scientific reports

Check for updates

OPEN

Color image encryption scheme based on alternate quantum walk and controlled Rubik's Cube

Jingbo Zhao[1], Tian Zhang[1], Jianwei Jiang[1,3], Tong Fang[1,3] & Hongyang Ma[2]✉

Aiming at solving the trouble that digital image information is easily intercepted and tampered during transmission, we proposed a color image encryption scheme based on alternate quantum random walk and controlled Rubik's Cube transformation. At the first, the color image is separated into three channels: channel R, channel G and channel B. Besides, a random sequence is generated by alternate quantum walk. Then the six faces of the Rubik's Cube are decomposed and arranged in a specific order on a two-dimensional plane, and each pixel of the image is randomly mapped to the Rubik's Cube. The whirling of the Rubik's Cube is controlled by a random sequence to realize image scrambling and encryption. The scrambled image acquired by Rubik's Cube whirling and the random sequence received by alternate quantum walk are bitwise-XORed to obtain a single-channel encrypted image. Finally the three-channel image is merged to acquire the final encrypted image. The decryption procedure is the reverse procedure of the encryption procedure. The key space of this scheme is theoretically infinite. After simulation experiments, the information entropy after encryption reaches 7.999, the NPCR is 99.5978%, and the UACI is 33.4317%. The encryption scheme with high robustness and security has a excellent encryption effect which is effective to resist statistical attacks, force attacks, and other differential attacks.

As multimedia technology is growing well today, an increasing number of fields are gradually developing in the direction of digitization and informatization, which has brought convenience to our lives and work. However, the security and confidentiality of data in the process of information transmission are becoming more and more important image plays. As one of the important carriers in the process of information transmission, digital images play a pivotal role in many fields, such as education, finance, medical treatment and so on. However, digital images are easily intercepted and tampered during transmission, which greatly threatens the privacy of image information[1–4]. In view of the security of digital images, many domestic and foreign researchers have brought forward various image encryption methods. For example, digital image encryption schemes are based on chaotic systems[5–8], which control the placement of image pixels by generating random sequences through the chaotic system. Based on digital image encryption schemes such as Fourier Transform[9,10], the image is transformed into the frequency domain, and then the amplitude value of the sine and cosine function of each frequency in the frequency domain is operated to realize image encryption; there are also classical digital image encryption methods, such as: Arnold transformation[11–14], AES transformation[15–18], DNA encoding encryption[19–25], etc. Based on the alternate quantum random walk and controlled Rubik's Cube transform, this paper comes up with a novel digital image encryption scheme. And the encryption algorithm designed by him makes full use of the characteristics of quantum random walk, which has the advantages of large key space and key sensitivity.

With the continuous development of quantum computing and quantum communication, many quantum algorithms and quantum technologies have emerged[26–34]. Quantum random walk is generated by applying classical random walk to quantum computing, and it plays an important part in a number of quantum algorithms[35–38]. Compared with classical random walking, quantum random walk has two main advantages, one is fast running speed, and the other is strong security. Similar to chaotic systems, quantum random walk has many excellent properties: sensitivity to initial values, stability, non-periodicity, etc. Thence, the key space of quantum random walk is very vast, and it has a perfect capability to resist external malicious attacks. Therefore, quantum random walk is very advantageous in the field of image encryption. Wang et al. designed an image encryption algorithm that combines quantum random walk with DNA encoding[19]. Based on quantum random walk and double random phase encoding technology, Abd-El-Atty et al. put forward an image encryption scheme[39].

[1]School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266000, China. [2]School of Science, Qingdao University of Technology, Qingdao 266000, China. [3]These authors contributed equally: Jianwei Jiang and Tong Fang. ✉email: hongyang_ma@aliyun.com

Based on quantum walk Abd-El-Atty et al. conducted in-depth research and proposed multiple algorithms for image encryption combined with classical algorithms[45–47]. MA et al. designed an image encryption scheme that combines alternating quantum random walk with discrete cosine transform, which makes full use of the characteristics of quantum random walk, which has the advantages of large key space and key sensitivity.

