

Quantum color image encryption: Dual scrambling scheme based on DNA codec and quantum Arnold transform

Tao Cheng(程涛), Run-Sheng Zhao(赵润盛), Shuang Wang(王爽), Kehan Wang(王柯涵), and Hong-Yang Ma(马鸿洋)

Citation: Chin. Phys. B, 2025, 34 (**1**): 010305. DOI: 10.1088/1674-1056/ad8a4b
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Variational data encoding and correlations in quantum-enhanced machine learning

Ming-Hao Wang(王明浩) and Hua Lü(吕桦)
Chin. Phys. B, 2024, 33 (**9**): 090307. DOI: 10.1088/1674-1056/ad5c3b

Preparation of entangled W states based on the cavity QED system

Ke Li(李可) and Jun-Long Zhao(赵军龙)
Chin. Phys. B, 2024, 33 (**9**): 090306. DOI: 10.1088/1674-1056/ad50bf

Delayed-measurement one-way quantum computing on cloud quantum computer

Zhi-Peng Yang(杨智鹏), Yu-Ran Zhang(张煜然), Fu-Li Li(李福利), and Heng Fan(范桁)
Chin. Phys. B, 2024, 33 (**9**): 090304. DOI: 10.1088/1674-1056/ad6253

A family of quantum von Neumann architecture

Dong-Sheng Wang(王东升)
Chin. Phys. B, 2024, 33 (**8**): 080302. DOI: 10.1088/1674-1056/ad50be

Interplay between topology and localization on superconducting circuits

Xin Guan(关欣), Bingyan Huo(霍炳燕), and Gang Chen(陈刚)
Chin. Phys. B, 2024, 33 (**6**): 060311. DOI: 10.1088/1674-1056/ad342c

---

Quantum color image encryption: Dual scrambling scheme based on DNA codec and quantum Arnold transform

Tao Cheng(程涛)[2], Run-Sheng Zhao(赵润盛)[1], Shuang Wang(王爽)[2], Kehan Wang(王柯涵)[1], and Hong-Yang Ma(马鸿洋)[1,†]

[1] *School of Sciences, Qingdao University of Technology, Qingdao* 266033, *China*
[2] *School of Information and Control Engineering, Qingdao University of Technology, Qingdao* 266033, *China*

(Received 27 August 2024; revised manuscript received 6 October 2024; accepted manuscript online 23 October 2024)

In the field of Internet, an image is of great significance to information transmission. Meanwhile, how to ensure and improve its security has become the focus of international research. We combine DNA codec with quantum Arnold transform (QArT) to propose a new double encryption algorithm for quantum color images to improve the security and robustness of image encryption. First, we utilize the biological characteristics of DNA codecs to perform encoding and decoding operations on pixel color information in quantum color images, and achieve pixel-level diffusion. Second, we use QArT to scramble the position information of quantum images and use the operated image as the key matrix for quantum XOR operations. All quantum operations in this paper are reversible, so the decryption operation of the ciphertext image can be realized by the reverse operation of the encryption process. We conduct simulation experiments on encryption and decryption using three color images of "Monkey", "Flower", and "House". The experimental results show that the peak value and correlation of the encrypted images on the histogram have good similarity, and the average normalized pixel change rate (NPCR) of RGB three-channel is 99.61%, the average uniform average change intensity (UACI) is 33.41%, and the average information entropy is about 7.9992. In addition, the robustness of the proposed algorithm is verified by the simulation of noise interference in the actual scenario.

Keywords: DNA codec, quantum Arnold transform, quantum image encryption algorithm

PACS: 03.67.Ac, 03.67.Lx, 03.67.–a

DOI: 10.1088/1674-1056/ad8a4b **CSTR:** 32038.14.CPB.ad8a4b

1. Introduction

In the era of continuous development of communication technology and network, images and videos have become the main carriers of data transmission and exchange. However, the question of how to ensure their security has become an important topic of research.[1–3] Therefore, the encryption and protection of traditional digital images have been extensively studied by many scholars.[4–8] Subsequently, digital images have been combined with quantum computing frameworks for quantum image processing (QIP). QIP exploits properties such as superposition and entanglement of qubits to provide more efficient image processing capabilities in certain situations.[9–13]

Image encryption generally includes traditional image encryption algorithms and quantum image encryption algorithms. Among them, DNA encoding combines the fields of mathematics and biology, with advantages such as parallel processing ability and strong computing power.[14,15] Its unique DNA complementary rules have been widely applied in a series of traditional encryption algorithms. In 2009, based on pseudo DNA operation, Kang *et al.* put forward a character encryption algorithm,[16] which utilizes the central principles of molecular biology to implement encryption technology. In 2014, Huang *et al.* proposed an image encryption algorithm based on a combination of hyperchaos and DNA sequences.[17] In 2018, Ur Rehman *et al.* proposed a color image encryption technique using exclusive-OR with DNA complementary rules, underpinned by chaos theory and the SHA-2 algorithm, which has good resistance to transmission noise and partially encrypted image loss characteristics.[18] However, due to the characteristics of quantum parallelism and entanglement, quantum computing has powerful computing and decryption capabilities.[19,20] The powerful performance of quantum computing often poses a direct threat to some traditional image encryption algorithms. Therefore, in the field of information security, quantum image encryption algorithms play an increasingly important role.[21–25]

Transforming classical images into quantum images is essential for the process of quantum image encryption. Therefore, various models for representing quantum images have been developed. In 2011, Le *et al.* introduced a flexible quantum image representation (FRQI), which encodes both the color and position information of image pixels in quantum states.[26] In 2013, Zhang *et al.* presented a new enhanced quantum representation model (NEQR),[27] which is evolved from the FRQI framework and utilizes the basic state of qubits to store pixel values in images. Moreover, there are

†Corresponding author. E-mail: hongyang_ma@aliyun.com

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

many quantum image representation methods, such as quantum log-polar image (QUALPI),[28] multi-channel quantum image (MCQI) model [29], normal arbitrary superposition state (NASS) model,[30] and others. In recent years, building on these quantum image representation techniques, an increasing number of quantum image encryption algorithms have been introduced.[31–34]

The commonly used method in quantum image encryption is to transform the position information of image pixels to achieve the conversion from the original image to an unordered image in order to improve the security of image information and resist external attacks. In 2014, Jiang *et al.* applied traditional image scrambling methods such as Hilbert, Fibonacci, and Arnold to the field of quantum image processing.[35,36] In 2017, Jin *et al.* introduced an image encryption algorithm that utilizes a key-generalized two-dimensional Arnold transform in conjunction with quantum chaotic mapping.[37] By using the Arnold scrambling algorithm to scramble pixels and using quantum chaos mapping to change the values of diffused pixels, the original image is encrypted. In 2022, Zhao *et al.* proposed a color image encryption scheme based on alternating quantum walking and controlled Rubik's cube[38] In 2024, Zhu *et al.* proposed a mixed double perturbation MQIR image encryption technique based on random permutation. Their experiment proves that the algorithm has a large key space and low computational complexity, making it suitable for non-square quantum images.[39]

In this paper, we combine DNA codec technology with quantum Arnold transform (QArT) to propose a new quantum color image encryption algorithm. Among them, we use the NEQR representation method to transform classical color images into quantum images and encode the color information of pixels by using DNA encoding technology. Meanwhile, we use QArT to scramble the position information of pixels to enhance the encryption effect. Then, we design a decryption method based on DNA decoding rules and the reversibility of quantum circuits. Finally, we prove that the encryption algorithm has good encryption effect and strong anti-attack ability through simulation.

