Hindawi
Quantum Engineering
Volume 2023, Article ID 3431107, 15 pages
https://doi.org/10.1155/2023/3431107

Research Article

A Dynamic Image Encryption Scheme Based on Quantum Walk and Chaos-Induced DNA

Nan Hua, Han-Yang Liu, Xiao-Yun Xiong, Jin-Long Wang, and Jun-Qing Liang

School of Information and Control Engineering, Qingdao University of Technology, Qingdao, China

Correspondence should be addressed to Jun-Qing Liang; liangjunqing@qut.edu.cn

Received 31 May 2022; Revised 10 September 2022; Accepted 23 May 2023; Published 1 June 2023

Academic Editor: Guo-Xing Miao

The development of quantum information technology and increasing attention of people to the secure transmission of image information in the Internet have put forward higher requirements for traditional image encryption algorithms that not only take advantage of the exponential acceleration ability of quantum computing compared with classical computing but also reduce the risk of encryption algorithms being cracked. Therefore, in order to seek the combination of the advantages of quantum computing and classical image encryption algorithms, this paper proposes a new dynamic encryption image scheme of quantum walk and chaos-induced DNA. Firstly, the RGB three-channel pixels of the color image are extracted and combined into a one-dimensional array, and a random sequence is generated by quantum walk to reorder it to obtain a preliminary scrambled image; secondly, the color image is processed by the SHA-256 algorithm and divided into the generated message digest as the initial condition of the chaotic model. The random sequence was generated by the high-dimensional chaotic model which encodes each pixel independently and disorderly as DNA bases. The difference of the chaotic sequence ensures the dynamic selection of random DNA encoding and decoding rules during encryption. At the same time, the number of times of DNA encryption of the encoded pixel value is also controlled by the dynamic induction of the chaotic sequence, and ultimately, the DNA coding sequence is replaced with the decimal pixel value to obtain the encrypted image. The simulation results show that the information entropy of the encrypted image is above 7.99, and the correlation of each channel is close to 0, which can effectively resist brute force attacks, plaintext attacks, statistical analysis attacks, noise attacks, etc. In addition, in this paper, extracting the watermark embedded in the encrypted image to judge whether image information is tampered or forged further improves the security of the image information.

1. Introduction

With the rapid development of Internet communication, as the carrier of information, color images are widely used in personal information exchange, medical pathological images, trade secrets, military satellite images, and other fields. At the same time, image privacy information disclosure and vulnerability to illegal attacks or tampering by unsafe third parties in transmission are also becoming more and more prominent. Traditional encryption algorithms such as AES and RSA cannot satisfy the strong correlation of image pixels. Some novel encryption schemes, such as the DNA base rule has become a common image encryption method. Compressed sensing technology is also more and more integrated into the process of image encryption. The reversible data hidden in the encrypted image are also a manifestation of encryption which have been proposed by researchers [1–4]. With the development of quantum computing [5] and quantum communication [6], researchers urgently need to find an encryption scheme that can adapt to the characteristics of color images and generate effective and reliable keys. The advantages of the proposed scheme are reflected in the use of the quantum walk algorithm and dynamic DNA coding to improve the security performance of image encryption.

Quantum walk has the behavior similar to that of the chaotic system, which can produce a reliable pseudo-random number sequence as the key of image encryption. In quantum computing, quantum walk is exponentially faster than classical walk because of its parallel processing of

quantum superposition states and the interference between qubits. This concept has been widely used since it was proposed by Aharonov et al. [7]. In 2011, Di Franco et al. [8] proposed to use the two-dimensional coin state to control the walker's quantum walk on the two-dimensional plane. In theory, the infinite key space makes it impossible to crack the key. In 2020, Abd El-Latif et al. [9] proposed application of controlled alternating quantum walk as the pseudo-random number generator in quantum color image encryption shows good security and efficiency. Then in 2021, Abd-El-Atty et al. [10] proposed a new image encryption scheme based on quantum walk and double random phase coding, which achieved good results in correlation, histogram, sensitivity, and other simulation experiments. In the same year, Wang et al. [11] combined the random probability distribution matrix generated by quantum random walk with the DNA coding of the image, which proved that the color image encryption is effective and feasible.

Due to the advantages of a sensitive initial value, large key space, and unpredictability, high level chaos is more common. Yousif et al. [12] proposed a fusion of high-dimensional chaotic systems and DNA sequence coding operations. The techniques used will make cryptographic systems more robust to attacks. The chaotic system plays an important role in image encryption and often appears together with other encryption technologies, which reduces the correlation between adjacent pixels when encrypting color images and improves the security of encryption by modifying pixel values [13–17]. In 2016, Tang and Jiang [18] used high-dimensional chaotic maps to encrypt images, which can effectively improve the key space of the encryption algorithm. In 2020, Hanif et al. [19] proposed an encryption system based on chaotic system, cyclic shift operation, and SHA-384 hash function, which increases the required key space and plaintext sensitivity. At the same time, the effectiveness, robustness, and practical applicability of the proposed RGB image cryptosystem are proved. In 2023, Zhang et al. [20] used a one-dimensional chaotic system to generate a series of new two-dimensional chaotic graphs with excellent chaotic performance, respectively, called 1D-NLSCM and 2D-NCTCM, and designed an adaptive image encryption algorithm to overcome the shortcomings of some existing encryption algorithms that are independent of the target image. Wu et al. [21] used the improved one-dimensional chaotic system to generate keys, and the key and the ordinary image were randomly transformed into the DNA matrix to strengthen the security of the encryption scheme.

DNA sequence [22] operation has the merit of ultra-large-scale parallelism and high-density data storage to achieve fast encryption and decryption applications. The encrypted image algorithm which combines image hashing and chaotic sequence control DNA coding has increasingly become the future research trend [23, 24]. In 2021, Dong et al. [25] proposed a color image DNA encryption system based on multioptical chaos and pseudo-random substitution of pixel values. The author claims that this scheme is expected to be used in color image encryption applications in optical communication. In 2022, Huang and Zhou [26] generated the initial conditions of the chaotic system by calculating the SHA-512 hash function value of the plaintext image and the external key, compressing the original image, reencrypting the diffused DNA image by bit-level replacement, and improving global dynamic diffusion, which improved the encryption speed and reduced the transmission burden.

Based on the quantum walk algorithm and image watermarking algorithm, the encryption scheme proposed in this paper can ensure the secure transmission of image information [27–30]. The main process of the encryption scheme in this paper is as follows: (1) reorder the random matrix of three-channel pixels of color images according to quantum walking as a means of image scrambling; (2) input the image hash value into the high-dimensional chaotic system to realize the correlation between plaintext and ciphertext; (3) set the key sequence to dynamically select eight DNA coding rules and replace pixel values to realize encryption. This process mainly involves different times of XOR operations, which increases the encryption complexity. Finally, the watermark information is introduced into the encryption link as a monitoring means to improve the security of image information.

The organizational structure of this paper is as follows: the first section is the introduction, the second section introduces the related work, the third section implements the specific encryption algorithm, the fourth section analyzes and compares the simulation results, and the final section draws a conclusion.

2. Related Work

2.1. Quantum Walk. The quantum walk uses a quantum state with phase instead of classical bits. The walker divides the whole quantum system into H_p position space and H_c coin space in Hilbert space $H = H_p \otimes H_c$, in which the coin state can be expressed as follows:

$$|\psi_c\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle, \tag{1}$$

where $|\uparrow\rangle$ indicates that the coin throwing result is upward, $|\downarrow\rangle$ indicates that the coin throwing result is downward, and $\alpha^2 + \beta^2 = 1$. Each walker performs two unitary operations. First, the coin flip operator is acted on the initial state $|\psi_0\rangle$ of the coin state to flip the coin. A commonly used coin tossing operator is the Hadamard operator:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2}$$

Its function is to obtain a superposition state:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3}$$

The walking direction is determined according to the different coin throwing results, and the walking is realized by the offset operator S.

$$S = \sum_{n} |n-1,0\rangle\langle n,\downarrow| + |n+1,1\rangle\langle n,\uparrow|. \tag{4}$$

Then, under the action of the offset operator, the walkers in different initial states move to the next adjacent point along the direction after coin tossing:

$$\begin{aligned} S|\uparrow,n\rangle &= |\uparrow,n+1\rangle, \\ S|\downarrow,n\rangle &= |\downarrow,n-1\rangle. \end{aligned} \tag{5}$$