The principle of Rubik's Cube transformation is inspired by Rubik's Cube. The Rubik's Cube is to change the position of the sub-block by moving the sub-blocks, so as to realize the scrambling of the Rubik's Cube. Similarly, applying the Rubik's Cube transformation to image scrambling is to scramble the image by moving the position of the image pixels[40–44]. For a third-order Rubik's Cube, if a certain layer is rotated 90 degrees at a time, there are eighteen ways for rotation. There are several ways of permutation and combination of a 3rd-order Rubik's Cube, but it is the only way to restore, so the computational complexity is very high. Thus it is feasible to combine the Rubik's Cube transformation with the image encryption. Zhang et al. proposed an image encryption scheme based on Rubik's Cube transformation and chaotic sequence[41]. Loukhaoukha et al. designed an image encryption method based on the Rubik's Cube rotation principle[43], and using the principle of Rubik's cube rotation, this encryption algorithm can scramble and encrypt the image very well, but its key space is small. At first, the original image was scrambled by using the Rubik's Cube principle, and then the rows and columns of the scrambled image were XORed with the key. Vidhya et al. designed a chaotic image encryption algorithm based on Rubik's Cube transformation and prime number decomposition algorithm[44], and the proposed method makes full use of the Rubik's cube principle to achieve bit-level image encryption, and has a good scrambling effect. I think that if we can add pixel space scrambling, it will achieve a better encryption effect.

This article combines quantum random walk with Rubik's Cube transformation to complete the encryption of digital images. Firstly, a random sequence is generated by quantum walking. Then the random sequence is used to control the magic cube transform to achieve the purpose of image scrambling. The full text of this article is structured as follows: The second part introduces the relevant knowledge needed in the paper. Next part introduces the principles and processes of image encryption and decryption. The Fourth part presents the simulation results and the analysis of the simulation results. Finally, we draw a conclusion about the scheme.

Principle

Alternate quantum walks. Quantum walk can be separated into two parts: One is discrete time quantum random walk and the other is continuous time quantum random walk. We focus on the former way of random walking in this paper.

Similar to the classic random walk, quantum walk is mainly composed of coin register (coin space $\mathcal{H}^c$) and rambler location information (rambler's location space $\mathcal{H}^l$).Therefore, the quantum walk is carried out in Hilbert space $\mathcal{H} = \mathcal{H}^C \otimes \mathcal{H}^P$. The process of quantum random walk is separated into two steps. The first step is to apply the coin operator on the coin state of the two-dimensional Hilbert space $\mathcal{H}^c$, and then apply the unitary operator $\hat{U}$ to the total Hilbert space $\mathcal{H}$. Thus the quantum also can be seen as the application of a unitary operator U that acts repeatedly on the quantum walk system and the operator can be descried as:

$$\hat{U} = SC = S(\hat{C} \otimes I) \tag{1}$$

Assume that the quantum walk coin operator always chooses the same operator$\hat{C}$:

$$\hat{C} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \tag{2}$$

when $\alpha = \frac{\pi}{4}$. the coin operator can be expressed as:

$$\hat{C} = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = H \tag{3}$$

The transfer operator S is used in quantum walks to manipulate the walker to decide the direction of the next walk. When the condition of coin state is $|0\rangle$ (spin up$|\uparrow\rangle$), the walker will move forward in a certain direction. While the condition of coin state is $|1\rangle$ (spin down$|\downarrow\rangle$), the walker will take one step further in the opposite direction. So the transfer operator $\mathcal{S}$ can be denoted as:

$$S = |0\rangle\langle 0| \otimes |n+1\rangle\langle n| + |1\rangle\langle 1| \otimes |n-1\rangle\langle n| \tag{4}$$