The outline of this paper is as follows. Section 2 introduces the quantum image representation scheme of NEQR, DNA codec and its quantum circuits, quantum Arnold transform method, and other related work. Section 3 presents the detailed operation of the proposed scheme. Section 4 presents experimental verifications of the algorithm's performance and feasibility. Finally, a conclusion is drawn in Section 5.

2. Related work

2.1. Quantum color image representation

We use the NEQR representation model, which converts digital images into quantum state representations and stores pixel values using ground states. For a classic image of size $2^N \times 2^N$, the NEQR model representation method is

$$|I\rangle = \frac{1}{2^N} \sum_{y_o=0}^{2^N-1} \sum_{x_o=0}^{2^N-1} |C(y_o, x_o)\rangle \otimes |y_o x_o\rangle , \tag{1}$$

where y_o and x_o, respectively, represent the vertical and horizontal position information of original image pixels,

$$|C(y_o, x_o)\rangle = \left| \overbrace{R_{yx}^{q-1} R_{yx}^{q-2} \cdots R_{yx}^{1} R_{yx}^{0}}^{\text{Red}} \overbrace{G_{yx}^{q-1} G_{yx}^{q-2} \cdots G_{yx}^{1} G_{yx}^{0}}^{\text{Green}} \overbrace{B_{yx}^{q-1} B_{yx}^{q-2} \cdots B_{yx}^{1} B_{yx}^{0}}^{\text{Blue}} \right\rangle$$

represents the color information, which is the range of pixel values of R, G, and B three-channel pixels satisfies $[0, 2^q - 1]$. Figure 1 shows a color image of size 4×4 and its NEQR form.

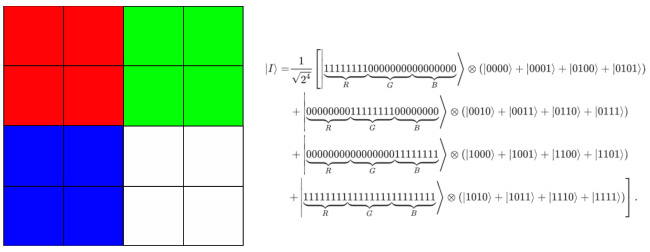


Fig. 1. The NEQR representation of a color image of size 4×4.

2.2. DNA codec

Cytosine (C), adenine (A), guanine (G), and thymine (T), that is, four nucleotides constitute the molecular structure of a deoxyribonucleotide (DNA). According to DNA pairing rules and binary sequences of image pixels, eight complementary schemes are given in Ref. [40]. In addition, Ref. [41] designed a quantum circuit of a DNA codec based on rule 1 with 7 encoding methods. It uses quantum encoding and decoding technology to encrypt the color information of pixels. Figure 2 shows the quantum circuit of DNA codec and how it works. Afterwards, the package of the analog circuit of the DNA codec. The DNA codec is shown in Fig. 3. If the high and low qubits are different, rule 2 can flip the high and low qubits to achieve the exchange pairing of C and G to achieve decoding. If the decoding is done using rule 3, all the low qubits can be flipped to achieve the exchange between A, T and C, G. In rule 4, all the high and low qubits are flipped simultaneously and the high qubits are flipped if they are dif-

ferent from the low qubits. Rule 5 reverses rule 4 by flipping the high qubit when it is different from the low qubit, and flipping the low qubit if the high qubit is the same as the low qubit. Rule 6 is to flip each set of high qubits, and rule 7 decodes by flipping both high and low qubits. Rule 8 switches between A and T and between C and G by inverting all high qubits and low qubits.

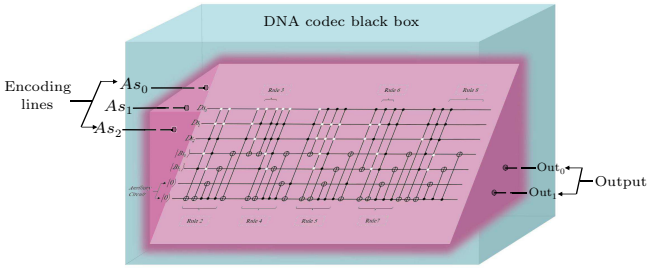


Fig. 2. The architecture of DNA codec black box. Image pixels are converted into binary sequences which serve as input to the DNA codec, and encrypt the color information using corresponding encoding and decoding rules.

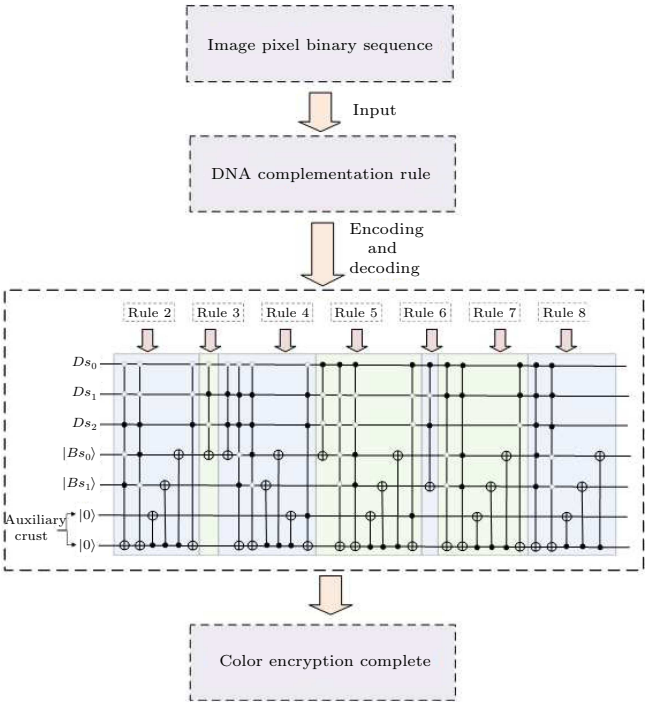


Fig. 3. Quantum circuit structure and working principle of DNA codec, where Ds_0, Ds_1, and Ds_2 represent the sequence numbers of the decoding rule, which are used for decoding. Bs_0 and Bs_1 represent binary sequences of encoded image color pixels.

2.3. Quantum Arnold transform

The classical Arnold transform is a two-dimensional discrete dynamical system often used to study chaos and image scrambling. For a classical image $|I_o\rangle$ of size $2^n \times 2^n$, the scrambling process is as follows:

$$\begin{pmatrix} x_{nt} \\ y_{nt} \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_o \\ y_o \end{pmatrix} (\mathrm{mod}\, 2^n), \quad x_o, y_o = 0, 1, \ldots, 2^n, \tag{2}$$

where x_{nt} and y_{nt} are the new positions of the pixels after the clutter.

The quantum Arnold transform (QArT) is a quantum version of the classical Arnold transform. The scrambling correlation quantum circuit is shown in Fig. 4. In QArT, we pass the quantum states through the corresponding quantum transformation matrix to achieve a similar disturbing effect. For a quantum image $|I_o\rangle$ of size $2^q \times 2^q$, the scrambling process is as follows:

$$\begin{cases} |x_{qt}\rangle = |x_{oq} + y_{oq}\rangle \bmod 2^q, \\ |y_{qt}\rangle = |x_{oq} + 2y_{oq}\rangle \bmod 2^q, \end{cases} \tag{3}$$

where (x_{oq}, y_{oq}) is the original position information of the pixel and (x_{qt}, y_{qt}) is the position information after transforming.