The process of quantum walk is from the initial state $|\psi_0\rangle$ to the final state $|\psi_T\rangle = (U_c)^T|\psi_0\rangle$ after the T step. This evolution process iterates $U_c = S \cdot (C \otimes I)$ constantly and maintains the superposition, which can be obtained by measuring the final state. The probability distribution similar to the classical walk in each position is as follows:

$$P_T(n) = \left|(\langle n|\langle\downarrow|)|\psi_T\rangle\right|^2 + \left|(\langle n|\langle\uparrow|)|\psi_T\rangle\right|^2. \tag{6}$$

2.2. Chaotic System. This paper adopts a high-dimensional Chen chaotic system in reference [31]. Its mathematical model is as follows, and it has high requirements on the initial value and control parameters and is sensitive to generate four chaotic sequences for encryption.

$$\begin{aligned} \frac{dx}{dt} &= i(y-x) \\ \frac{dy}{dt} &= -w + ky + hx - xz \\ \frac{dz}{dt} &= xy - jz \\ \frac{dw}{dt} &= x + l. \end{aligned} \tag{7}$$

When the control parameter $i = 36$, $j = 3, k = 28, h = 16$, and $-0.7 \le l \le 0.7$ of the system is selected, the system has a chaotic attractor, and the chaotic system enters a chaotic state. Compared with low-dimensional chaos, the nonlinear behavior of high-dimensional chaos is more difficult to predict, which ameliorates the security performance of the image encryption algorithm.

2.3. DNA Sequence. The main function of the DNA sequence in image encryption technology is to encode and decode image pixels into specific DNA bases and carry out XOR operation to replace the original pixel values. For example, a color digital image with pixel values between 0 and 255. The 8-bit binary pixel value is represented as 4 DNA bases. For example, one pixel value is 77, and its binary value is "01 00 11 01." The DNA encoding of changing this value depends on choosing a different encoding rule when encrypting the image. For example, if you choose rule 8, it will become "CTAC." Using the same DNA rule 8, "CTAC" is converted to a digital format to get the same pixel value of 77. But if you choose another DNA rule to decode, such as rule 1, then "CTAC" will be"10 11 00 10," and the pixel value will be 178. The eight DNA codes are as follows (Table 1). In addition, DNA base XOR operations are introduced in Table 2. XOR operation is used for encryption in this paper.

3. Algorithm

In this paper, the algorithm firstly uses quantum walk to generate a random sequence to scramble the image, then uses classical high-dimensional chaos to generate a random sequence, controls and selects different DNA coding rules and XOR rules, and finally realizes the process of dynamic coding, which improves the coding randomness of image encryption pixel values and achieves high security encryption effect. However, based on the above encryption algorithm, the security of the image can only be guaranteed at the transmission source, and it is unable to detect whether the image information is attacked or whether the image information's copyright is protected in the transmission process. Therefore, the sender embeds the imperceptible watermark information in the encrypted image, and the receiver recognizes the watermark information to know whether the encrypted image is from the other party and whether it is attacked.

3.1. Initial Scrambling. The image was separated by RGB three channels to obtain three $N \times N$ matrices, and the pixel values were extracted by row and synthesized into a one-dimensional array $Img[]$ of $3 \times N \times N$. Next, the two-dimensional quantum walk was adopted. That is, $|\uparrow\rangle$ coin state is used to determine the left of the walker along the x-axis (up the y-axis), that is, $|\downarrow\rangle$ coin state is used to determine the right of the walker along the x-axis (down the y-axis). The initial state is selected as follows:

$$|\psi_0'\rangle = \left[\frac{1}{\sqrt{2}}|\downarrow\rangle + i|\uparrow\rangle\right] \times \left[\frac{1}{\sqrt{2}}|\downarrow\rangle + i|\uparrow\rangle\right] |0_x\rangle|0_y\rangle, \tag{8}$$

where $|0_x\rangle$ indicates the walker's position on the x-axis, $|0_y\rangle$ indicates the walker's position on the y-axis, and the state after performing a unitary operation U_c after one step is as follows:

$$|\psi_1'\rangle = U_C'\,|\psi_0'\rangle = \mathrm{S_x} \cdot \mathrm{S_x}\left[\mathrm{H_1} \otimes \mathrm{H_2} \times \left[\frac{1}{\sqrt{2}}|\downarrow\rangle + \mathrm{i}|\uparrow\rangle\right] \times \left[\frac{1}{\sqrt{2}}|\downarrow\rangle + \mathrm{i}|\uparrow\rangle\right]\right] |0_\mathrm{x}\rangle|0_\mathrm{y}\rangle. \tag{9}$$

Table 1: Eight DNA coding rules.

1	2	3	4	5	6	7	8
00-A	00-A	01-A	01-A	10-A	10-A	11-A	11-A
11-T	11-T	10-T	10-T	01-T	01-T	00-T	00-T
10-C	01-C	11-C	00-C	11-C	00-C	10-C	01-C
01-G	10-G	00-G	11-G	00-G	11-G	01-G	10-G

Table 2: Eight DNA XOR rules.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

After walking N steps: $|\psi_1^N\rangle = (\widehat{U}_C')^N|\psi_0'\rangle$, the probability distribution of the quantum walker in each position is calculated, the probability distribution value is multiplied by 10^{12} to get a large enough integer, and then the modulus of 255 is taken to get a series of random remainder sequence N' with a size of $3 \times M \times N$.

As shown in Figure 1, this sequence is used as the index of the abovementioned one-dimensional array $Img[]$, N' is arranged in ascending order while array $Img[]$ is also rearranged, and then divided into three arrays and restored to the original pixel matrix position by row, thus achieving the initial scrambling effect of the image.

3.2. DNA Encryption. On the basis of Section 3.1, the SHA-256 algorithm is used to generate a series of fixed hash values for the scrambled image, which is represented as a hexadecimal message digest of 64 in length. Any slight change to the pixel of an image will produce different hash values. The message digest is divided into four m_j blocks; each block contains 16 hexadecimal numbers, which are converted to floating-point values as input of new initial values of the chaotic system, where $j = 1, 2, 3, 4$.

$$m_j = \frac{\text{hex2dec}(m_1, \ldots, m_4)}{2^{30}},$$

$$\begin{cases} x_0' = x_0 + m_1 + \text{key} \\ y_0' = y_0 + m_2 + \text{key} \\ z_0' = z_0 + m_3 + \text{key} \\ w_0' = w_0 + m_4 + \text{key} \end{cases} \bmod 1, \tag{10}$$

$$\text{key} = m_1 + m_2 + m_3 + m_4 \bmod 1.$$

The plaintext image is associated with the generated chaotic sequence, which ensures that the encryption key depends on the image, resists the chosen-plaintext attack, and improves the security.

The chaotic system generates four chaotic sequences X, Y, Z, and W with a length of $t + 3 \times N \times N$. In order to avoid the transient effect, the first t elements were taken out, the pixel values of the three channels of the image were converted into binary, and different DNA coding and decoding methods were independently selected for different ranges of random number values in the X sequence. Then, for the encoded DNA base, the XOR operation is carried out by randomly repeating a certain random number of chaotic sequences, and the Y and Z sequences are modified to get the following equation:

$$\begin{aligned} Y' &= Y(i) \times 10^{12} \bmod 8 \\ Z' &= Z(i) \times 10^{12} \bmod 8. \end{aligned} \tag{11}$$

The new sequence elements are randomly arranged in integers of 0–7. The DNA sequence at the starting position of XOR operation is selected through sequence Y', and the number of XOR operations is determined through sequence Z'. The sequence of DNA XOR rules is flexible. Different output chaotic sequence values dynamically select different DNA rules. This way of randomly and dynamically selecting rules determines the complexity of XOR operation. Compared with fixed selection, DNA coding encryption is more complex, which improves the difficulty of cracking.

Eight DNA XOR rules are put into an array with a length of 8 according to the custom order: $D[8]$ = [ACGT, CTAG, TGCA, GATC, CATG, GTAC, TCGA, AGCT]. For example, a point with a pixel value of 77 is coded as CTAC by the x-sequence selection coding rule 8. If the values of the chaotic sequence at this time are $Y'[2]$ and $Z'[5]$, the process of each operation is as follows: CTAC starts with the value TGCA at the position of $D[2]$, and then XOR operation is performed in the order of $D[2]$, $D[3]$, $D[4]$, $D[5]$, i.e. TGCA, GATC, CATG, and GTAC. The result of each iteration is as follows:

$$\begin{aligned} &1\text{: GCCC} = \text{CTAC} \oplus \text{TGCA} \\ &2\text{: ACGA} = \text{GCCC} \oplus \text{GATC} \\ &3\text{: CCCG} = \text{ACGA} \oplus \text{CATG} \\ &4\text{: TGCT} = \text{CCCG} \oplus \text{GTAC}. \end{aligned} \tag{12}$$

The final output is TGCT. According to the chaotic sequence W according to the above rules, another decoding rule is selected to replace the pixel value and converted to decimal pixels. The image matrix is output, and the encryption is completed at this time. The image encryption process is shown in Figure 2.