In the alternate quantum walk, it is formed by the position state tensor$\{|\mathbf{x}, \mathbf{y}\rangle, x, y \in Z\}$, walking alternately in two directions in a two-dimensional space. Therefore, in the quantum random walk process, the unitary operator repeatedly acting on the quantum walk system can be denoted as:

$$\hat{U} = \hat{S}_y(I \otimes \hat{C})\hat{S}_x(I \otimes \bar{C}) = \hat{S}_y(I \otimes H)\hat{S}_x(I \otimes H) \tag{5}$$

$$\begin{aligned} \hat{S}_y = &|0\rangle\langle 0| \otimes \sum_{m,n \in Z} |n+1, m\rangle\langle n, m| \\ &+ |1\rangle\langle 1| \otimes \sum_{m,n \in Z} |n-1, m\rangle\langle n, m| \end{aligned} \tag{6}$$

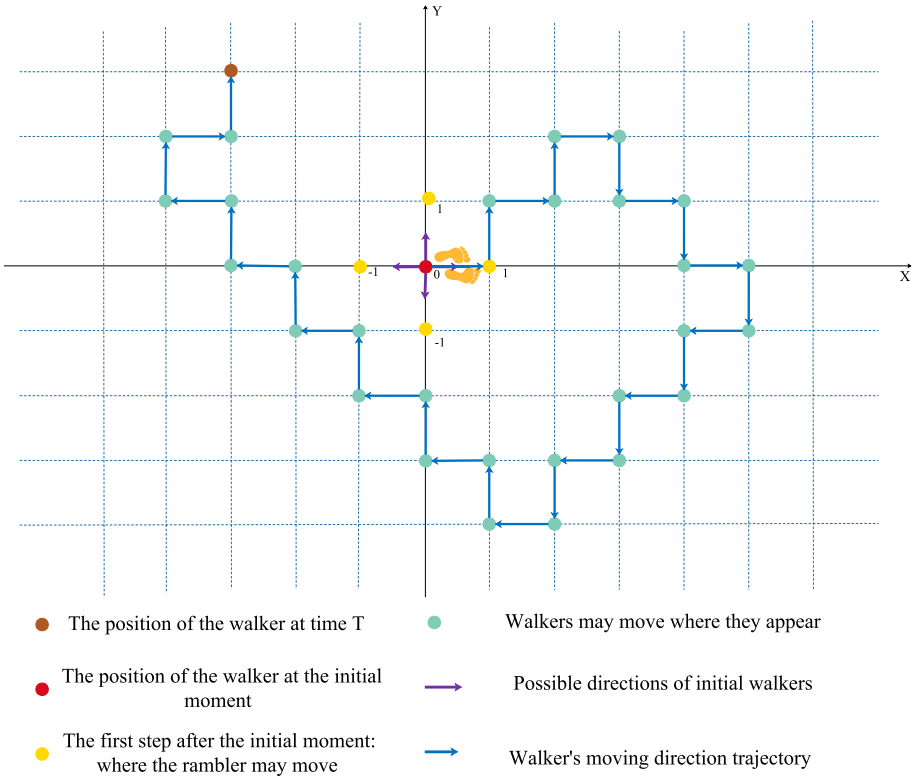

Figure 1. Alternate quantum walk.

$$\begin{aligned}\hat{S}_x =& |0\rangle\langle 0| \otimes \sum_{m,n\in Z} |n, m+1\rangle\langle n, m| \\ &+ |1\rangle\langle 1| \otimes \sum_{m,n\in Z} |n, m-1\rangle\langle n, m|\end{aligned} \tag{7}$$

When the coin state is $|0\rangle$ ($|1\rangle$), act on the walker to walk up (down) along the Y axis , and act on the walker to make it walk right (to the left) along the X axis as shown in Fig. 1. Assuming that the walker is locally at the initial moment $(y, x) = (0, 0)$, the initial state of the coin state is a superposition state $|\text{coin}\rangle = a|0\rangle + b|1\rangle$, and the quantum state of the initial quantum walk can be expressed as:$|\psi_0\rangle = |00\rangle \otimes |\text{ coin }\rangle$. Here, after walking N steps, the final quantum state of the entire system is$|\psi_N\rangle = \hat{U}^N|\psi_0\rangle$, The probability that the walker is at the location(y, x) is:

$$P_{Y,X} = \sum \left|\left\langle y, x, 0 \middle| \hat{U}^N \middle| \psi_0 \right\rangle\right|^2 + \sum \left|\left\langle y, x, 1 \middle| \hat{U}^N \middle| \psi_0 \right\rangle\right|^2 \tag{8}$$

Rubik's Cube transform. The concept of Rubik's Cube transformation comes from Rubik's Cube toys, which disrupt the patterns on the surface of the Rubik's Cube by rotating the cubes. The algorithm in this paper is based on the third-order Rubik's Cube. The third-order Rubik's Cube is a special cube that is composed of 26 sub-blocks and can be rotated along each axis. The six faces of the Rubik's Cube have different colors.