Meanwhile, for quantum Arnold inverse transform, the formula is

$$\begin{cases} |x_{oq}\rangle = \mathrm{QArT}^{-1} |x_{qt}\rangle = (2|x_{qt}\rangle - |y_{qt}\rangle) \bmod 2^q, \\ |y_{oq}\rangle = \mathrm{QArT}^{-1} |y_{qt}\rangle = (-|x_{qt}\rangle + |y_{qt}\rangle) \bmod 2^q. \end{cases} \tag{4}$$

3. Encryption and decryption algorithm

3.1. Encryption scheme

The diffusion and scrambling of pixels in an image are two key stages of image encryption. During the diffusion process, we use DNA encoding and decoding to confuse images, and use quantum XOR operations to encode image pixels, and encrypt the position information of image pixels through QArT. The detailed encryption process is shown in Fig. 4.

Step 1 Divide the original image into RGB three channels and then process each color channel of the original image using the NEQR model to achieve the conversion from classical images to quantum images. Here Eq. (1) can be redefined as

$$\begin{aligned} |I_{\mathrm{image1}}\rangle &= \frac{1}{2^q} \sum_{y_{oq}=0}^{2^q-1} \sum_{x_{oq}=0}^{2^q-1} |C(y_{oq}, x_{oq})\rangle \otimes |y_{oq} x_{oq}\rangle \\ &= \frac{1}{2^q} \sum_{y_{oq}=0}^{2^q-1} \sum_{x_{oq}=0}^{2^q-1} |C(y_{oq}, x_{oq})\rangle \\ &\quad \otimes |y_{q-1} \cdots y_2 y_1 y_0\rangle |x_{q-1} \cdots x_2 x_1 x_0\rangle, \end{aligned} \tag{5}$$

where y_{oq} and x_{oq} represent the positional information of original pixels.

Step 2 In this paper, the color information is converted into a binary sequence using rule 1, which serves as input to the quantum DNA codec to achieve encoding operations on quantum color images, and using the corresponding quantum circuit part of rule 4, decoding is realized by simultaneously inverting high and low qubits. The process is as follows:

$$|I_{\mathrm{image2}}\rangle = E_{\mathrm{r1,r4}} |I_{\mathrm{image1}}\rangle, \tag{6}$$

where ri and rj, respectively, represent the encoding and decoding schemes used. $|I_{\mathrm{image2}}\rangle$ is the image after DNA encoding and decoding, with a pixel size of $2^q \times 2^q$.

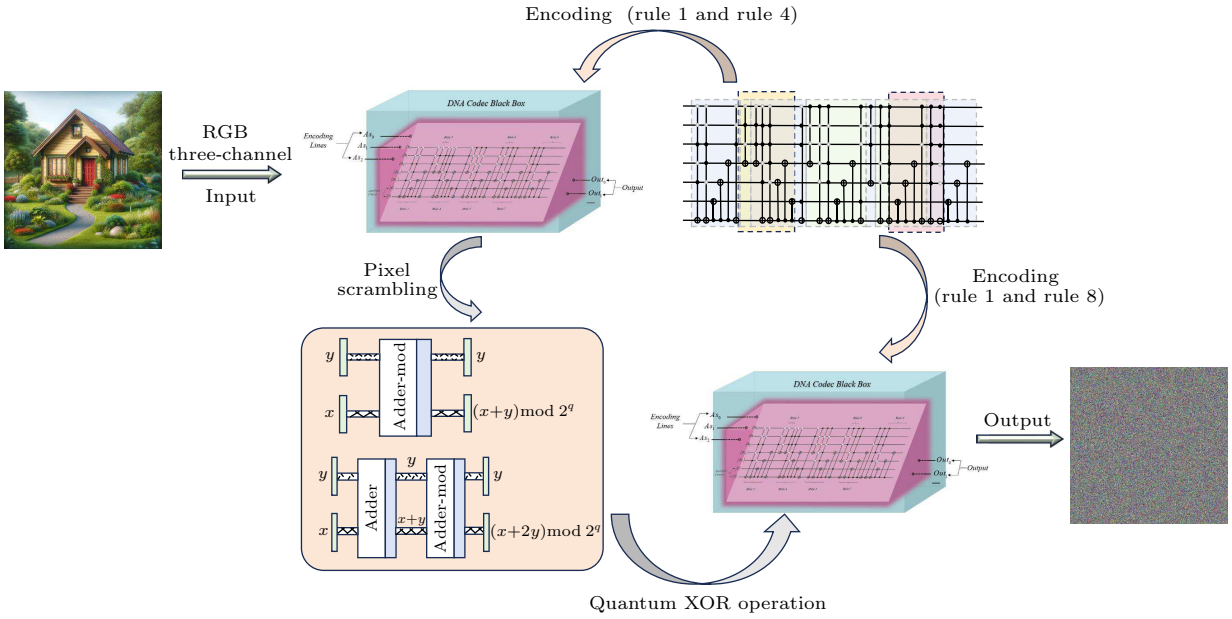


Fig. 4. The flow of the proposed encryption algorithm.

Step 3 Use QArT to perform quantum image scrambling on $|I_{\text{image2}}\rangle$.

According to Ref. [42], we used qubits carrying position information, i.e., $|y_{q-1}\cdots y_2y_1y_0\rangle\,|x_{q-1}\cdots x_2x_1x_0\rangle$, to perform block processing on $|I_{\text{image2}}\rangle$. Assuming that each subblock size is $2^w\times 2^w$, then leave the least significant w bit unchanged, and use the other $q-w$ qubits to determine the image block index. After partitioning, we obtain the number of image subblocks as $2^{q-w}\times 2^{q-w}$, where $q-w$ qubits represent the position information of each segmented image subblock. We apply QArT to $q-w$ qubits representing the position information of image subblocks, and get scrambled images $|I_{\text{image2b}}\rangle$. The process is as follows:

$$\begin{aligned}
|I_{\text{image2b}}\rangle &= \text{QArT}\,|I_{\text{image2}}\rangle \\
&= \frac{1}{2^q}\sum_{y'_{\text{oq}}=0}^{2^q-1}\sum_{x'_{\text{oq}}=0}^{2^q-1}|C(y'_{\text{oq}},x'_{\text{oq}})\rangle \\
&\quad\otimes\text{QArT}\,|y_{q-1}y_{q-2}\cdots y_w\rangle\,|y_{w-1}y_{w-2}\cdots y_0\rangle \\
&\quad\otimes\text{QArT}\,|x_{q-1}x_{q-2}\cdots x_w\rangle\,|x_{w-1}x_{w-2}\cdots x_0\rangle \\
&= \frac{1}{2^q}\sum_{y'_{\text{oq}}=0}^{2^q-1}\sum_{x'_{\text{oq}}=0}^{2^q-1}|C(y'_{\text{oq}},x'_{\text{oq}})\rangle \\
&\quad\otimes|y'_{q-1}y'_{q-2}\cdots y'_w\rangle\,|y_{w-1}\cdots y_1y_0\rangle \\
&\quad\otimes|x'_{q-1}x'_{q-2}\cdots x'_w\rangle\,|x_{w-1}\cdots x_1x_0\rangle\,, \qquad (7)
\end{aligned}$$

where y'_{oq} and x'_{oq} represent the image pixel information after codec in DNA codec according to rule 1 and rule 4, and $|y'_{q-1}y'_{q-2}\cdots y'_w\rangle\,|y_{w-1}\cdots y_1y_0\rangle$ and $|x'_{q-1}x'_{q-2}\cdots x'_w\rangle\,|x_{w-1}\cdots x_1x_0\rangle$ represent the position information after scrambling. According to Eq. (3), the location information of the subblock is that

$$\begin{aligned}
|x'_{q-1}x'_{q-2}\cdots x'_w\rangle &= \text{QArT}(|x_{q-1}x_{q-2}\cdots x_w\rangle) \\
&= (|x_{q-1}x_{q-2}\cdots x_w\rangle \\
&\quad+|y_{q-1}y_{q-2}\cdots y_w\rangle) \bmod 2^{q-w}, \qquad (8)\\
|y'_{q-1}y'_{q-2}\cdots y'_w\rangle &= \text{QArT}(|y_{q-1}y_{q-2}\cdots y_w\rangle) \\
&= (|x_{q-1}x_{q-2}\cdots x_w\rangle \\
&\quad+2|y_{q-1}y_{q-2}\cdots y_w\rangle) \bmod 2^{q-w}. \qquad (9)
\end{aligned}$$

Finally, we restore the subblocks of the transformed image to the original size:

$$|I_{\text{image3}}\rangle = \text{QArT}_{2^q}\,|I_{\text{image2b}}\rangle\,, \qquad (10)$$

where QArT_{2^q} represents scrambling an image of size $2^q\times 2^q$ by using QArT, and I_{image3} represents the transformed image.