3.3. Watermark Embedding. Immediately after the completion of Section 3.2 encryption, the watermarking algorithm based on DWT (discrete wavelet transform) and SVD (singular value decomposition) is used to embed and extract the watermark of the encrypted image. The whole process is shown in Figure 3. First, the image is transformed by DWT transform, and the DWT of the image $f(i, j)$ with the size of $M \times N$ is defined as follows:

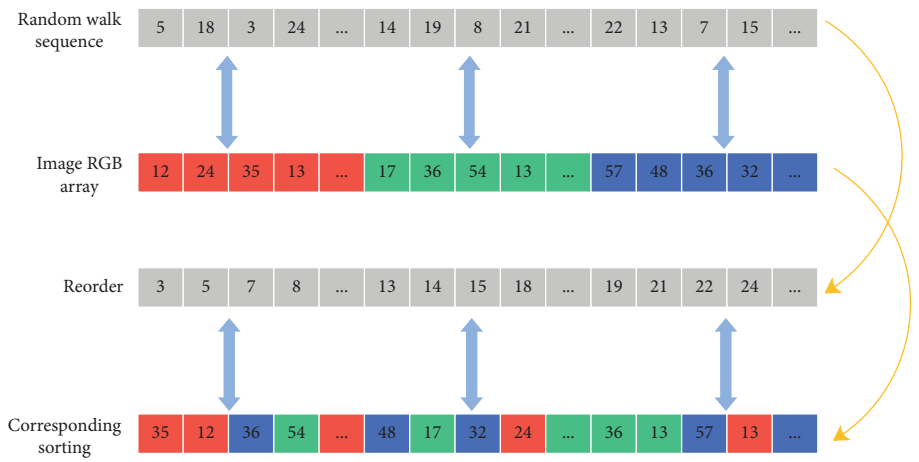

Figure 1: Pixel rearrangement.

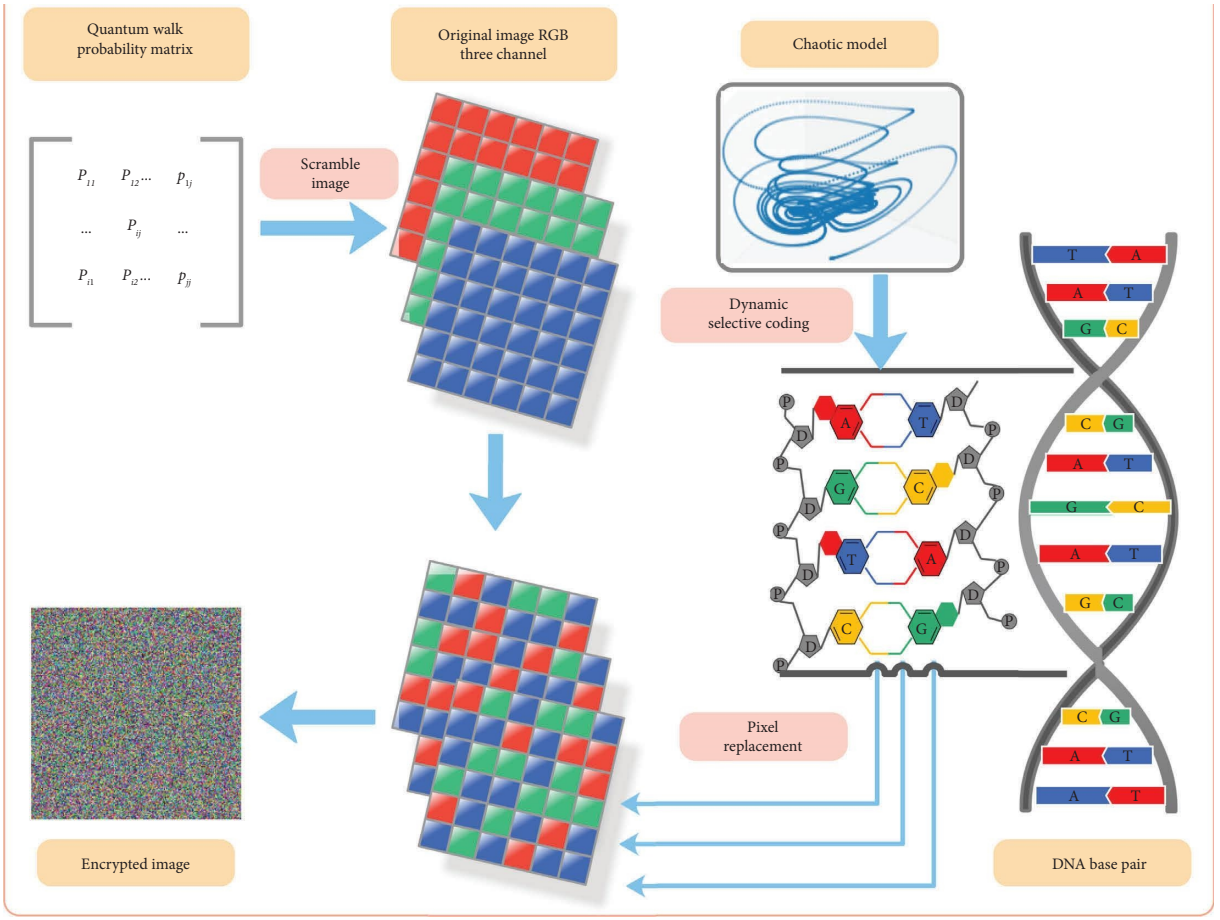

Figure 2: The flow diagram of image encryption.

$$W_{\varphi}(t_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}f(i,j)\varphi_{j_0,m,n}(i,j)$$
$$W_{\psi}^{l}(t_0,m,n)=\frac{1}{\sqrt{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}f(i,j)\psi_{j_0,m,n}^{l}(i,j). \quad (13)$$

Usually, let $t_0=0$, where $t=1,2,\ldots,t-1$ and $M=N=2^t$. One scale function $\varphi(i,j)$ and three two-dimensional wavelet functions $\psi^H(i,j),\psi^V(i,j),\psi^D(i,j)$ represent the changes of column direction, row direction, and diagonal direction, respectively. Haar wavelet is selected as wavelet basis function. The change of measurement function corresponds to the gray change of the image:

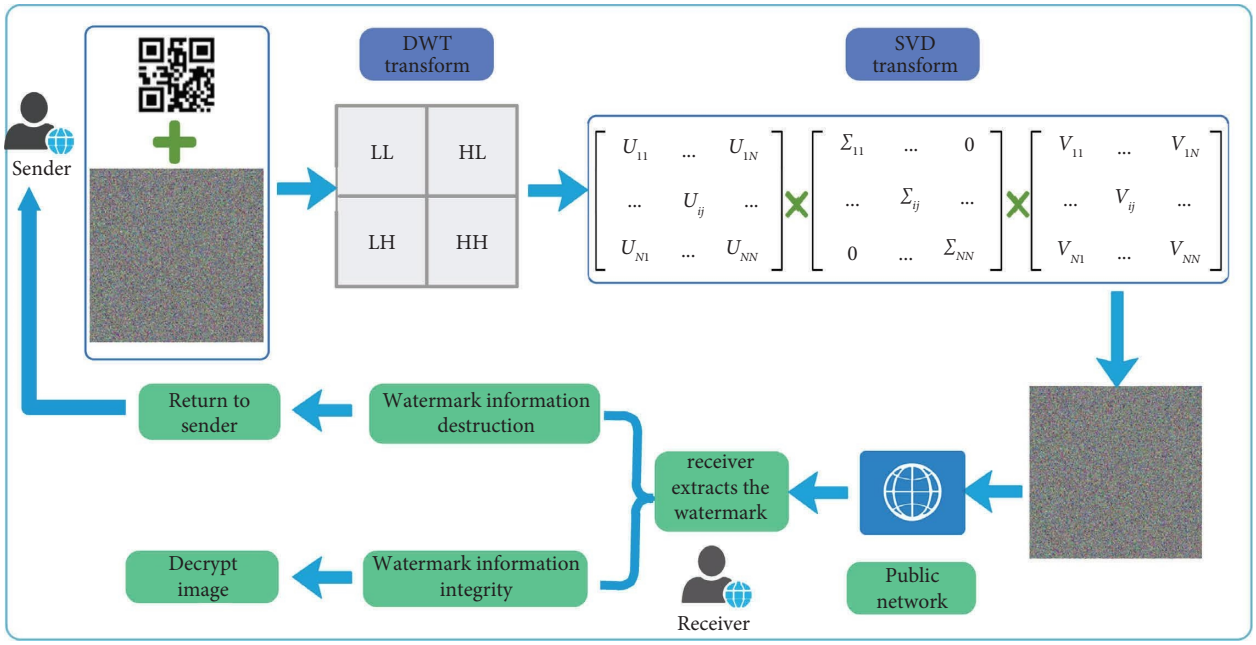

Figure 3: The flow chart of image transmission.