For a 3rd-order Rubik's Cube, we firstly determine the representation of the six faces of the Rubik's Cube, and mark each sub-block of the Rubik's Cube. Third-order Rubik's Cube expansion map is displayed in Fig. 2, the top side is represented as U, the front side is represented as F, the right side is represented as R, the bottom side is represented as D, the back side is represented as B, and the left side is represented as L. Because U surface and D surface, R surface and L surface, and F surface and B surface are relative, we only consider the three surfaces: U, R, and F. For example, when the first layer of the U side of the Rubik's Cube is rotated 90° to the right, the state of the Rubik's Cube is demonstrated in Fig. 2. And the U surface is rotated 90° counterclockwise, while the D surface does not change. When the middle layer of the U side of the Rubik's Cube is rotated 90 degrees, the middle layers of the four sides of F, R, B, and L are also cyclically shifted, while the U and D surfaces do not change. Similarly, the same principle applies to rotating other surfaces.

Through the above principles, rotating the Rubik's Cube can be pieced together into a specific pattern, or the specific pattern can be messed up. We apply the theory of Rubik's Cube transformation to image encryption. The pixels of the image are mapped to the Rubik's Cube, and a sub-block of the Rubik's Cube is regarded as a pixel on the image. According to the principle of Rubik's Cube transformation and a specific whirling rule, the pixel