Step 4 Use quantum XOR encoding between the original image and the transformed quantum image. According to Ref. [43], it is necessary to divide it into 2^{2n} sub-operations to perform XOR operation on pixel information of each image.

We set sequence $D=\{d_1,d_2,\ldots,d_{2^{2n}}\}$ based on the pixel color information of image $|I_{\text{image1}}\rangle$, where $d_{YX}=m^0_{YX}m^1_{YX}m^2_{YX}m^3_{YX}\ldots m^{23}_{YX}, m^i_{YX}\in[0,1]$, and convert it into an octal sequence. Afterwards, according to the formula and sequence D, generate the consequential quantum operation

$$S_{YX}=Q^0_{YX}Q^1_{YX}Q^2_{YX}Q^3_{YX}\cdots Q^{23}_{YX}, \qquad (11)$$

where 0–7, 8–15, and 16–23, respectively, control the R, G, and B channels, and

$$Q^i_{YX}=X^{m^i_{YX}}=\begin{cases}X, & m^i_{YX}=1\\ I, & m^i_{YX}=0\end{cases}$$

represents X-gate transformation or I-gate transformation.

The XOR operation of pixel values can be achieved through S_{YX}. Construct quantum operation O_{YX} through S_{YX}:

$$O_{YX} = \left(I \otimes \sum_{y=0}^{2^q-1} \sum_{x=0}^{2^q-1} |yx\rangle \langle yx|\right) + S_{YX} \otimes |YX\rangle \langle YX|, \quad (12)$$

where $yx \neq YX$.

Finally, apply O_{YX} to the entire image, and finally get the image $|I_{\text{image4}}\rangle$ after the operation. The integration process is

$$\begin{aligned} O|I_{\text{image4}}\rangle &= \prod_{Y=0}^{2^q-1} \prod_{X=0}^{2^q-1} B_{YX} |I\rangle \\ &= \frac{1}{2^q} \sum_{Y=0}^{2^q-1} \sum_{X=0}^{2^q-1} \otimes_{i=0}^{23} |C_{YX}^i \oplus m_{YX}^i\rangle |YX\rangle \\ &= \frac{1}{2^q} \sum_{Y=0}^{2^q-1} \sum_{X=0}^{2^q-1} |f(Y,X)\rangle |YX\rangle. \end{aligned} \quad (13)$$

Step 5 Put the obtained image $|I_{\text{image4}}\rangle$ into the quantum DNA codec, and use rule 8 to decode the image by inverting all high and low qubits to obtain $|I_{\text{image5}}\rangle$. The encryption process ends

$$|I_{\text{image5}}\rangle = E_{\text{r1,r8}} |I_{\text{image4}}\rangle. \quad (14)$$

3.2. Decryption scheme

Based on the reversibility of quantum circuits, we design a quantum color image decryption technique. The specific steps are as follows:

Step 6 For encrypted image, the preliminary decryption is achieved by utilizing the quantum circuit of DNA codec and analyzing the decoding and encoding processes of rule 8 and rule 1. We perform inverse quantum DNA decoding and inverse XOR encoding operations on the image, as follows:

$$|I_{\text{image3}}\rangle = \text{XOR}^{-1} D_{\text{r8,r1}} |I_{\text{image5}}\rangle. \quad (15)$$

Step 7 Because of the reversible design of quantum circuits, there will be no information loss during the decryption process of images using quantum circuits. Therefore, based on this condition, we perform quantum Arnold inverse transform on the image. The specific process is as follows:

$$|I_{\text{image2}}\rangle = \text{QArT}_{2^q}^{-1} |I_{\text{image3}}\rangle. \quad (16)$$

According to Eqs. (4), (8), and (9), the original coordinates of the pixel positions after inverse transformation can be obtained by

$$\begin{aligned} |x_{\text{oq}}\rangle &= \text{QArT}^{-1} |x'_{\text{oq}}\rangle \\ &= \big(2|x'_{q-1}x'_{q-2}\cdots x'_w\rangle \\ &\quad - |y'_{q-1}y'_{q-2}\cdots y'_w\rangle\big) \bmod 2^{q-w}, \\ |y_{\text{oq}}\rangle &= \text{QArT}^{-1} |y'_{\text{oq}}\rangle \\ &= \big(-|x'_{q-1}x'_{q-2}\cdots x'_w\rangle \\ &\quad + |y'_{q-1}y'_{q-2}\cdots y'_w\rangle\big) \bmod 2^{q-w}. \end{aligned} \quad (17)\ (18)$$

Step 8 Use the decoding of the DNA codec and the inverse operation of rule 4 and 1 to obtain the final decrypted original image:

$$|I_{\text{image1}}\rangle = D_{\text{r4,r1}} |I_{\text{image2}}\rangle. \quad (19)$$

4. Analysis and verification of security

We comprehensively evaluate the effectiveness of encryption and decryption algorithms by using color images such as "Monkey", "Flower", and "House" as the original images for security analysis. The pixel size of each image is 512×512. We use the following indicators to assess the capabilities of encryption algorithms: time complexity analysis, histogram analysis, pixel correlation, key sensitivity analysis, information entropy, and analysis of anti-noise effect.

4.1. Encryption effect

Because there is currently a lack of available quantum devices to actually execute the proposed encryption scheme, we use classic computing environments such as MATLAB and Python to evaluate and verify the ability of the algorithm by simulating the quantum computing. Figure 5 shows the comparison of encryption and decryption effects. By using the proposed algorithm to encrypt plaintext images, the encrypted images cannot see any plaintext information, which proves the feasibility of the technique. Meanwhile, the ciphertext image is decrypted, and through comparison the obtained image is identical to the original image.

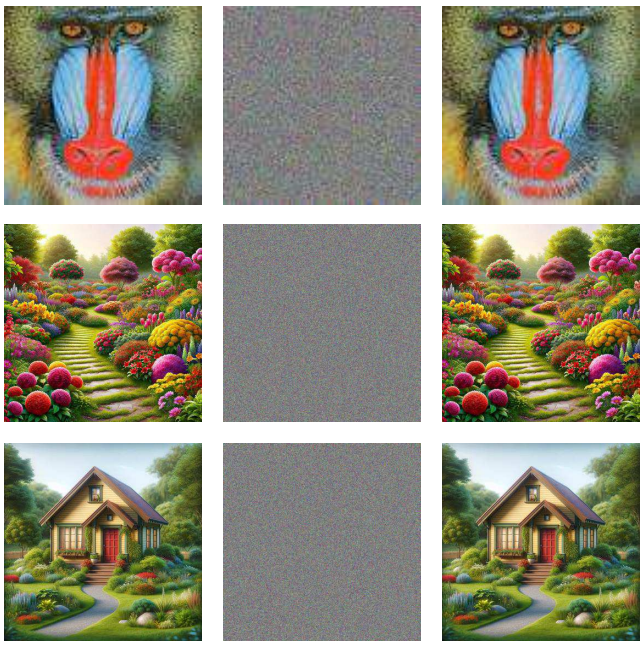


Fig. 5. Analysis of encryption and decryption effects. The three columns represent the encryption and decryption effects of "Monkey", "Flower", and "House", respectively.

