.2. Particle Swarm Optimization. Optimizing equation (13) above is equivalent to optimizing the following formula [26–29]:

$$t^{(k+1)} = \arg\min_{t} \left\| v^{(k+1)} - W(t) f \right\|_2^2. \tag{16}$$

The above equation is regarded as a quadratic optimization problem related to the vector $t = (a, b, c, d, e)$. The particle swarm optimization algorithm (PSO) is used to solve the problem, and the optimal solution is searched by iteratively updating the position and velocity parameters of the vector t.

The specific algorithm steps are as follows [30–32]:

(1) Randomly initialize variable parameters: position X and velocity V

(2) The position X and speed V are updated by

$$\begin{cases} V_i^{k+1} = \omega V_i^k + C_1 r_1 \left(P_{\text{best}}{}^k - X_i^k\right) + C_2 r_2 \left(P_g{}^k - X_i^k\right), \\ X_i^{k+1} = X_i^k + V_i^{k+1}. \end{cases} \tag{17}$$

In equation (17), ω represents the inertia coefficient, C_1 and C_2 represent the learning factor, P_{best} is the front position, P_g is the global optimal position, r_1 and r_2 are random values in $[0, 1]$, and the value of k is $k = 0, 1, 2, \cdots, K-1$

(3) In general, to improve the efficiency of the algorithm to achieve iterative termination conditions, define ω as

$$\omega = \omega_{\max} - (\omega_{\max} - \omega_{\min}) \times \frac{k}{K}, \tag{18}$$

where $\omega_{\max}$ and $\omega_{\min}$ represent the maximum inertia coefficient and the minimum inertia coefficient, respectively

(4) Take $t = p_g$ to complete the optimization of formula (13)

For any image, the main steps of decomposing the image using the optimized wavelet method proposed in this paper are as follows:

Step 1. Input the original image f and initialize vector $t = (\alpha, \beta, \gamma, \delta, \zeta)$.

Step 2. For $k = 0, 1, 2, \cdots, K-1$, perform lifting wavelet decomposition and let

$$v^{(k)} = T_\lambda\left(W\left(t^{(k)}\right) f\right). \tag{19}$$

Perform the PSO algorithm to adapt the vector t to formula (16).

Step 3. Output the optimized $t^{(K)}$.

2.4. Chaotic Map Scrambling Low-Frequency Coefficients. In this paper, the logistic chaotic system in chaos theory is applied. The logistic chaotic system belongs to one-dimensional chaotic systems and is widely used in image encryption because of its complex dynamic behavior [25]. The following formulas (20) and (21) are two one-dimensional logistic mapping formulas with different parameters:

$$x_{n+1} = r x_n (1 - x_n), \quad 0 \leq r \leq 4, x_n \in (0, 1), \tag{20}$$

$$y_{n+1} = \mu y_n (1 - y_n), \quad 0 \leq \mu \leq 4, \mathrm{y}_n \in (0, 1). \tag{21}$$

In the formulas, r and μ are parameters, when $r, \mu \in (3.5699456, 4)$. The basic steps of using the chaotic theory to add interference factors to low-frequency coefficients are as follows:

(1) The low-frequency coefficient to be scrambled is taken as a numerical matrix X of $M \times N$, where each element $a_i \in [0, 255]$. The $M \times N$ pixel values in the matrix X are converted into 8-bit binary numbers, and the position of each pixel is represented by $l(m, n)$, where $m \in [0, M-1]$ and $n \in [0, N-1]$. The x_0 and r of the chaotic map are set, and a set of chaotic sequences $\{x_0, x_1, \cdots x_k\}$ is generated by the logistic chaotic map (20), where $k = 1, 2, \cdots$, and r and x_0 are used as the keys of the system. The

chaotic sequence $\{x_0, x_1, \cdots x_k\}$ is discretized according to

$$S_k = \begin{cases} \text{if } x_1 < 0.45, \text{then } s_1 = 0, & \text{otherwise, } s_1 = a, k = 1, \\ \text{if } x_k < x_{k-1}, \text{then } s_k = 0, & \text{otherwise, } s_k = 1, k > 1. \end{cases} \tag{22}$$