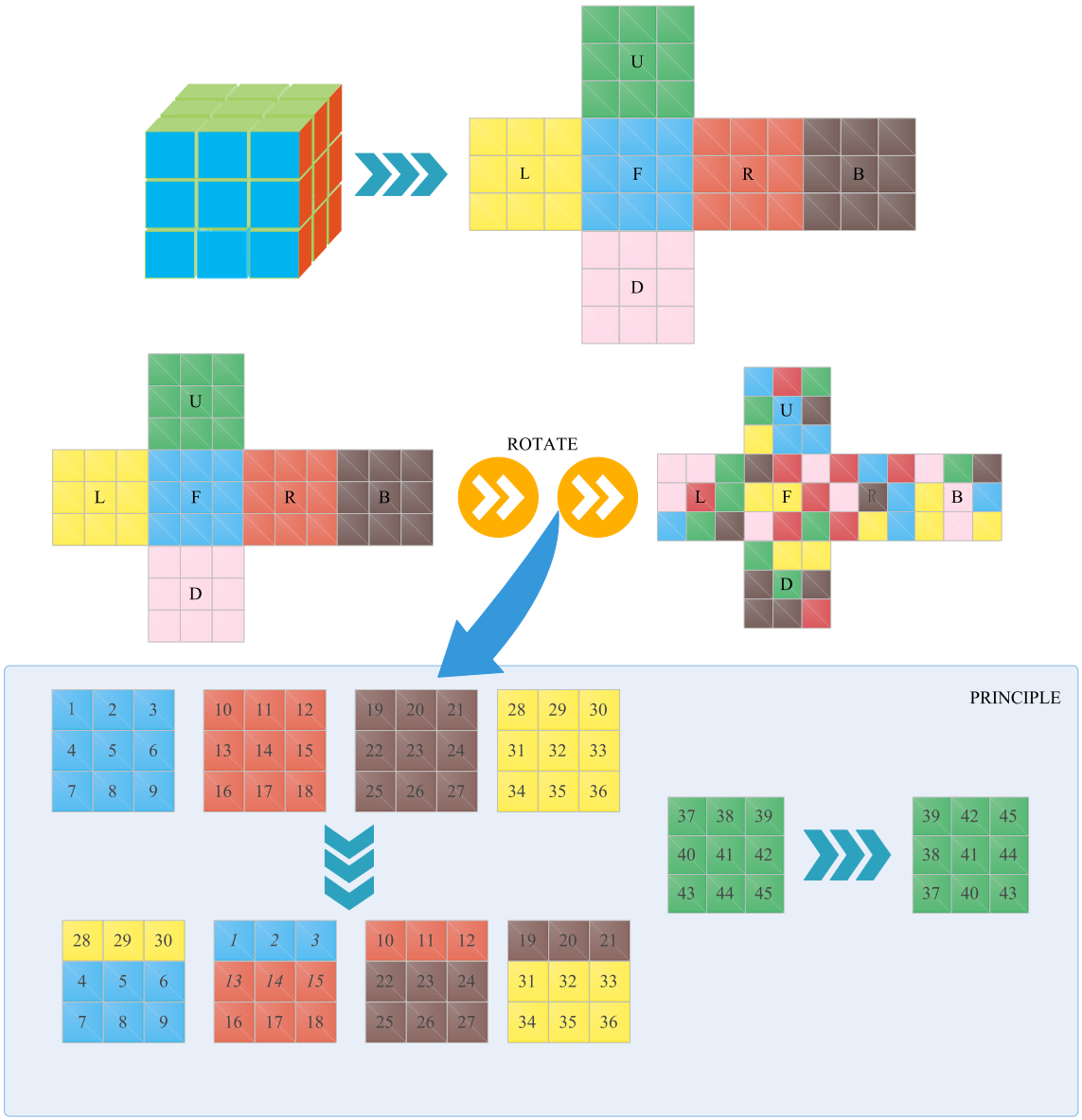

Figure 2. Third-order Rubik's Cube principle. The upper part is the expansion diagram of the Rubik's Cube, the middle is the Rubik's Cube rotation, and the lower layer is the basic Rubik's Cube rotation principle.

position of the original image is shuffled to generate an irregular image. The recipient can use the key to decrypt the encrypted image to acquire the original image. Therefore, the privacy and security of image information in the transmission process can be improved.

Principle of encryption and decryption

In this paper, a random probability matrix is generated by alternating quantum walks and transformed an one-dimensional sequence,the rotation of the Rubik's Cube is controlled by this sequence. Through rotation, the scrambling image is XORed with the matrix converted from the random probability matrix to obtain the encrypted image.

Encryption algorithm. The random sequence can be obtained through quantum walk, which makes the image difficult to be eavesdropped on. Therefore the scheme has good security. The detailed steps of the encryption algorithm are as follows (Fig. 3 is the encryption flowchart):

Step 1: Enter the image $\mathcal{I}$ to be encrypted, analyze the image information, especially the size information$\mathcal{I}(m, n, 3)$. Split the original color image $\mathcal{I}(m, n, 3)$ into $\mathcal{R}(m, n)$, $\mathcal{G}(m, n)$, $\mathcal{B}(m, n)$ three-channel images and represent them in a pixel matrix:

$$\mathcal{I}(m, n, 3) = [\mathcal{R}(m, n), \mathcal{G}(m, n), \mathcal{B}(m, n)] \tag{9}$$