4.2. Time complexity analysis

In the process of using DNA codec to realize color information scrambling of quantum image, we process R, G, and B three-channel images respectively, and the time complexity is $O(N \times N)$. After that, QArT is used to realize the scrambling of quantum image position information, and the time complexity is $O(N \times N)$, so the complexity of the whole encryption process is $O(N \times N)$. The key generation time is 0.4521 s.

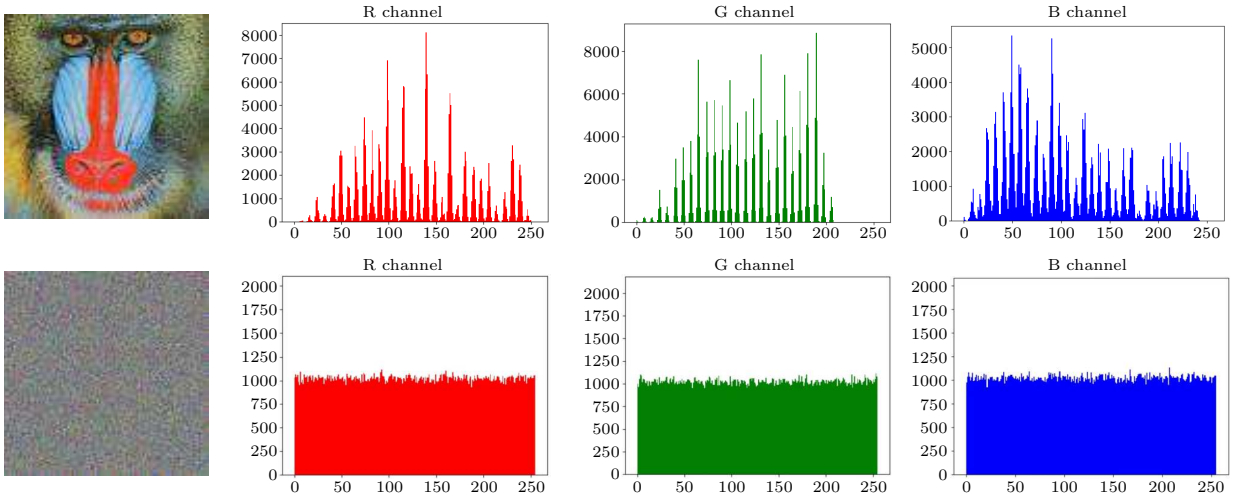


Fig. 6. A comparison of the RGB three-channel histogram of the encrypted "Monkey" image with the plaintext image.

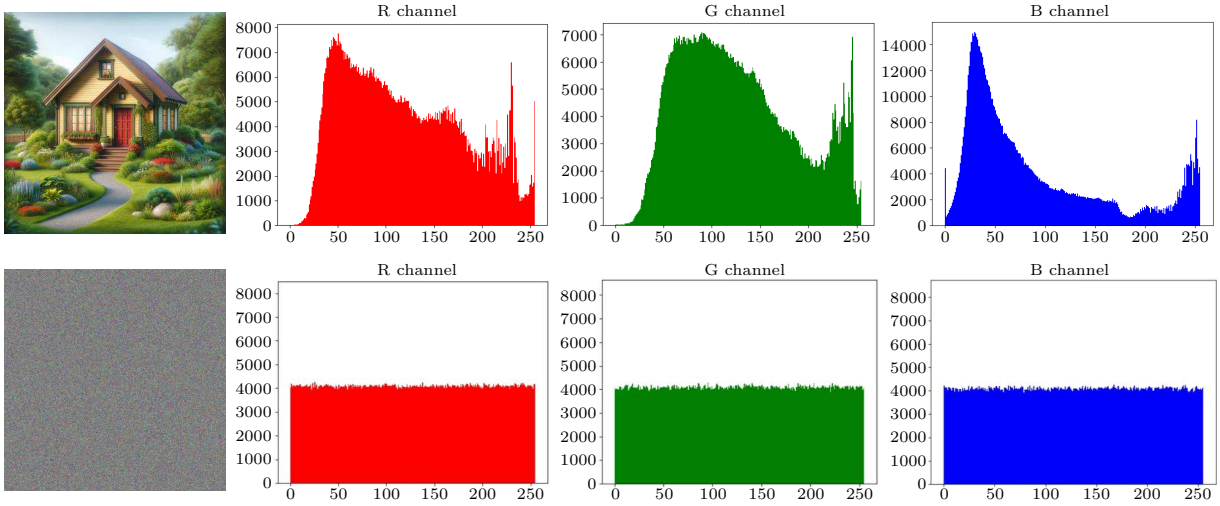


Fig. 7. A comparison of the RGB three-channel histogram of the encrypted "Flower" image with the plaintext image.

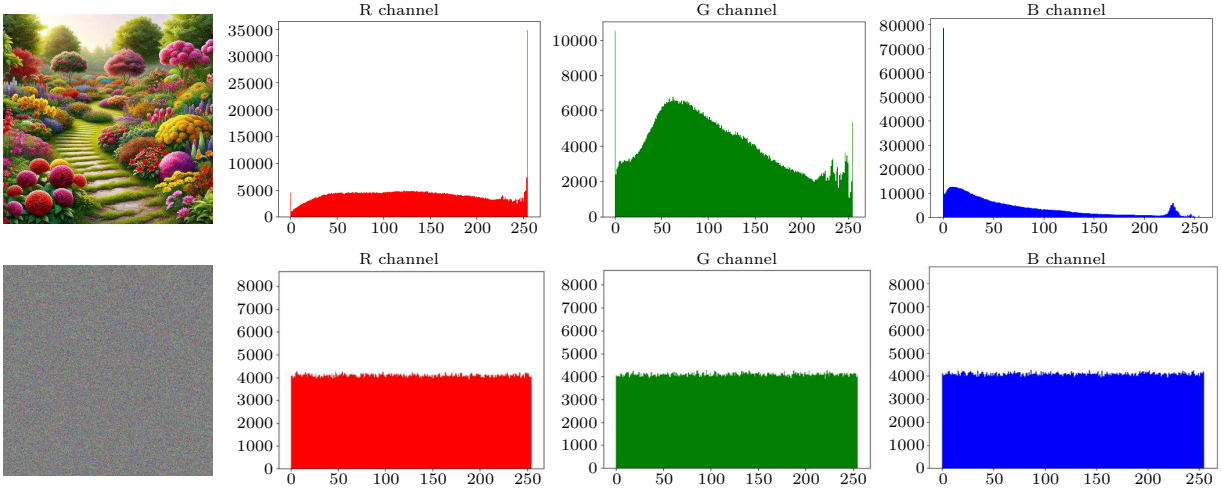


Fig. 8. A comparison of the RGB three-channel histogram of the encrypted "House" image with the plaintext image.