After discretizing the chaotic sequence $\{x_0, x_1, \cdots x_k\}$, a set $\{s_k\}$ consisting of 0 and 1 is obtained. When the sum of $m + n$ is an even number, the 8-bit binary numbers of $\{s_{m+n}, s_{m+n+1}, \cdots, s_{m+n+7}\}$ and $l(m, n)$ in the discretized set $\{s_k\}$ are XORed. When the sum of $m + n$ is an odd number, the $l(m, n)$ are exchanged with the last four bits, and then the $\{s_{m+n}, s_{m+n+1}, \cdots, s_{m+n+7}\}$ in the discretization sequence s_k is XORed. After the calculation is completed, a new matrix X' is generated and each element is represented by $l'(m, n)$

(2) A set of chaotic sequences $\{y_0, y_1, \cdots, y_k\}$ is generated by formula (21), where $k = 1, 2, \cdots$. The μ and y_0 are used as scrambled keys for the chaotic system. The discretization of $\{y_0, y_1, \cdots, y_k\}$ by formula (22) results in a discretized set $\{t_k\}$, and the value of t_k is 0 or 1. Set three arrays of ONE, ZERO, and COMBINE with the initial values are null, reorder X' in (1), and convert X' to a one-dimensional array $G(k)$ using the reshape function in MATLAB. If $t_k = 1$, the value of $G(k)$ is written to the array ONE; if $t_k = 0$, the value of $G(k)$ is written to the array ZERO. ONE and ZERO merge to get the array COMBINE. Using the reshape function in MATLAB, the array COMBINE is converted into a two-dimensional matrix X'' of M rows and N columns, as shown in

$$X'' = \text{reshape}(\text{COMBINE}, M, N). \tag{23}$$

2.5. Adaptive Cyclic Encryption. A grayscale image of $m \times n$ size can be expressed as shown in Figure 3.

A two-dimensional traversal matrix $A_{m\times n}$ is a bijective function $A_{m\times n} = \{q(i, j): 1 \le i \le m, 1 \le j \le n\}$ with all elements coming from the set $\{1, 2, 3, \cdots, mn - 1, mn\}$. Traversing the matrix is actually accessing all the elements in a two-dimensional matrix in a certain order. Several commonly used traversal models are as follows, as shown in Figure 4.

2.5.1. Main Traversal Matrix. A matrix of $m \times n$ is defined as a traversal matrix. If each element in the matrix belongs to set $\{1, 2, 3, \cdots, mn - 1, mn\}$, and $r(i, j) = r(i', j')$, then there are $i = i'$ and $j = j'$, denoted as $r_{(i-1)n+j} = r(i, j)$.

The following matrix is defined as a main traversal matrix, as shown in Figure 5.

In fact, in the algorithm of this paper, the main traversal matrix represents an arrangement order, representing an arrangement of elements in order of magnitude.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Figure 3: Image matrix.

2.5.2. Image Scrambling. $A_{m\times n}$ is the original matrix. To scramble $A_{m\times n}$, first assign the element r_{ij} in $R_{m\times n}$ to the corresponding tag value of each element in $A_{m\times n}$; that is, the element r_{ij} in $R_{m\times n}$ is the tag value of a_{ij}. All the elements in $A_{m\times n}$ are reordered according to the tag values in the order of the elements of the main traversal matrix defined in Figure 5, and the scrambled matrix is A', such as the scrambling of the matrix of Figure 6.

The traversal model matrix $R_{m\times n}$ can be randomly selected, or a matrix composed of specific sorting rules can be used, such as the Arnold sorting and Hilbert sorting.

2.5.3. Standardization of the Traversal Model Matrix. In the above scrambling process, when we do not specify a traversal model $R_{m\times n}$, an external random matrix can be used as a traversal model in the above process. In the algorithm of this paper, the traversal model $R_{m\times n}$ is the subblock after the block in the encryption algorithm module 2, and the specific steps for standardizing it are as follows [32]:

The first step: traverse all the elements in $R_{m\times n}$. Compare to find the minimum values in the matrix and mark them as 1. If multiple equal minimum elements appear, they are marked in the order of the upper left minimum priority, for example, the standardization process of Figure 7.