$$\varphi_{t,m,n}(i,j) = 2^{t/2}\varphi\left(2^t i - m, 2^t j - m\right),$$
$$\psi_{t,m,n}'(i,j) = 2^{t/2}\psi\left(2^t i - m, 2^t j - m\right), \tag{14}$$

where $l = \{H, V, D\}$, and the expression of $f(i,j)$ is obtained by inverse discrete wavelet transform.

$$f(i,j) = \frac{1}{\sqrt{MN}} \sum_m \sum_n W_\varphi(t_0, m, n)\varphi_{t_0,m,n}(i,j) + \frac{1}{\sqrt{MN}} \sum_{l=H,V,D} \sum_{t=t_0}^{\infty} \sum_m \sum_n W_\psi^i(t,i,j)\psi_{t_0,m,n}^i(i,j). \tag{15}$$

The imperceptibility and robustness of the watermark are considered to be contradictory. Generally, the low-frequency part concentrates most of the energy of the image. Although the robustness effect of embedding is good, it is easy to cause image distortion, and the high-frequency part is vulnerable to attack. Therefore, this paper comprehensively selects HL subband to embed the watermark information. Then, the HL subband is divided into $8 * 8$ blocks, and each block is SVD decomposed $B_i = U_i \sum_i V_i^T$. Then, the watermark information is superimposed on the first singular value σ_i (maximum singular value) of $\sum_i$ according to the embedding factor, according to the following rules, $Z = \sigma_i \bmod q$

$$\text{when } W_{(i,j)}' = 0 \begin{cases} \sigma_i' = \sigma_i - Z + \frac{5q}{4}, Z \geq \frac{3q}{4} \\ \sigma_i' = \sigma_i - Z + \frac{q}{4}, \text{other}, \end{cases}$$
$$\text{when } W_{(i,j)}' = 1 \begin{cases} \sigma_i' = \sigma_i - Z + \frac{3q}{4}, Z \geq \frac{q}{4} \\ \sigma' = \sigma_i - Z - \frac{q}{4}, \text{other}, \end{cases} \tag{16}$$

where q is the watermark embedding intensity factor, $W(i,j)$ is the scrambled watermark information, and the embedded block is $B_i = U_i \sum_i V_i^T$. Finally, the synthetic image embedded with watermark is obtained by IDWT transform.

3.4. Watermark Extraction. The receiver receives the image sent by the sender, which is composed of a watermark image embedded in an encrypted image. In this paper, the watermark is extracted by blind extraction, that is, DWT transformation is carried out on the synthetic image without the participation of the original image, and $8 * 8$ block processing is also carried out and decomposed according to SVD. $B_i' = U_i \sum_i' V_i^T$. Let $Z = \sigma_i'$ mod q, then

$$\begin{cases} W'_{(i,j)} = 0, & Z \le \dfrac{q}{2} \\ W'_{(i,j)} = 1, & \text{other.} \end{cases} \tag{17}$$

Perform the next analysis based on the extracted watermark information. When the encrypted image is attacked, the change of the watermark information is the same as the image. Therefore, the identity information of the sender can be verified according to the integrity of the extracted watermark information and the content of the watermark information, and the receiver can know whether the image transmitted by the other party has been attacked by a third party. If there is no change in the information, the image is decrypted. The whole process is shown in Figure 3.

3.5. Reverse Decryption. In this paper, the process of image decryption is the inverse process of image encryption. The main process is as follows: the receiver of the image information firstly performs DWT and SVD transformation on the image. (1) If the completely effective and correct watermark information is extracted, the random sequence X, Y, Z, and W is used in encryption provided by the sender and the self-defined XOR rule D[8]. At this time, the decryption is carried out according to the following procedure:

The DNA coding of the pixel value is calculated with the W sequence to obtain De_img[], the application rule is reversed through $Y'[i]$ to obtain the initial pixel coding $De\_img[]$, $Time()$ represents the number of $Z'[i]$ XOR operations, and finally the uncoded pixel value of the scrambled image $img'[]$ is obtained according to $X[i]$.

$$\begin{aligned} \text{De\_img}[] &= \text{decode}(W[i], \text{img}[]) \\ \text{En\_img}[] &= \text{Time}\left(\text{De\_img}[] \oplus Y'[i] \oplus Y'[i-1] \ldots\right) \\ \text{img}'[] &= \text{encode}(X[i], \text{En\_img}[]). \end{aligned} \tag{18}$$

The initial state and walking steps of the quantum walk provided by the sender are calculated to obtain the sequence, which is divided into $\text{key}_1\,\text{key}_2\,\text{key}_3$ and arranged with the three channel pixels $R[i], G[i], B[i]$ of the image. As shown below, $R'[i], G'[i], B'[i]$ are output to merge the original image.

$$\begin{aligned} R'[i] &= \text{sort}(\text{key}_1, R[i]) \\ G'[i] &= \text{sort}(\text{key}_2, G[i]) \\ B'[i] &= \text{sort}(\text{key}_3, B[i]). \end{aligned} \tag{19}$$

(2) If the extracted watermark information is damaged, it will be deemed that the transmission is invalid and the sender will resend the encrypted information.

4. Experimental Simulation

4.1. Experimental Conditions. This paper uses plaintext images from the standard test diagram in the USC-SIPI database, where 4.1.07.tiff (256*256) and 4.1.08.tiff (256*256) are free to use. The simulation environment is Win10 operating system and 2.5 GHz CPU. Pycharm software and tool libraries such as Qiskit, Numpy, and Scipy are used to program and run Python code and show the results.

4.2. Encryption Effect and Security Analysis

4.2.1. Key Sensitivity Analysis. The change of any bit of the key used in the ideal image encryption scheme will cause a completely different encryption and decryption result. The key sensitivity of the chaotic system is related to the initial value and control parameters. When the value $w_0 = 0.1345875401$ of one of the decryption keys is changed by $w_0' = w_0 \pm 10^{-12}$, the original plaintext image cannot be recovered, which proves that the encryption system is very sensitive to the key change. After changing the encryption key w_1 by one bit, w_2 is obtained. The same image is encrypted with w_1 and w_2, respectively. Comparing the pixel change rate after two encryptions, the key is only different by one bit. By comparing the difference between the two ciphertext images, the number of pixel change rate (NPCR in Section 4.3.1) is 99.5941%, and it shows that the key sensitivity is very high. The test of plaintext sensitivity is explained in the differential attack.

4.2.2. Time Complexity Analysis. In the process of replacing image pixels with random sequences generated by quantum walk, three channel images are processed separately, with a time complexity of $O(N * N)$. In the process of encrypting image pixels with DNA base coding pixels, a total of four chaotic sequences are involved, with a time complexity of $O(4 * 3 * N * N)$ (N is the image size). The key generation time is 0.447 s, and the encryption and decryption time of DNA encoded pixels is shown in Table 3.

4.2.3. Histogram Analysis. The histogram shows the statistical information of the image through the distribution of the gray values of the pixels in the color image. The more uniform the histogram distribution of the encrypted image is, the more difficult it is for the attacker to decipher the transformation relationship between the plaintext and ciphertext image through statistical analysis. The effect of image histogram before and after encryption is shown in Figures 4 and 5.

The experimental results show that the histogram effect distribution of the encryption algorithm is very uniform and can "hide" the pixel distribution characteristics of the original image, that is, the attacker cannot analyze the rules of ciphertext and plaintext, so it can resist statistical attacks. Figures 4 and 5, respectively, show the histogram distribution of the 4.1.07.tiff image before and after encryption and the 3D visual histogram effect. Figure 6, respectively, shows the histogram effect of the 4.1.08.tiff image before and after encryption.

According to reference [32], the same plaintext image is encrypted with different keys (key1 and key2) by changing one bit parameter in the encryption key, and the variance

Table 3: Time cost of encrypting and decrypting images (time (s)).