4.3. Histogram analysis

As an important evaluation indicator for the feasibility of encryption algorithms, histograms reflect the pixel intensity distribution of the image. As shown in Figs. 6–8, the original histograms and encrypted histograms of the three images prove that the algorithm successfully blurred the statistical features of different plaintext images after encryption, resulting in similar distributions of peak values on the histogram of their encrypted images. This similarity indicates that the algorithm effectively maintains the overall appearance consistency of the image, making it difficult to easily distinguish different plaintext images through histogram analysis. It effectively resists attacks from external histogram analysis, thereby improving the security of encryption.

4.4. Correlation analysis

To demonstrate that the encryption scheme can decrease the high relevance of contiguous pixels, we selected 3000 sets of contiguous pixels from the horizontal, vertical, and diagonal directions of plaintext and ciphertext images as references to achieve the visualization results of correlation analysis. The specific results are shown in Figs. 9 and 10. We prove the capability of the scheme by computing the relevance coefficient $C_{W,Z}$ of contiguous pixels. The results are shown in Tables 2 and 3. The calculation process of the correlation coefficient is as follows:

$$C_{W,Z} = \frac{\operatorname{cov}(W,Z)}{\sqrt{D(W)D(Z)}}$$

$$= \frac{\frac{1}{Q}\sum_{i=1}^{Q}\left[\left(W_i - E(W)\right)\left(Z_i - E(Z)\right)\right]}{\sqrt{\frac{1}{Q}\sum_{i=1}^{Q}\left(W_i - E(W)\right)^2 \frac{1}{Q}\sum_{i=1}^{Q}\left(Z_i - E(Z)\right)^2}}, \quad (20)$$

where W and Z represent adjacent average pixel values, $E(W)$ and $E(Z)$ represent the average value of adjacent pixels, i.e., $E(W) = \frac{1}{Q}\sum_{i=1}^{Q} P_i$ and $E(Z) = \frac{1}{Q}\sum_{i=1}^{Q} Z_i$, $\operatorname{cov}(W,Z)$ represents the covariance of adjacent pixel values, $D(W)$ and $D(Z)$ represent variance, and Q represents the total logarithm of adjacent pixels.

From Figs. 9 and 10, the encrypted image pixels have almost no correlation. Moreover, Tables 1 and 2 indicate that the plaintext image has high pixel correlation, almost approaching 1, while the ciphertext images are approaching 0. The above results indicate that our algorithm has the ability to resist attacks from correlations.

Table 1. The correlation coefficient in the ciphertext images.

Image	Channel	Horizontal	Vertical	Diagonal
Monkey	R	0.9148	0.8588	0.8462
	G	0.8625	0.7773	0.7525
	B	0.9001	0.8708	0.8400
Flower	R	0.9244	0.9037	0.8752
	G	0.9158	0.8914	0.8605
	B	0.9186	0.8932	0.8653
House	R	0.9631	0.9610	0.9452
	G	0.9605	0.9583	0.9423
	B	0.9753	0.9742	0.9651

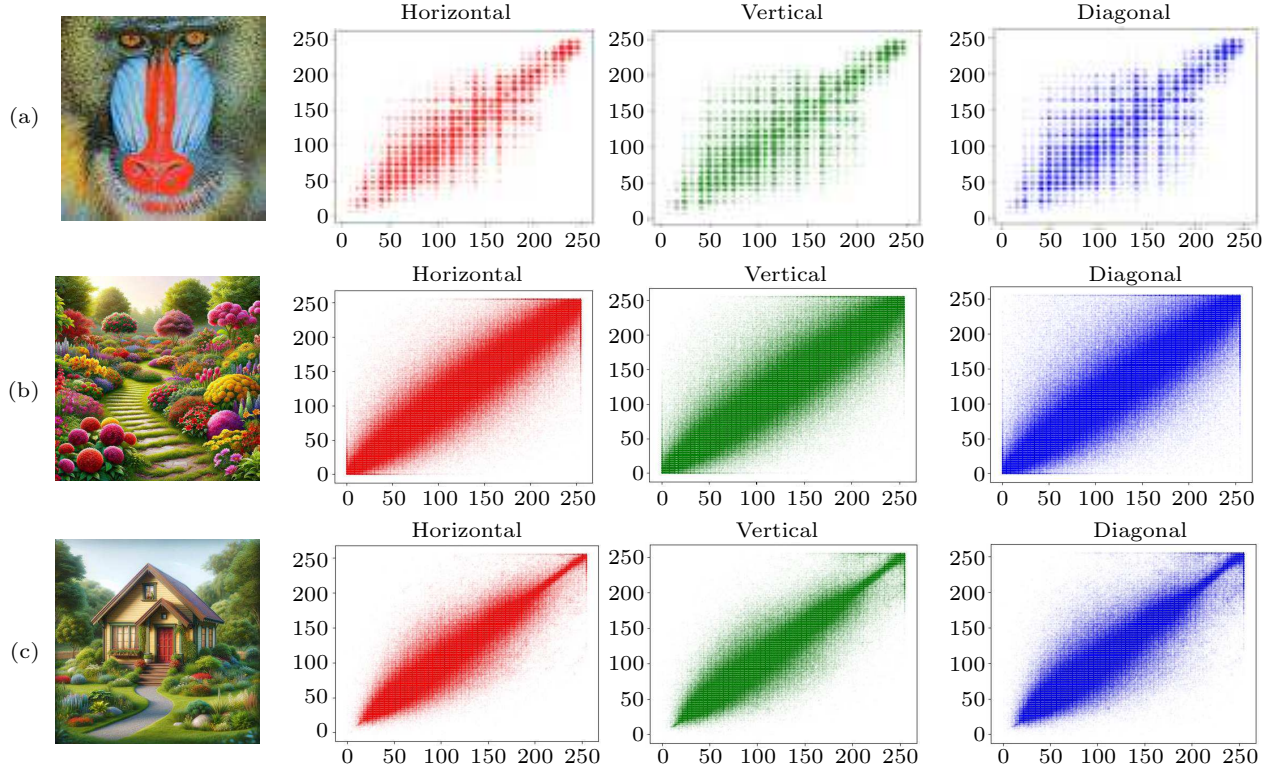


Fig. 9. (a) The relevance of plaintext image "Monkey", (b) the relevance of plaintext image "Flower", and (c) the relevance of plaintext image "House".