The second step: follow the principle of the first step, from 1 to mn in order from small to large, until all elements are converted to a positive integer from 1 to mn, as a standardized traversal model matrix.

The scrambling algorithm implemented by traversing the matrix, which can scramble the location of the original data and encrypt the original image. The above scrambling algorithm is improved in the encryption algorithm module 2. The image is segmented first, and the subimage of the image itself is used as the traversal model matrix in the encryption process to implement adaptive encryption, and the SHA-1 key sequence is introduced to cycle the adaptive encryption algorithm; therefore, the security and adaptability of the algorithm is improved. The complete encryption steps of the encryption algorithm module 2 in this paper are as follows:

Step 1. Generate a binary SHA-1 key sequence. The key used in the algorithm which is a 160-bit value returned from the plaintext image is calculated by the SHA-1 algorithm described in section 2.1, that is, a set of hexadecimal numbers totaling 40 bits. Each hexadecimal number is represented by a 4-bit binary number, and finally, a set of binary key sequences of 160 bits in length is formed. A binary key sequence is obtained from

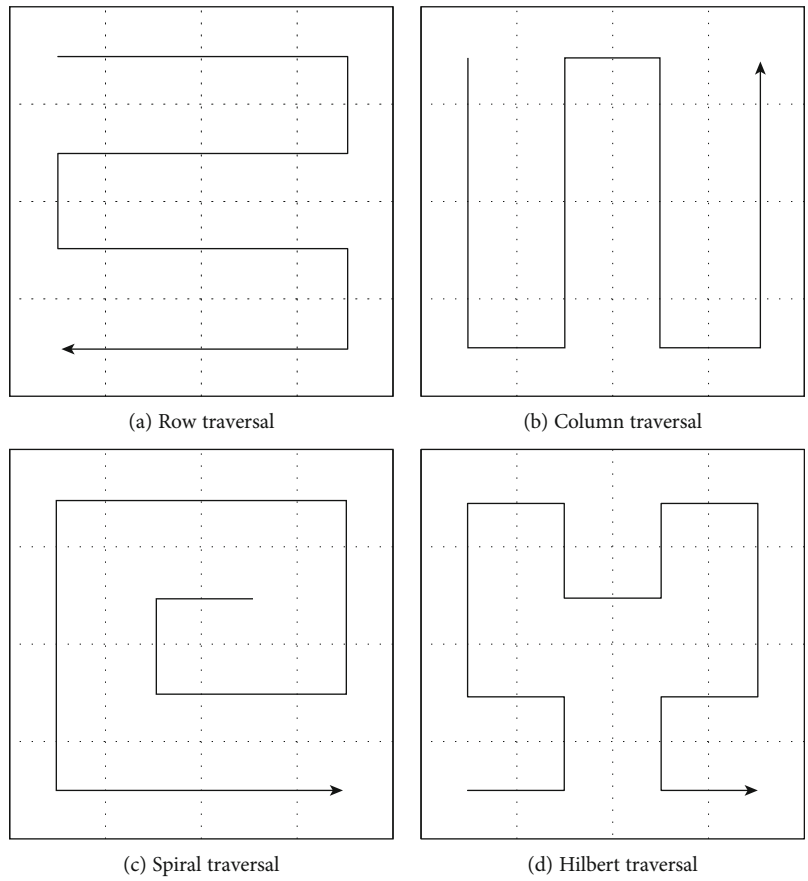


Figure 4: Traversing the model Diagram.

$$\begin{bmatrix} 1 & 2 & 3 & \dots & n \\ n+1 & n+2 & n+3 & \dots & 2n \\ \dots & \dots & \dots & \dots & \dots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \dots & mn \end{bmatrix}_{m\times n}$$

Figure 5: Main traversal matrix.

the original image, such as 1011001. In the encryption process, "0" and "1" represent different encryption models.