Algorithm	Encryption	Decryption
Proposal 4.1.07.tiff	3.8974	4.0015
Proposal 4.1.08.tiff	4.1021	3.9048

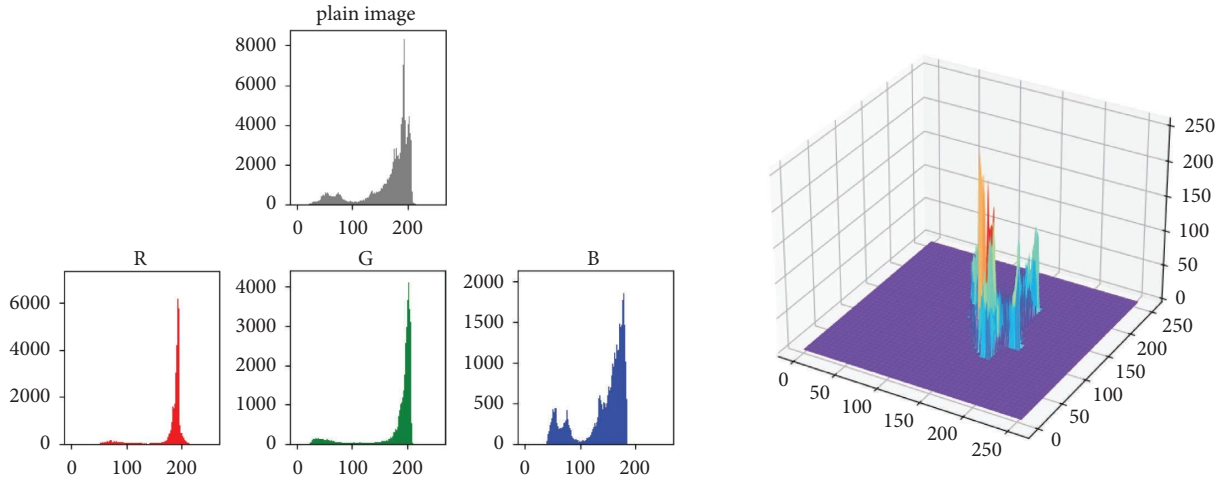

Figure 4: (4.1.07.tiff) image before encrypted RGB histogram and 3D visualization.

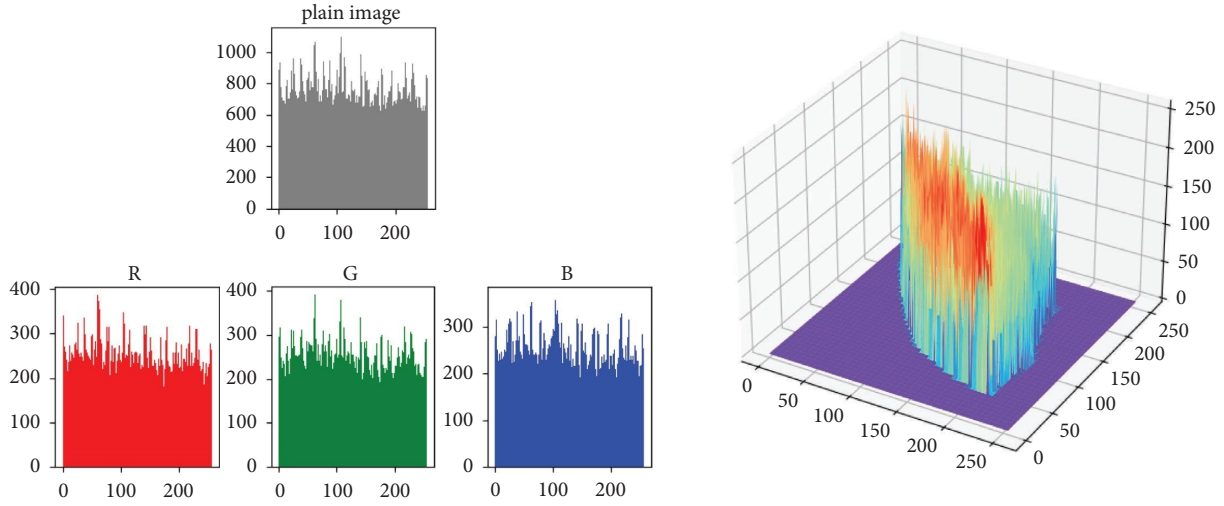

Figure 5: (4.1.07.tiff) image after encrypted RGB histogram and 3D visualization.

value of the histogram of the encrypted image is calculated. The variance value is around 5400, which indicates that the average gray value of each pixel fluctuates around 73. The closer the variance value of the two encryption results, the higher the uniformity of the encrypted image and the better the encryption performance when the key changes. The experimental results are shown in Table 4.

In addition, the similarity of the two histograms is judged by the Chi-Square experiment and calculating the Bhattacharyya distance of the histogram. For the image, the greater the chi-square value is, the lower the image similarity is; otherwise, the higher the similarity is, the maximum value has no upper bound and the minimum value is 0. Bhattacharyya distance is used to measure the similarity of two probability distributions. In fact, in image recognition, it is to judge the distribution of different pixels between them. The higher the Pap distance is, the lower the similarity is, the maximum value is 1, and the minimum value is 0. The experimental results are shown in Table 5.

4.2.4. Correlation Analysis. It is a necessary standard for the encryption algorithm to abate the correlation between adjacent pixels in the encrypted image. The correlation coefficient of adjacent pixels is calculated in each channel of the plaintext image and the ciphertext image, and adjacent pixels

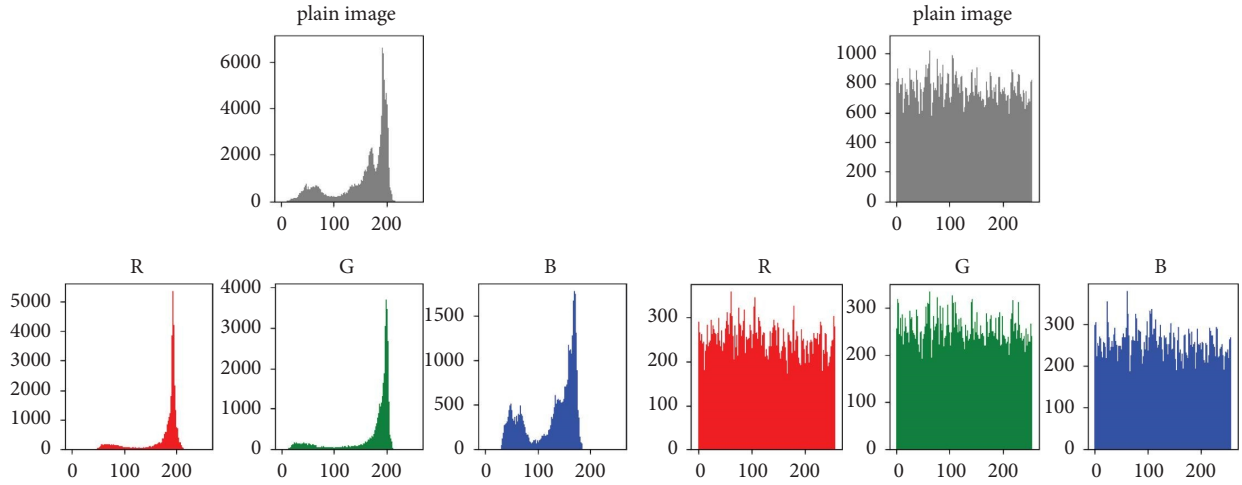

Figure 6: (4.1.08.tiff) RGB histogram before and after encryption of the image.

Table 4: Histogram variance values of different images.

Image	Key1	Key2
4.1.07.tiff	5390.70651	5424.81370
4.1.08.tiff	5403.07695	5409.56588

Table 5: The Chi-square value and Bhattacharyya distance of different images.

Image	Chi-square	Bhattacharyya distance
4.1.07.tiff	728148.86650	0.7039
4.1.08.tiff	821178.18596	0.7162

are randomly selected to compare in horizontal, vertical, and diagonal directions. The formula is as follows:

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2,$$

$$R_{xy} = \frac{(1/N)\sum_{i=1}^{N}\left(x_i - (1/N)\sum_{i=1}^{N}x_i\right)\left(y_i - (1/N)\sum_{i=1}^{N}y_i\right)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{20}$$

The experimental results in Figures 7 and 8 show that the pixels of each channel of the plaintext image are concentrated in the diagonal, while the pixels of the ciphertext image are uniformly distributed. The experimental results are shown in Table 6, which indicate that the correlation coefficient is lower than that of the plaintext image, indicating that the adjacent pixels are irrelevant and have a strong ability to resist statistical analysis.