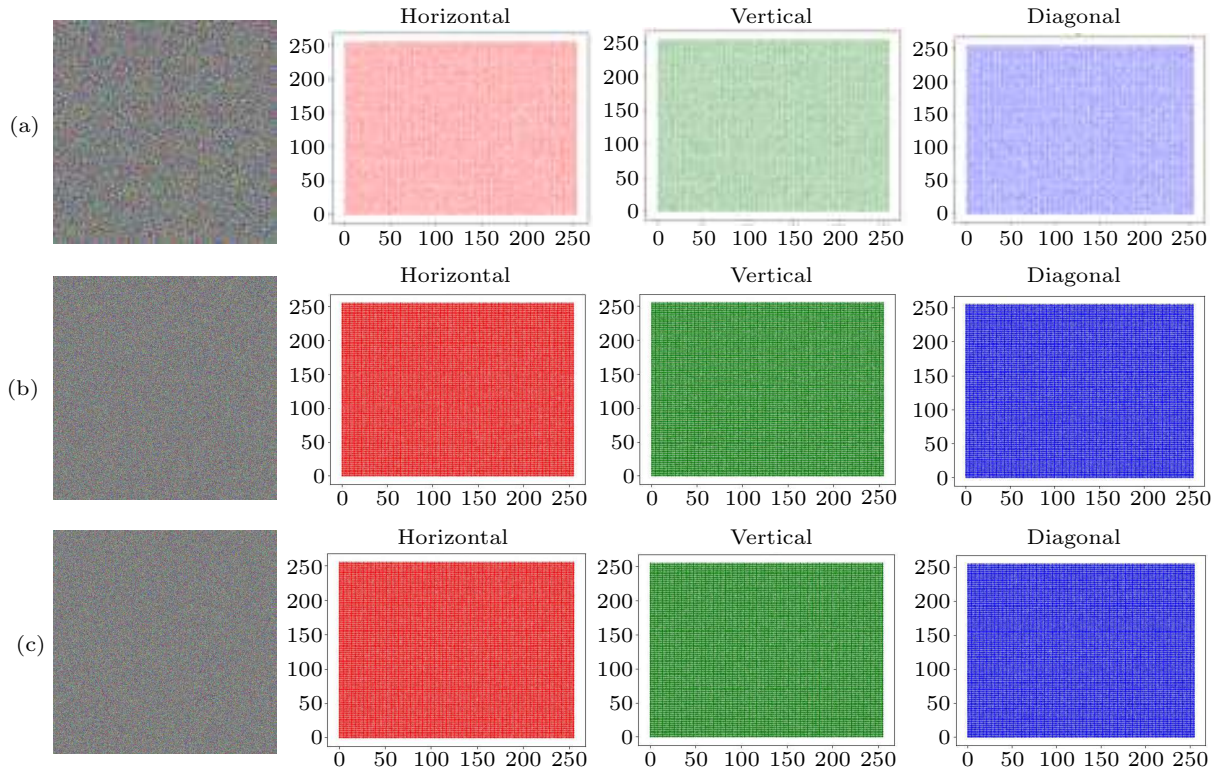


Fig. 10. (a) The relevance analysis of the cryptographic image "Monkey", (b) the correlation analysis of the cryptographic image "Flower", (c) the correlation analysis of the encrypted cryptographic image "House".

Table 2. The correlation coefficient in plaintext images.

Image	Channel	Horizontal	Vertical	Diagonal
Monkey	R	−0.0151	−0.0029	−0.0061
	G	0.0248	−0.0003	0.0077
	B	0.0063	0.0347	0.0098
Flower	R	0.0024	−0.0027	0.0003
	G	−0.0085	0.0161	−0.0119
	B	−0.0012	0.0167	0.0279
House	R	0.0010	−0.0034	−0.0026
	G	0.0033	0.0154	−0.0051
	B	-0.0141	0.0173	−0.0107

Table 3. The NPCR and UCAI of cryptographic images.

Image	Channel	NPCR (%)	UCAI (%)
Monkey	R	99.6082	33.0673
	G	99.6078	33.5795
	B	99.6094	33.6274
Flower	R	99.6065	33.4045
	G	99.6099	33.5298
	B	99.6102	33.3976
House	R	99.6047	33.4903
	G	99.6133	33.4306
	B	99.6094	33.1811

4.5. Key sensitivity analysis

We obtain the key sensitivity of the image by calculating normalized pixel change rate (NPCR) and uniform average change intensity (UACI) between the plaintext and cryptographic images to obtain key sensitivity of the image. The process follows

$$\begin{cases} \text{NPCR} = \frac{\sum_{\omega,\tau} T(\omega,\tau)}{H\times K} \times 100\%, \\ \text{UACI} = \frac{1}{H\times K} \frac{\sum(C_1(\omega,\tau)-C_2(\omega,\tau))}{255} \times 100\%, \end{cases} \tag{21}$$

where H represents the height of the image, K represents the width, and the value of $T(\omega,\tau)$ is 0 or 1, which is represented as follows:

$$T(\omega,\tau) = \begin{cases} 1, & C_1(\omega,\tau) \neq C_2(\omega,\tau), \\ 0, & \text{otherwise}, \end{cases} \tag{22}$$

where $T(\omega,\tau)$ represents the pixel value at position (ω,τ), and C_1 and C_2 are images encrypted with different keys.

Table 4. The NPCR and UCAI of different schemes.

Schemes	NPCR (%)	UCAI (%)
Ours	99.61	33.41
Only DNA codec	98.69	30.41
Only QArT	99.27	31.58
Ref. [44]	99.61	31.60
Ref. [45]	99.63	31.46
Ref. [46]	99.57	35.08
Ref. [47]	99.57	33.38

Ideally, when NPCR approaches 99.6094% and UCAI approaches 33.4635%, the key sensitivity of the image becomes stronger. Table 3 shows the average NPCR and UCAI of images before and after encryption. Meanwhile, on the premise of ensuring the same image size, we conduct comparative experiments on our encryption scheme with other schemes. The results are shown in Table 4. Tables 3 and 4 prove that our encryption scheme has better performance and stronger confi-

dentiality.

4.6. Information entropy

In the field of image encryption, pixel values can be used as random variables, and information entropy can measure the uncertainty of pixel value distribution based on pixel values. In general, the uniformity of pixel distribution in the three channels of encrypted images directly affects the capability of the encryption algorithm. The calculation formula is as follows:

$$E(\ell) = -\sum_{i=1}^{Q} P(\ell_i)\log_2 P(\ell_i), \tag{23}$$

where $P(\ell_i)$ is the probability that ℓ takes value ℓ_i, and the perfect value of $E(\ell)$ is 8.[48] Table 5 indicates the information entropy of "Monkey", "Flower", and "House", the average value of all cryptographic images is about 7.9992, which fully verifies the capability of the algorithm.

Table 5. Information entropy of cryptographic image.

Image	Channel R	Channel G	Channel B
Monkey	7.9994	7.9991	7.9992
Flower	7.9990	7.9994	7.9993
House	7.9993	7.9991	7.9994

4.7. Analysis of anti-noise effect

In the real environment, the influence of environmental factors or external attackers will add interference in the process of image information transmission, resulting in noise, which will affect the effect of image decryption. Therefore, the detection of image anti-noise ability is a vital index to measure the robustness of the encryption algorithm.

In this paper, "House" image and "Flower" image are taken as examples, and salt and pepper noise and Gaussian noise of different degrees are added to the two encrypted images, respectively, to simulate the real environment or attack. We add salt and pepper noise levels of 0.05, 0.10, and 0.15 to the cryptographic image of "House". At the same time, Gaussian noise is added to the encrypted "Flower" image, where the values of var are 0.10, 0.15, and 0.20, respectively. In addition, we carry out clipping attack on the encrypted image, and test the anti-clipping performance of the proposed algorithm. The final generated cryptographic image is decrypted, and the results are shown in Fig. 11, which prove that the proposed encryption algorithm has the advantage of high robustness.