Step 2. Image segmentation. The scrambled image processed by the encryption algorithm module 1 is subjected to a block operation. First, fill the image and insert rows or columns into the image, so that the number of rows and columns are even. The elements filling the row or column are between 0 and 255 and use them as keys. Also, the filled portion needs to be removed when decrypting; the adjusted image is divided into four blocks: LH represents the upper left portion, LF the lower left portion, RH the upper right portion, and RF the lower right portion.

Step 3. Adaptive encryption. Here, the encryption is performed in accordance with the value and length of the SHA-1 key sequence. When the value $K[i] = 0$ in the SHA-1 key sequence, the block image is adaptively scrambled in a clockwise direction, as shown in Figure 8.

When the value $K[i] = 1$ in the SHA-1 key sequence, the block image is adaptively scrambled in a counterclockwise direction, as shown in Figure 9.

The four subblock matrices are sequentially encrypted, taking the clockwise adaptive encryption as an example. According to the above rules, LH is used as the index to encrypt RH to obtain R H$'$, RH$'$ is used as the index to encrypt RF to obtain RF$'$, RF$'$ is used as the index to encrypt LF to obtain LF$'$, and LF$'$ is used as the index to encrypt LH to obtain LH$'$. After the last cyclic encryption is completed according to the SHA-1 key sequence, the ciphertext image A'' is outputted.

Step 4. Cyclic encryption. After performing Step 3 above, do the following:

$$\begin{cases} \text{Continue Step 3}, i < m, \\ \text{Encryption}, i = m. \end{cases} \quad (24)$$

$$A_{4\times4}=\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \quad R=\begin{bmatrix} 5 & 11 & 7 & 12 \\ 14 & 1 & 8 & 3 \\ 16 & 6 & 4 & 9 \\ 2 & 13 & 15 & 10 \end{bmatrix} \rightarrow A'_{4\times4}=\begin{bmatrix} a_{22} & a_{41} & a_{24} & a_{33} \\ a_{11} & a_{32} & a_{13} & a_{23} \\ a_{34} & a_{44} & a_{12} & a_{14} \\ a_{42} & a_{21} & a_{43} & a_{31} \end{bmatrix}$$

Figure 6: Matrix scrambling example.

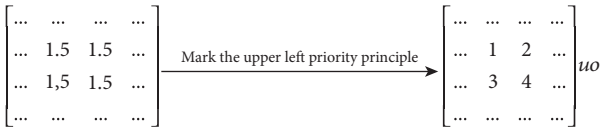


Figure 7: Matrix standardization map.

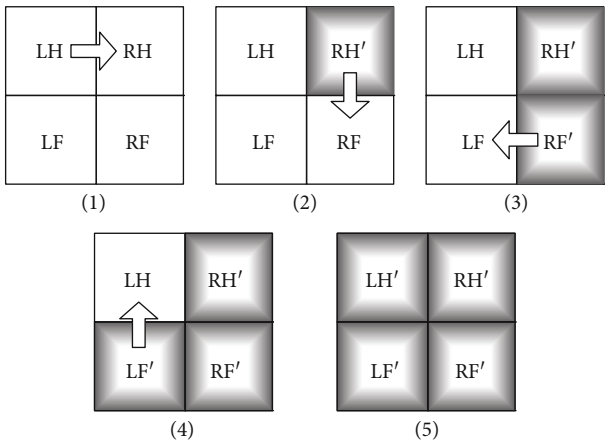


Figure 8: Clockwise adaptive scrambling.

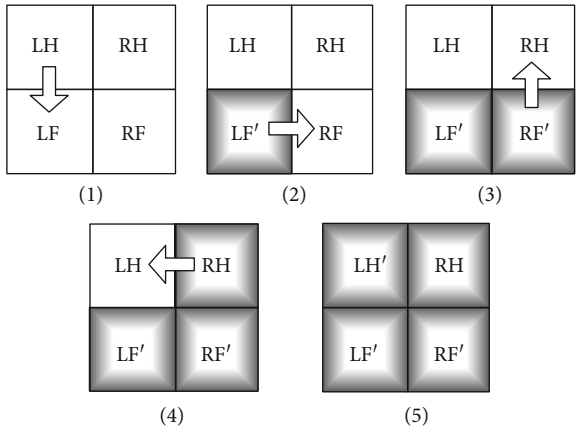


Figure 9: Counterclockwise adaptive scrambling.