4.2.5. Information Entropy Analysis. Image information entropy mainly measures the uncertainty or randomness of pixel information. For an image with completely random pixels, if its distribution is uniform enough, the ideal value of information entropy is 8. The calculation formula is as follows:

$$H(x) = -\sum_{i=1}^{L}P(x_i)\log_2 P(x_i), \tag{21}$$

where x_i is the gray value and $P(x_i)$ is the probability of the grayscale x_i.

The experimental results are shown in Table 7, which show that the information entropy of the encrypted image reaches more than 7.99, which shows excellent performance, and indicate that the probability distribution of each gray value in the image is uniform, which can effectively resist statistical information attacks.

4.2.6. Randomness of Sequences. According to the requirements of the NIST SP 800-22 standard, this paper detects the randomness of the set of random numbers and encrypted image pixel values generated by the chaotic system. After several tests, it is found that the P value of the test result is greater than 0.01, and it has passed 15 tests. The experimental results show that the Chaotic sequence as the key and the ciphertext image have good randomness, as shown in Table 8.

4.2.7. Gray Difference Analysis. Gray value difference (GVD) is a measure of randomness between the original image and the encrypted image. By comparing the information difference between the two images, if the two images are exactly the same, it is 0; otherwise, it is 1.

$$\mathrm{GN}(x,y) = \sum\frac{\left[G(x,y) - G\left(x^{'} - y^{'}\right)\right]^2}{4},$$

$$\left(x^{'}, y^{'}\right) = \{(x-1,y),(x+1,y),(x,y+1),(x,y-1)\}, \tag{22}$$

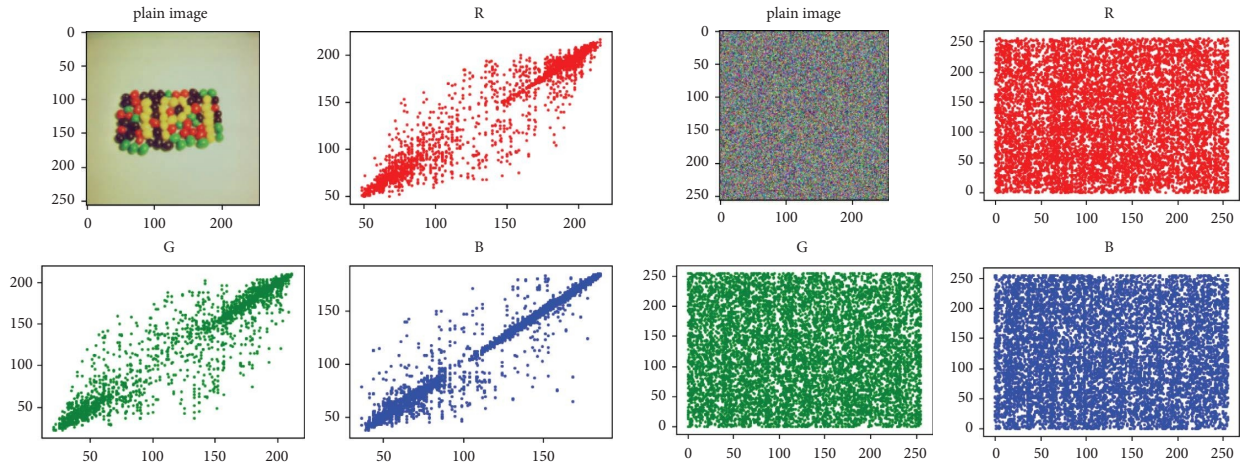

Figure 7: (4.1.07.tiff) histogram effect of different images before and after encryption.

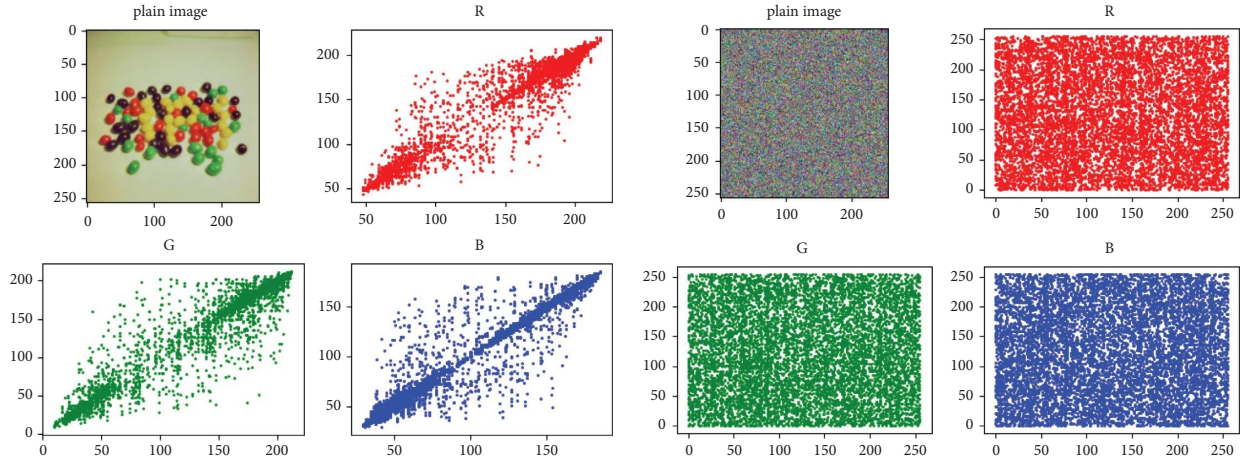

Figure 8: (4.1.08.tiff) histogram effect of different images before and after encryption.

Table 6: Image correlation analysis and comparison.

Algorithm	Channel	Horizontal	Vertical	Diagonal
4.1.07.tiff	R	0.9762	0.9793	0.9567
	G	0.9763	0.9790	0.9549
	B	0.9907	0.9883	0.9817
Encrypt 4.1.07.tiff	R	−0.0275	−0.0001	−0.0219
	G	0.0331	0.0305	0.0016
	B	0.0203	−0.0081	−0.0133
4.1.08.tiff	R	0.9743	0.9712	0.9492
	G	0.9727	0.9739	0.9479
	B	0.9782	0.9815	0.9601
Encrypt 4.1.08.tiff	R	−0.0224	0.0027	−0.0175
	G	0.0053	0.0139	0.0063
	B	0.0002	0.0309	0.0055

where $G(x, y)$ represents the gray value at position (x, y). The average neighborhood gray difference of the image is calculated, which can be calculated with the following formula: VN and VN′ represent the average neighborhood gray value.

Table 7: Information entropy of different images.

Image	Channel	Information entropy
4.1.07.tiff	R	7.9961
	G	7.9943
	B	7.9903
4.1.08.tiff	R	7.9949
	G	7.9938
	B	7.9919

$$\mathrm{GVD} = \frac{\mathrm{VN}'[\mathrm{GN}(x,y)] - \mathrm{VN}[\mathrm{GN}(x,y)]}{\mathrm{VN}'[\mathrm{GN}(x,y)] + \mathrm{VN}[\mathrm{GN}(x,y)]},$$

$$\mathrm{VN}[\mathrm{GN}(x,y)] = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GN(x,y)}{(M-2)(N-2)}. \tag{23}$$

The experimental results (Table 9) show that the gray difference of the encrypted image is very close to the ideal value 1, which is quite different from the original image. It is difficult to analyze the relationship between the two through

Table 8: Chaos sequence and randomness of encrypted images.

Statistical	Chaos sequence	Encrypted image	Results
The monobit test	0.860756	0.689611	Pass
The frequency within the block test	0.401163	0.990926	Pass
The runs test	0.600514	0.946440	Pass
The longest run ones in a block test	0.480094	0.893439	Pass
The binary matrix rank test	0.214521	0.345263	Pass
The discrete Fourier transform test	0.546087	0.248709	Pass
The nonoverlapping template matching test	0.095765	0.182840	Pass
The overlapping template matching test	0.304126	0.354126	Pass
The maurer's universal test	0.275141	0.543087	Pass
The linear complexity test	0.363908	0.627588	Pass
The serial test	0.764028	0.807876	Pass
The approximate entropy test	0.960277	0.718097	Pass
The cumulative sums test	0.191262	0.883478	Pass
The random excursion test	0.246383	0.215611	Pass
The random excursion variant test	0.220671	0.150435	Pass

Table 9: Image GVD analysis.