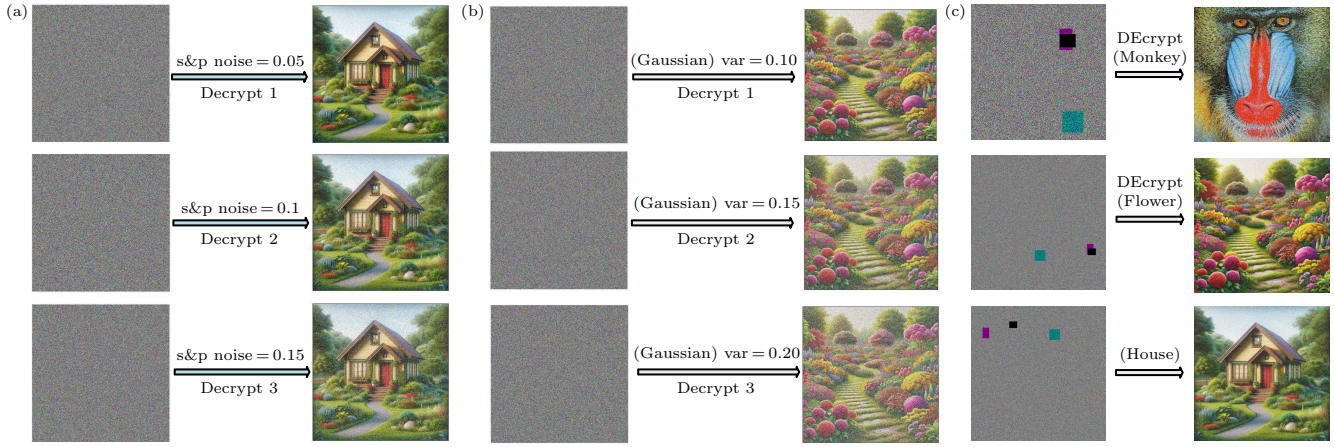


Fig. 11. (a) The encryption effect of "House" image under the influence of different s&p noises. (b) The encryption effect of "Flower" image under the influence of different Gaussian noises. (c) The decryption result of three color images under cropping attack.

5. Conclusion

In this paper, we propose a quantum color image encryption algorithm that combines DNA codecs and QArT, and have successfully achieved double scrambling of color and position, which greatly improves the encryption efficiency. Afterwards, we conduct comparative analysis experiments on the plaintext image and the ciphertext image from six aspects: time complexity analysis, histogram, correlation, key sensitivity, information entropy, and analysis of anti-noise effect. The simulation verifies that the proposed algorithm has better encryption performance, strong robustness, and security. In the future, we will work hard to improve and research encryption algorithms to improve the algorithm's performance and encryption efficiency.

Acknowledgments

Project supported by the Natural Science Foundation of Shandong Province, China (Grant No. ZR2021MF049), Joint Fund of Natural Science Foundation of Shandong Province (Grant Nos. ZR2022LLZ012 and ZR2021LLZ001), and the Key R&D Program of Shandong Province, China (Grant No. 2023CXGC010901).

References

[1] Nagarajan S M, Deverajan G G, Kumaran U, Thirunavukkarasan M, Alshehri M D and Alkhalaf S 2021 *IEEE Transactions on Industrial Informatics* **18** 12

[2] Chen H C, Guo J I, Huang L C and Yen J C 2003 *EURASIP Journal on Advances in Signal Processing* **2003** 902741

[3] Chinnasamy C 2018 *Ingenierie des Systemes d'Information* **23** 6

[4] Pourasad Y, Ranjbarzadeh R and Mardani A 2021 *Entropy* **23** 341

[5] Arab A, Rostami M J and Ghavami B 2019 *The Journal of Supercomputing* **75** 6663

[6] Zhang Y 2020 *Information Sciences* **520** 177

[7] Parvaz R and Zarebnia M 2018 *Opt. Laser Technol.* **101** 30

[8] Xu Q, Sun K, He S and Zhu C 2020 *Opt. Lasers Eng.* **134** 106178

[9] Wang Z, Xu M and Zhang Y 2022 *Arch. Comput. Methods Eng.* **29** 737

[10] Yao X W, Wang H, Liao Z, Chen M C, Pan J, Li J, Zhang K C, Lin X C, Wang Z H, Luo Z H, Zheng W Q, Li J D, Zhao M S, Peng X H and Suter D 2017 *Phys. Rev. X* **7** 031041

[11] Cai Y, Lu X and Jiang N 2018 *Chin. J. Electron.* **27** 718

[12] Zhao R, Cheng T, Wang R, Fan X and Ma H 2024 *New J. Phys.* **26** 053016

[13] Wang H, Xue Y, Qu Y, Mu, X and Ma H 2022 *npj Quantum Information* **8** 134

[14] Adleman L M 1994 *Science* **266** 1021

[15] Chang W L, Guo M and Ho M S H 2005 *IEEE Transactions on Nanobioscience* **4** 149

[16] Ning K 2012 *Computers & Electrical Engineering* **38** 1240

[17] Huang X and Ye G 2018 *Multimedia Tools and Applications* **72** 57

[18] Ur Rehman A, Liao X, Ashraf R, Ullah S, and Wang H 2018 *Optik* **159** 348

[19] Imre S 2014 *Computers & Electrical Engineering* **40** 134

[20] Gupta M,and Nene M J 2020 *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)* pp. 1

[21] Abura'ed N, Khan F S and Bhaskar H2017 *ACM Computing Surveys (CSUR)* **49** 1

[22] Farhi E and Neven H 2021 *International Journal of Theoretical Physics* **60** 2930

[23] Hu W W, Zhou R G, Luo J, Jiang S X and Luo G F 2021 *Quantum Inf. Process.* **19** 1

[24] Liu X, Xiao D, Huang W and Liu C 2019 *IEEE Access* **7** 57188

[25] Guo L, Du H and Huang D 2022 *Quantum Inf. Process.* **21** 20

[26] Le P Q, Dong F and Hirota K 2011 *Quantum Inf. Process.* **10** 63

[27] Zhang Y, Lu K, Gao Y and Wang M 2013 *Quantum Inf. Process.* **12** 2833

[28] Zhang Y, Lu K, Gao Y and Xu K 2013 *Quantum Inf. Process.* **12** 3103

[29] Sun B, Iliyasu A, Yan F, Dong F and Hirota K 2021 *J. Adv. Comput. Intell. Intell. Inform* **17** 3

[30] Li H S, Zhu Q, Zhou R G, Song L and Yang X J 2014 *Quantum Inf. Process.* **13** 991

[31] Hao W, Zhang T, Chen X and Zhou X 2023 *Signal Processing* **105** 108890

[32] Liu X 2023 *Physica Scripta* **98** 115112

[33] Zhu H H, Chen X B and Yang Y X 2021 *Quantum Inf. Process.* **20** 315

[34] Li H S, Li C, Chen X and Xia H Y 2018 *International Journal of Theoretical Physics* **57** 3745

[35] Jiang N, Wu W Y and Wang L 2014 *Quantum Inf. Process.* **13** 1223

[36] Jiang N, Wang L and Wu W Y 2014 *International Journal of Theoretical Physics* **53** 2463

[37] Jin C and Liu H 2017 *Int. J. Netw. Secur* **19** 347

[38] Zhao J, Zhang T, Jiang J, Fang T and Ma H 2022 *Scientific Reports* **12** 14253

[39] Zhu H, Chen Z and Leng T 2024 *J. Appl. Phys.* **135** 014401

[40] Wei X, Guo L, Zhang Q, Zhang J and Lian S2012 *Journal of Systems and Software* **85** 290

[41] Sharma N, Jain V and Mishra A 2018 *Journal of Systems and Software* **132** 377

[42] Gao J, Wang Y, Song Z and Wang S 2023 *Entropy* **25** 865

[43] Gong L H, He X T, Cheng S, Hua T X and Zhou N R 2016 *International Journal of Theoretical Physics***55** 3234

[44] Rajakumaran C and Kavitha R 2020 *Multimedia Tools and Applications* **79** 23849

[45] Abd El-Latif A A, Abd-El-Atty B and Talha M 2017 *IEEE Access* **6** 1073

[46] Abanda Y and Tiedeu A 2016 *IET Image Processing* **10** 742

[47] Li C and Yang X 2022 *Optik* **260** 169042

[48] Kumari M, Gupta S and Sardana P 2017 *3D Research* **8** 37