In the cyclic encryption process, when proceeding to Step 3 again, the A'' that has been encrypted in the previous round is used as a blocked image matrix for cyclic encryption. The initial value of i is 0, indicating the number of times the cyclic encryption has been performed. m can be the set number of the cycle, or it can be the default length of the SHA-1 binary sequence.

3. Simulation Experiment Results and Key Security Analysis

In this paper, MATLAB R2018a is used as the simulation experiment platform. The 256×256 Lena.jpg image and the 256×256 peppers.jpg image are selected as examples to carry out experiments and analysis. The plain text image is shown in Figure 10.

Encrypting Lena.png and peppers.png using the image encryption algorithm proposed in this paper, the obtained encrypted and decrypted images are shown Figures 11 and 12. The encrypted images (Figures 11(b) and 12(b)) do not show any information related to the plaintext images. It can be seen that the encryption algorithm effectively hides the plaintext information.

3.1. Key Space Analysis. The key of the encryption algorithm proposed in this paper consists of four parts. The formula (25) represents the key composition of the algorithm:

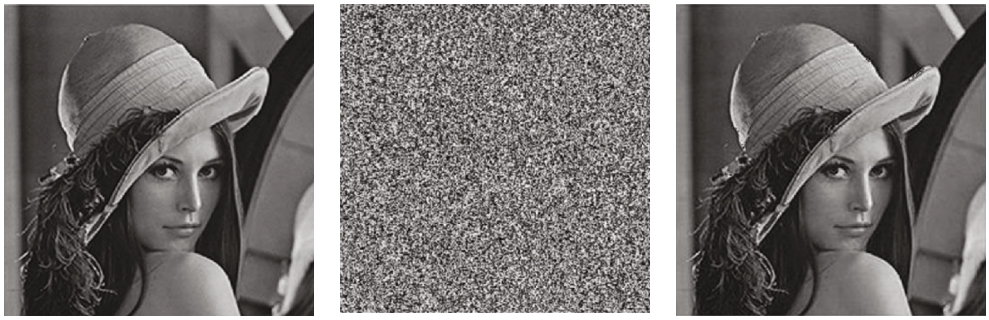
$$\text{key} = \left\{\text{key}_{l,\varepsilon}, \text{key}_{\text{SHA-1}}, \text{key}_{\text{logistic}}, \text{key}_{\text{add}}\right\}. \quad (25)$$

The key $\text{key}_{l,\varepsilon}$ is the number l of the wavelet decomposition, the threshold ε is related to the SHA-1 sequence, the parameters r and μ are of the chaotic system, the initial values x_0 and y_0 form the key $\text{key}_{\text{logistic}}$, and the 160-bit key sequence $\text{key}_{\text{SHA-1}}$ is generated from the plaintext image; the matrix key_{add} fills the image matrix before cyclic encryption. For the integer key, the key space corresponding to the key of length n is 2^n and the key space of each decimal key is 10^{15}; therefore, the key space of the algorithm is about 2^{200}, which is much larger than the key space requirement of 2^{100}, so the key space of the algorithm of this paper can resist exhaustive attacks.

3.2. Key Sensitivity Analysis. Figure 13 shows the experimental results of encrypting and decrypting the Lena.png only when a slight change (only 10^{-15}) is made to the two key parameters r in the key. As can be seen in Figure 13, when the error key is used for decryption, the obtained image (b) is a chaotic image in which no information can be obtained. It can be proved that the sensitivity of the encryption algorithm to the key parameter r can reach 10^{-15}. Combined with the results of the key space analysis in the previous section, it can fully demonstrate that the encryption algorithm of this paper has strong key sensitivity and can effectively resist statistical analysis attacks.