Image	4.1.07.tiff	4.1.08.tiff
R	0.9855	0.9853
G	0.9829	0.9739
B	0.9833	0.9807

Table 10: NPCR and UACI results of images.

Algorithm	Channel	NPCR (%)	UACI (%)
4.1.07.tiff	*R*	99.6188	33.3568
	G	99.6005	33.4222
	B	99.5968	33.4020
4.1.08.tiff	*R*	99.6048	33.2679
	G	99.5636	33.3312
	B	99.5972	33.5127

statistical information to prove that the encryption security is high.

4.3. Robustness Analysis of Different Attacks

4.3.1. Differential Attack Analysis. The differential attack performance depends on the sensitivity to plaintext. A pixel is randomly selected in the plaintext image, and its pixel value is changed. Differential attack is a kind of selective plaintext attack, and the performance of resisting differential attack depends on the sensitivity to plaintext. In order to resist differential attack, the ciphertext image with great change is obtained by changing a pixel value in the same plaintext image, which shows that the stronger the ability to resist differential attack, the stronger the ability to resist selective plaintext attack. The number of pixels change rate (NPCR) and unified average changed in intensity (UACI) are defined as follows:

$$\mathrm{NPCR} = \frac{\sum_{i,j} T(i,j)}{M \times N} \times 100\%. \tag{24}$$

M and N are the width and height of two random images, which are defined as follows:

$$T(i,j) = f(x) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & \text{other.} \end{cases} \tag{25}$$

UACI can be used to measure the average value of color component contrast intensity. The calculation formula is as follows:

$$\mathrm{UACI} = \frac{1}{M \times N} \frac{\sum C_1(i,j) - C_2(i,j)}{255} \times 100\%. \tag{26}$$

The experimental results (Table 10) show that the NPCR value of each channel pretty approaches its ideal value of 99.6094%, and the UACI value approaches its ideal value of 33.4635%.

Four classical attacks are mentioned in reference [33]: ciphertext-only attack, known plaintext attack, plaintext selected attack, and ciphertext selected attack. If a cryptographic system can withstand selective plaintext attacks, it can withstand other types of attacks. The encryption scheme in this paper has the ability to resist statistical analysis attack, and the large key space cannot be used to brute force crack the plaintext image when only the ciphertext is known. At the same time, differential attack is a selective plaintext attack, and experimental results show that the encryption scheme can effectively resist this type of attack.

4.3.2. Noise Attack Analysis. The mean square error (MSE) and the peak signal to noise ratio (PSNR) are important indicators to measure image robustness. It is defined as follows: the smaller the mean square error, the higher the PSNR, which means that the distortion between the two images is smaller. Salt and pepper noise is achieved by randomly changing the original image pixels to black or white pixels. The proportion of added noise to the number of image pixels varies, and the number of noise also varies. In this chapter's experiment, the proportion added is 5%, 10%, and 50%. Gaussian noise refers to the addition of noise that follows a Gaussian distribution. The level of added noise can be controlled by adjusting the size of

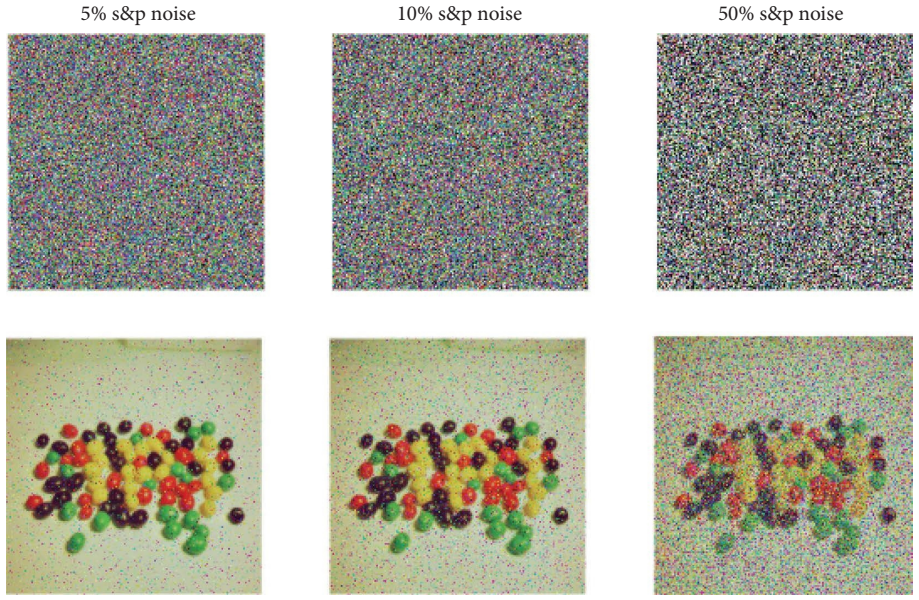

Figure 9: Salt and pepper noise attacks and decrypt images.

the Gaussian distribution standard deviation. The intensity added in this chapter's experiment is 0.002, 0.05, and 0.3, as shown in Figure 9. The comparison with other reference is shown in Table 11.

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[d(i,j) - d^{'}(i,j) \right]^2, \tag{27}$$

$$\frac{\mathrm{PSNR}}{10} = \log_{10}\left(\frac{255^2}{MSE}\right).$$

The experimental results show that although the PSNR of the encrypted image against the attack decreases after decryption, the original image can still be seen visually after decryption, indicating that the encryption algorithm has good security and certain robustness to noise attack.

4.3.3. Analysis of Occlusion Attack. The pixels of 1/16, 1/8, and 1/4 area of the whole image in the encrypted image are randomly removed or covered, and then its PSNR is decrypted and analyzed, as shown in Table 12.

The experimental results (Figure 10) show that the decrypted image can still restore the image to a certain extent, indicating that the encryption algorithm has strong robustness.

4.4. Watermark Attack Detection and Analysis

4.4.1. Imperceptibility Evaluation of Watermark. Taking the *r*-channel image in the RGB component of the encrypted test image as an example, this paper embeds a $64 * 64$ binary watermark QR code image. The experimental results (Figure 11) show that the embedded watermark image is almost the same as the encrypted image visually. The PSNR of the encrypted image is 41.24 db. The higher the PSNR value, the better the invisibility of the watermark.

Table 11: Noise attack analysis.

Noise type	Attack intensity (%)	PSNR (db)
Salt and pepper noise	5	22.89
	10	19.14
	50	15.60
Gaussian noise	0.2	18.55
	5	13.08
	30	10.34

Table 12: The PSRN value of occlusion attack analysis.

Occlusion area	*R*	*G*	*B*
1/16	20.65	20.21	21.15
1/8	17.61	17.29	18.22
1/4	14.57	14.48	15.21

4.4.2. Watermark Attack Detection. By simulating the addition of salt and pepper noise attack with a density of 0.005 (Figure 12(a)), Gaussian noise attack with a variance of 0.002 (Figure 12(b)), 1/8 clipping attack (Figure 12(c)), and 90-degree rotation attack (Figure 12(d)) to the encrypted image embedded with watermark, the watermark image is extracted as follows:

The experimental results show that according to the above simulation attack, the watermark information changes greatly intuitively, and the information in the two-dimensional code cannot be recognized. This paper does not aim at the robustness of the watermark but uses the change of the watermark information as a means of detecting the attack in the transmission process of the

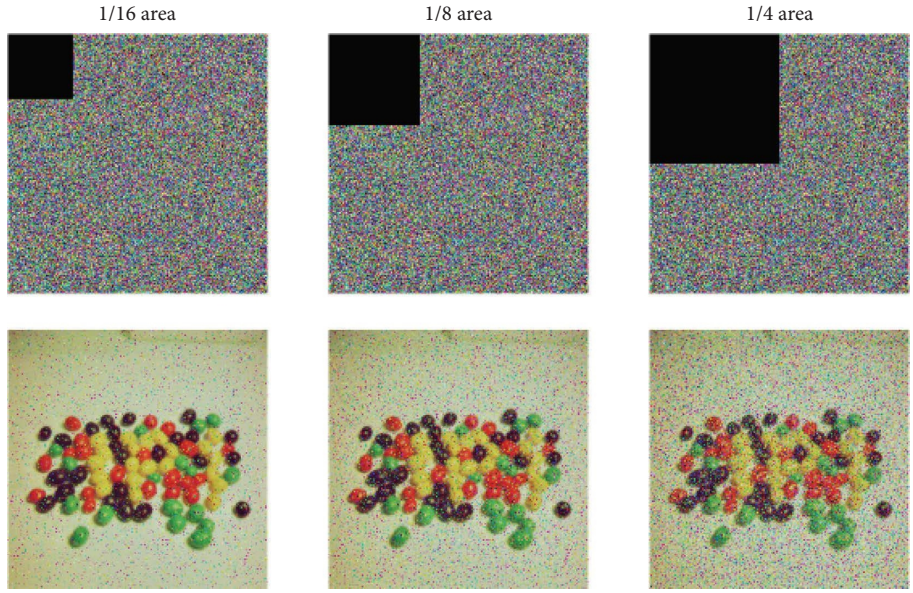

Figure 10: Occlusion attacks and decrypt images.