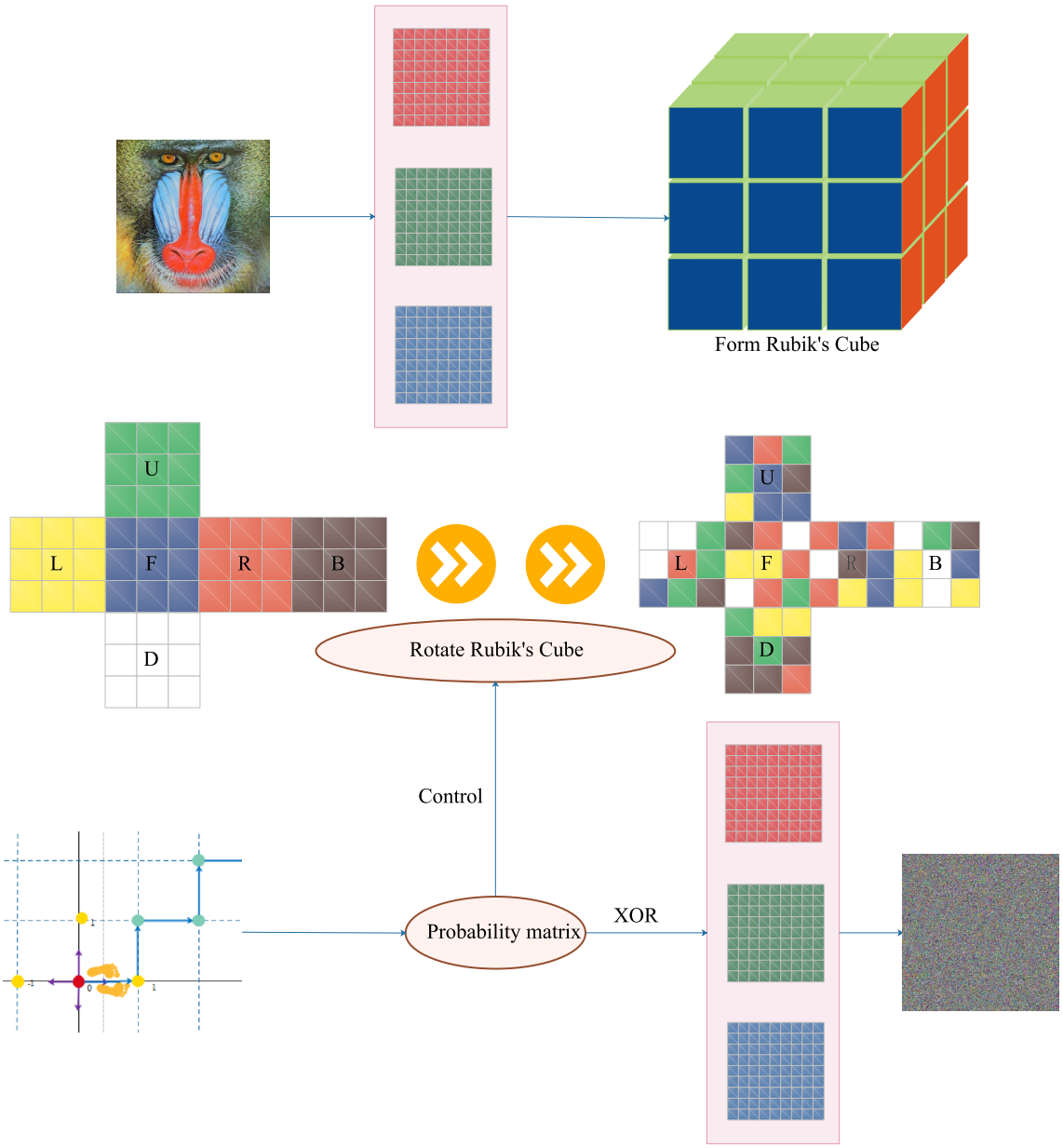

Figure 3. Encryption flowchart. Separate the three channels, select pixels to form a Rubik's Cube, use alternate quantum walks to control the Rubik's cube rotation, scramble and encrypt, merge the three channels to get an encrypted image.

Step 2: Select the parameters (N_1, N_2, a, b) of the alternate quantum walk, walk $\mathcal{N}$ steps on the initial state ψ_0, and generate a probability distribution matrix: $P_{y,x}$ of size(m, n):

$$P_{Y,X} = \sum \left| \left\langle y, x, 0 \middle| \hat{U}^N \middle| \psi_0 \right\rangle \right|^2 + \sum \left| \left\langle y, x, 1 \middle| \hat{U}^N \middle| \psi_0 \right\rangle \right|^2 \tag{10}$$