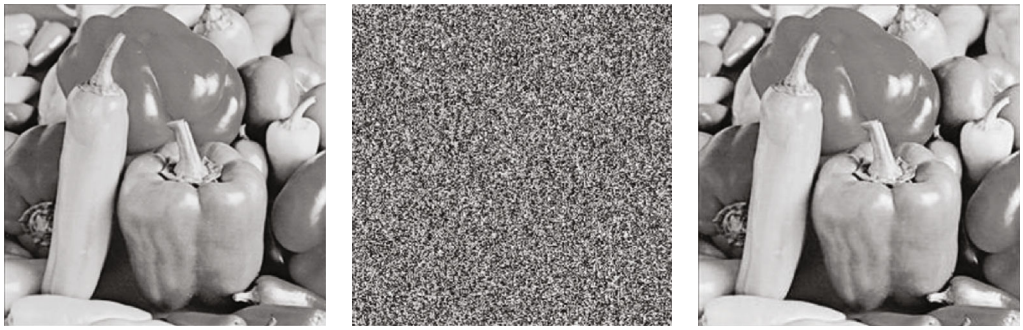
(a) Lena (b) Peppers

Figure 10: The plaintext image.



(a) Lena image (b) Encrypted Lena image (c) Lena image after decryption

Figure 11: The encrypted and decrypted images of Lena.



(a) Pepper image (b) Encrypted pepper image (c) Pepper image after decryption

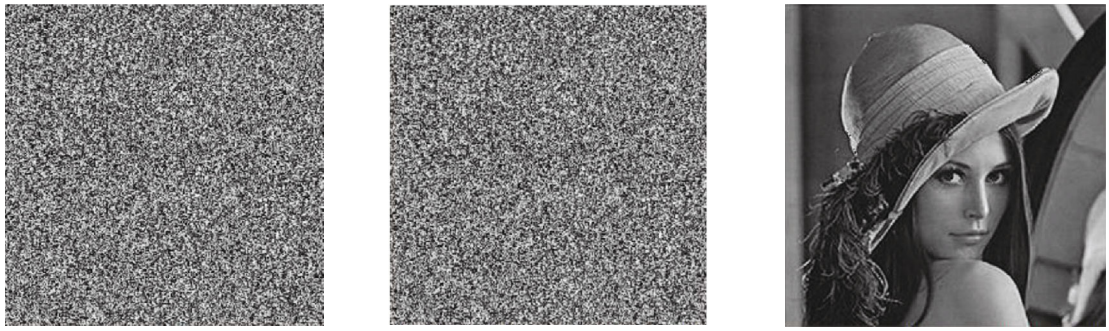
Figure 12: The encrypted and decrypted images of peppers.

3.3. Information Entropy Analysis. Information entropy defines an important feature of randomness and uncertainty in digital image data. It is widely used to measure the uniform distribution of the pixel gray scale in images. If the gray value is distributed evenly, the amount of information of the image is larger. The information entropy calculation formula is as follows:

$$H(x) = -\sum_{i}^{n} p(x_i)\log_2 p(x_i), \begin{cases} 0 \le p(x_i) \le 1, (i = 1, 2, \cdots, n), \\ \sum_{i}^{n} p(x_i) = 1, \end{cases} \tag{26}$$

where $p(x_i)$ represents the probability that the symbol set x_i appears in the message. To better verify the advantages of the encryption algorithm proposed in this paper, Table 1 shows the information entropy of the three different images using the algorithm and other mainstream encryption algorithms.

It can be seen from Table 1 that the ciphertext image information entropy of the encryption algorithm proposed in this paper is the highest, reaching 7.998 or more. It is also the encryption algorithm closest to the best information entropy value of 8. It also verifies that the image distribution encrypted by the encryption algorithm of this paper is very random, and the amount of information needed to crack it is also the largest, and it is the easiest to find the law.



(a) Encrypted Lena image (b) Image after decryption with the wrong key (c) Image decrypted with the correct key

Figure 13: Key sensitivity analysis.

Table 1: Comparison of image information entropy after encryption of four algorithms.

Method type	Lena	Couple	Gray
[26]	7.9729	7.9836	7.9755
[27]	7.9798	7.9832	7.9817
[28]	7.9817	7.9928	7.9801
Ours	7.9983	7.9985	7.9989

Table 2: Comparison of PSNR of images after decryption by four encryption algorithms.