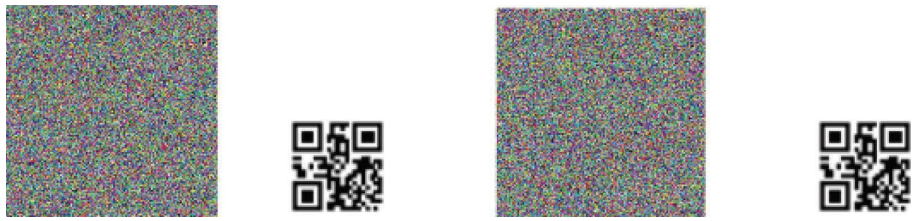

Figure 11: Encrypted image watermark embedding and extraction.

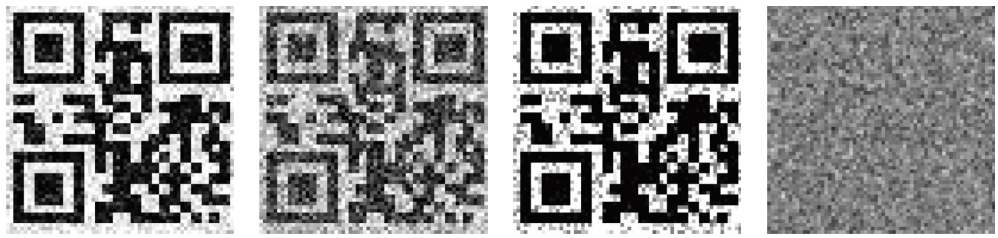

Figure 12: Watermark extraction after attack.

encrypted image so that the receiver can be keenly aware of the malicious attack and tampering in the transmission process according to the change of the watermark information and inform the sender to retransmit.

5. Conclusion

In this paper, the dynamic encryption algorithm based on quantum walking and chaos-induced DNA limits the access of image information at the source of transmission. In the classical chaotic control DNA image encryption algorithm based on improved encryption code complexity, the experimental results show that the randomness of the encrypted image information, key sensitivity, and information entropy effect are good. It can effectively resist statistical analysis attack and differential attack. In addition, the watermarking algorithm based on DWT and SVD detects whether the image is tampered or forged in the transmission process. The combination of the whole process establishes the secure transmission scheme of the image in the open network channel, which provides a new idea for the image encryption scheme. Of

course, the time efficiency of the scheme still needs to be further optimized.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

N.H. and X.X. proposed experimental ideas and completed experimental simulations. H.N. and H.L. completed experimental analysis. J.W. and H.L. wrote the manuscript. J.W. and J.L. reviewed and revised the manuscript.

Acknowledgments

This work was supported by the Natural Science Foundation of Shandong Province, China (Grant nos. ZR2021MF049 and ZR2019YQ01), NSFC under Grant no. 11975132, and Joint fund of the Shandong Natural Science Foundation in 2021 (Grant no. ZR202108020011).

References

[1] A. JarJar, "Two advanced classics exploiting DNA and RNA characteristics to encrypt a color image," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 24603–24629, 2021.

[2] Z. Hua, K. Zhang, Y. Li, and Y. Zhou, "Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing," *Signal Processing*, vol. 183, Article ID 107998, 2021.

[3] D. Xiao, F. Li, M. Wang, and H. Zheng, "A novel high-capacity data hiding in encrypted images based on compressive sensing progressive recovery," *IEEE Signal Processing Letters*, vol. 27, pp. 296–300, 2020.

[4] I. C. Dragoi and D. Coltuc, "On the security of reversible data hiding in encrypted images by MSB prediction," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 187–189, 2021.

[5] G. Long, "Duality quantum computing and duality quantum information processing," *International Journal of Theoretical Physics*, vol. 50, no. 4, pp. 1305–1318, 2011.

[6] R. Qi, Z. Sun, Z. Lin et al., "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, pp. 22–28, 2019.

[7] Y. Aharonov, L. Davidovich, and N. Zagury, "Quantum random walks," *Physical Review A*, vol. 48, no. 2, pp. 1687–1690, 1993.

[8] C. Di Franco, M. Mc Gettrick, and T. Busch, "Mimicking the probability distribution of a two-dimensional Grover walk with a single-qubit coin," *Physical Review Letters*, vol. 106, no. 8, Article ID 080502, 2011.

[9] A. A. Abd El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption," *Physica A: Statistical Mechanics and Its Applications*, vol. 547, Article ID 123869, 2020.

[10] B. Abd-El-Atty, A. M. Iliyasu, A. Alanezi, and A. A. Abd El-latif, "Optical image encryption based on quantum walks," *Optics and Lasers in Engineering*, vol. 138, Article ID 106403, 2021.

[11] Y. Wang, Z. Song, Y. L. Ma, N. Hua, and H. Y. Ma, "Color image encryption algorithm based on DNA code and alternating quantum random walk," *Acta Physica Sinica*, vol. 70, no. 23, pp. 230302–230341, 2021.

[12] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, "A new image encryption based on bit replacing, chaos and DNA coding techniques," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27453–27493, 2022.

[13] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, 2015.

[14] X. Fu, B. Liu, Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–15, 2018.

[15] A. U. Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, 2018.

[16] A. U. Rehman and X. Liao, "A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2," *Multimedia Tools and Applications*, vol. 78, no. 2, pp. 2105–2133, 2019.

[17] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on DNA coding and spatio-temporal chaos," *International Journal on Network Security*, vol. 20, no. 1, pp. 110–120, 2018.

[18] Q. Tang and J. Jiang, "An image encryption algorithm based on high-dimensional chaotic systems," in *Proceedings of the 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1–4, IEEE, Hong Kong, August 2016.

[19] M. Hanif, S. Abbas, M. A. Khan et al., "A novel and efficient multiple RGB images cipher based on chaotic system and circular shift operations," *IEEE Access*, vol. 8, pp. 146408–146427, 2020.

[20] Z. Zhang, J. Tang, H. Ni, and T. Huang, "Image adaptive encryption algorithm using a novel 2D chaotic system," *Nonlinear Dynamics*, vol. 111, no. 11, pp. 10629–10652, 2023.

[21] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[22] J. D. Watson and F. H. Crick, "Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737-738, 1953.

[23] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Journal of Systems and Software*, vol. 85, no. 2, pp. 290–299, 2012.

[24] A. U. Rehman, H. Wang, M. M. Ali Shahid, S. Iqbal, Z. Abbas, and A. Firdous, "A selective cross-substitution technique for encrypting color images using chaos, DNA rules and SHA-512," *IEEE Access*, vol. 7, pp. 162786–162802, 2019.

[25] W. Dong, Q. Li, Y. Tang, M. Hu, and R. Zeng, "A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme," *Optics Communications*, vol. 499, Article ID 127211, 2021.

[26] Z. W. Huang and N. R. Zhou, "Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion," *Optics & Laser Technology*, vol. 149, Article ID 107879, 2022.

[27] X. Ye, X. Chen, M. Deng, S. Hui, and Y. Wang, "A multiple-level DCT based robust DWT-SVD watermark method," in *Proceedings of the 2014 Tenth International Conference on Computational Intelligence and Security*, pp. 479–483, IEEE, Kunming, China, November 2014.

[28] S. M. Arora and S. M. Arora, "A DWT-SVD based robust digital watermarking for digital images," *Procedia Computer Science*, vol. 132, pp. 1441–1448, 2018.

[29] Y. Shen, C. Tang, M. Xu, M. Chen, and Z. Lei, "A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO," *Expert Systems with Applications*, vol. 168, Article ID 114414, 2021.

[30] W. H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "An FPP-resistant SVD-based image watermarking scheme based on chaotic control," *Alexandria Engineering Journal*, vol. 61, no. 7, pp. 5713–5734, 2022.

[31] A. U. Rehman, A. Firdous, S. Iqbal et al., "A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine," *IEEE Access*, vol. 8, pp. 172275–172295, 2020.

[32] Y. Zhang and X. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Information Sciences*, vol. 273, pp. 329–351, 2014.

[33] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.