Step 3: Divide the single-channel image into 6 parts without superimposition to obtain 6 sub-images of different matrices, and treat the 6 matrices as 6 faces of the Rubik's Cube-front (F), back (B), and top (U) , Bottom surface (D), left side (L), right side (R):

$$I = (F, B, U, D, L, R) \tag{11}$$

Step 4: Take out the $3 * 3$ pixel matrix from the six matrices to form six faces and form a 3rd-order cube cube, and the surface has 54 pixel values, so the image can produce a cube.
Step 5: Obtain the random probability matrix $P_{y,x}$ through the discrete time alternate quantum walk, and convert it to an integer value of [0–17] and use it to represent the rotation method as shown in Table 1:

Method	Direction	Affected four faces	Surface affected by rotation
U1	Clockwise	F R B L	U
U2	Clockwise	F R B L	NULL
U3	Clockwise	F R B L	D
L1	Clockwise	F D B U	L
L2	Clockwise	F D B U	NULL
L3	Clockwise	F D B U	R
F	Clockwise	U R B L	F
F2	Clockwise	U R B L	NULL
F3	Clockwise	U R B L	B
U1'	Counterclockwise	F R B L	U
U2'	Counterclockwise	F R B L	NULL
U3'	Counterclockwise	F R B L	D
L1'	Counterclockwise	F D B U	L
L2'	Counterclockwise	F D B U	NULL
L3'	Counterclockwise	F D B U	R
F1'	Counterclockwise	U R B L	F
F2'	Counterclockwise	U R B L	NULL
F3'	Counterclockwise	U R B L	B

Table 1. Third-order Rubik's Cube rotation. U1: Rotate the first layer from top to bottom. U2: Rotate the second layer from top to bottom. U3: Rotate the third layer from top to bottom. L1: Rotate the first layer from left to right. L2: Rotate the second layer from left to right. L3: Rotate the third layer from left to right. F1: Rotate the first layer from front to back. F2: Rotate the second layer from front to back. F3': Rotate the third layer from front to back. U1': Rotate the first layer from top to bottom. U2': Rotate the second layer from top to bottom. U3': Rotate the third layer from top to bottom. L1': Rotate the first layer from left to right. L2': Rotate the second layer from left to right. L3': Rotate the third layer from left to right. F1': Rotate the first layer from front to back. F2': Rotate the second layer from front to back. F3': Rotate the third layer from front to back.

$$K = fix\left(P_{y,x} \times 10^{16}\right) \bmod 18 \tag{12}$$

Step 6: Rotating the Rubik's Cube, dividing the sequence obtained in discrete time into 6 parts, each part corresponds to a different Rubik's cube rotation mode, and the set K of integer value is [0–17] representing 18 rotation modes $\mathcal{R}_{ot}$.
Step 7: Rotate each face element of the Rubik's cube that has just been rotated firstly by row and bitwise right circularly shifted by the value of K, and then circularly shifted bitwise right by column by the value of K:

$$K = fix\left(P_{y,x} \times 10^{16}\right) \bmod 18 \tag{13}$$

Step 8: Convert the random matrix $P_{y,x}$ to an integer matrix of [0–255]: $L = fix\left(P_{y,x} \times 10^{16}\right) \bmod 256$, and then react to the third step, and perform bitwise XOR processing with rotated matrix to obtain a single-channel encrypted image.

$$I_{en} = I_1 \oplus L = I_1 \oplus [fix(P_{y,x} \times 10^{16}) \bmod 256] \tag{14}$$

Step 9: Perform the same steps above for three channels, combine the encrypted three channel image of R, G, and B to obtain a color encrypted image.

Decryption algorithm. Decryption is the contrary procedure of encryption. Briefly describe the decryption process.

Step 1: Split the encrypted color image into R, G, and B three-channel images to obtain three single-channel encrypted images.
Step 2: Use the parameters selected in the encryption process to perform a discrete time alternate quantum walk, generate a matrix, convert it into a pixel value matrix of [0–255], and take bitwise XOR with the encrypted image
Step 3: Divide the image matrix into six parts and the sequence obtained in discrete time is divided into six parts.
Step 4: Convert the probability matrix $P_{y,x}$ to the integer sequence value of [0–17], and perform the Rubik's Cube reduction based on this.