Method type	Lena	Couple	Gray
[26]	19.32	20.09	19.56
[27]	19.71	20.49	19.95
[28]	20.37	20.18	21.06
Ours	21.08	20.94	21.18

Therefore, from the perspective of information entropy attack, the encryption algorithm proposed in this paper is the most secure compared to other encryption algorithms.

3.4. Peak Signal-to-Noise Ratio Analysis. To verify the encryption effect of the proposed algorithm, Table 2 shows the peak signal-to-noise ratio (PSNR) of the decrypted image after the Lena, couple, and gray grayscale images are encrypted using the algorithm and other mainstream encryption algorithms.

It can be seen from Table 2 that although the PSNR of the image obtained by the encryption algorithm is not much higher than that obtained by other algorithms, the PSNR of the image after decryption is still the highest. It further shows that the encryption algorithm proposed in this paper retains the richest original information and loses the least information.

3.5. NIST Random Test. This paper uses the STS2.1 version of NIST to perform randomness testing on the pseudorandomness of the proposed encryption algorithm. In this paper, 2000 pseudorandom sequences are randomly generated for testing, and each sequence has a length of 1×106 bits. The results are shown in Table 3.

It can be seen from Table 3 that the encryption algorithm proposed in this paper has passed various indicator tests.

3.6. Speed Analysis and Antiaggressive Analysis. The image encryption algorithm should not only consider the security performance but also consider whether its running speed meets the actual needs. Therefore, this section uses the encryption algorithm proposed in this paper to perform encryption and decryption tests on different sizes of images and to calculate the calculation time. The experimental environment is a CPU Core Duo 2.84 GHz, memory 8 GB, Windows 7 system and the test software is MATLAB 2018a. The details are shown in Table 4. At the same time, this experiment gives the encryption and decryption calculation times of this paper's encryption algorithm and other mainstream encryption algorithms for a same-sized image, as shown in Table 5.

Table 3: Statistical tests result.

Test class	Proportion	*P* value
Frequency	0.9850	0.84672
Block frequency	0.9980	0.57986
Cumulative sums (forward)	0.9850	0.49073
Cumulative sums (reverse)	0.9880	0.46982
Runs	0.9920	0.31092
Rank	0.9930	0.12098
Fft	0.9850	0.95823
Nonperiodic templates$^{\Delta}$	0.9870	0.95621
Overlapping templates	0.9900	0.60925
Universal	0.9780	0.18251
Approximate entropy	0.9800	0.66823
Random excursions$^{\Delta}$	0.9860	037874
Random excursion variant$^{\Delta}$	0.9860	0.26987
Serial I	0.9960	0.39023
Serial II	0.9910	0.16934
Linear complexity	0.9940	0.24549

$^{\Delta}$Test contains multiple subtests, listed as worst case.

Table 4: Statistics of image encryption and decryption time in different sizes (unit: s).

Image size	Bit	Ours (s)
256×256	24	0.21
512×512	24	1.19
1024×1024	24	1.78
2048×2048	24	3.27

Table 5: Statistics of encryption and decryption time of different encryption algorithms (unit: s).

Image size	Bit	Ours	[28]	[29]	[30]	[31]
2048×2048	24	3.27	3.92	4.89	3.72	3.58

It can be seen from Tables 4 and 5 that the encryption algorithm proposed in this paper is not only acceptable for encryption efficiency. Moreover, the encryption algorithm proposed in this paper is more effective than the encryption of other mainstream encryption algorithms.

Since the encryption algorithm proposed in this paper initializes the scrambled data in a one-time-one-manner, that is, the same plaintext is used to encrypt the same plaintext, the result of each encryption will not be the same. Therefore, this paper can resist the plaintext attack to a certain extent.

4. Conclusion

With the advancement and development of computer application technology, the proportion of images in the data transmitted through the Internet is increasing, and the security of image transmission has become the focus of attention. The encryption technology that was widely recognized as high security has gradually become less secure with the development of cryptanalysis technology. This paper studies and improves the security problems in image encryption technology. The main conclusions of this paper are as follows:

(1) This paper proposes an image encryption method based on adaptive optimization wavelet transform. It integrates an adaptive optimization wavelet into image encryption, which can effectively improve the adaptive ability and encryption efficiency of a traditional wavelet image encryption algorithm. In this process, the particle swarm optimization algorithm is used to optimize the parameters involved in the traditional 9/7 wavelet transform, which can effectively improve the sparsity of the coefficients after wavelet decomposition

(2) A block-based adaptive encryption method based on spatial domain is proposed. In the cyclic encryption process, each cyclic encryption will block the input image, and the subblocks use their own data to encrypt each other, which improves the adaptability of the entire encryption algorithm

(3) Combining the image encryption system based on adaptive wavelet transform with the spatial domain-based block adaptive encryption algorithm, an improved digital image encryption algorithm based on the adaptive wavelet is proposed. The plaintext image is encrypted in the frequency domain and the airspace. The experimental results show that the image encryption algorithm proposed in this paper can effectively improve the encryption effect and encryption efficiency

The authors completed the experimental design work on the basis of theory and used MATLAB R2018a as the simulation experiment platform to realize the encryption and decryption process of the image encryption algorithm. Through the analysis of the experimental results and the strong support of the experimental data, it is proven that the improved algorithm improves the self-adaptation, improves the security of the encryption algorithm, and makes up for the shortcomings of the traditional encryption algorithm. The algorithm has obvious advantages in resisting the chosen-plaintext attacks and hiding the probability distribution of the pixels in the plaintext image. The example analysis shows that the proposed algorithm has certain advantages over the mainstream algorithms in terms of information entropy, peak signal-to-noise ratio, calculation speed, and antiaggression. It objectively verifies the validity, rationality, and reliability of the proposed algorithm.

Data Availability

The data and code used to support the findings of this study are included within the paper.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This study was funded by the National Natural Science Foundation of China (No. 61701188), China Postdoctoral Science Foundation (No. 2019M650512), and Beijing Intelligent Logistics System Collaborative Innovation Center (No. BILSCIC-2019KF-22).

References

[1] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2017.

[2] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[3] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[4] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[5] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[6] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[7] A. Jolfaei, X. W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 235–246, 2016.

[8] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "Hash key-based image encryption using crossover operator and chaos," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4753–4769, 2016.

[9] A. Belazi, A. A. Abd el-Latif, A. V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, pp. 37–50, 2017.

[10] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, 2017.

[11] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[12] A. Yaghouti Niyat, M. H. Moattar, and M. Niazi Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[13] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, 2018.

[14] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," *Optics and Lasers in Engineering*, vol. 67, pp. 145–156, 2015.

[15] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 447–460, 2015.

[16] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Optics and Lasers in Engineering*, vol. 96, pp. 39–49, 2017.

[17] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Processing*, vol. 10, no. 10, pp. 742–750, 2016.

[18] W. H. Chen, S. Luo, and W. X. Zheng, "Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 12, pp. 2696–2710, 2016.

[19] Y. G. Yang, J. Tian, H. Lei, Y. H. Zhou, and W. M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," *Information Sciences*, vol. 345, pp. 257–270, 2016.

[20] X. Wang and H. L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[21] L. Y. Zhang, Y. Liu, F. Pareschi et al., "On the security of a class of diffusion mechanisms for image encryption," *IEEE Transactions on Cybernetics*, vol. 48, no. 4, pp. 1163–1175, 2018.

[22] X. J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333–2356, 2016.

[23] L. Teng, X. Wang, and J. Meng, "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6883–6896, 2018.

[24] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimedia Tools and Applications*, vol. 75, no. 10, pp. 5455–5472, 2016.

[25] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, 2017.

[26] Y. Liu, J. Wang, J. Fan, and L. Gong, "Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4363–4382, 2016.

[27] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607–629, 2017.

[28] M. Li, Y. Guo, J. Huang, and Y. Li, "Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure," *Signal Processing: Image Communication*, vol. 62, pp. 164–172, 2018.

[29] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[30] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia*, vol. 25, no. 4, pp. 46–56, 2018.

[31] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4585–4608, 2018.

[32] J. Wang, W. Liu, and S. Zhang, "Adaptive encryption of digital images based on lifting wavelet optimization," *Multimedia Tools and Applications*, vol. 23, pp. 1–24, 2019.