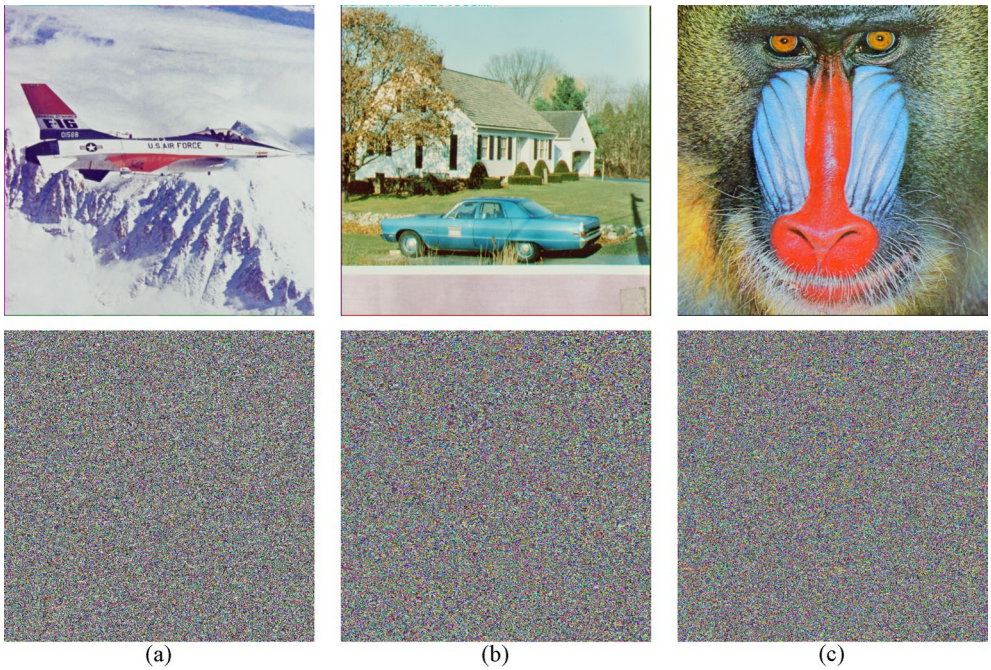

Figure 4. Entryption results. (**a**) Jetplane and it's encryption image. (**b**) House and it's encryption image. (**c**) Baboon and it's encryption image.

$$\begin{cases} k' = k + 3, k \in (0, 1, 2, 6, 7, 8, 12, 13, 14) \\ k' = k - 3, k \in (3, 4, 5, 9, 10, 11, 15, 16, 17) \end{cases} \tag{15}$$

Step 5: Apply step 3 in the reverse direction, merge the sub-images into a single-channel image of size, and then merge the decrypted three channel image to obtain the original image.

Experiments and performance analysis

So as to prove that the proposed encryption scheme has sufficient security, we select four color images with size of 512×512 for simulation analysis. This section analyzes the histogram, correlation, information entropy, key space, key sensitivity, and PSNR of encrypted images. The parameters of the alternate quantum walk generation key are $(512, 512, \alpha, \beta)$, α, β are obtained by calculating the image's hash.

Encryption effect. We choose three color images to perform a simulation, and the results are demonstrated in Fig. 4. From the Fig. 4, it's obvious that the encrypted image has no visual information about original image.

Histogram analysis. From the perspective of ciphertext histogram, they tend to be uniform, balance the frequency of each pixel value, and have the capability to resist statistical attacks. The histogram of the original image. The ciphertext is demonstrated in Figs. 5, 6, 7 and 8.

We find that the pixels of the original image are not uniformly distributed, which is easy to be attacked by statistical analysis. The pixel values of encrypted images are evenly dispersed, which can resist statistical analysis attacks well and ensure the security of information.

Information entrop analysis. Information entropy is usually used to measure the randomness of a system. In the field of image encryption, information entropy is advantaged to weigh the uncertainty of image information. The more evenly the pixel points of each gray level of the encrypted image R, G, and B are distributed, the better the encryption effect and the stronger the capability to resist external attacks. The formula for calculating information entropy is as follows:

$$H(\alpha) = -\sum_{i=1}^{L} P(\alpha_i) \log_2 P(\alpha_i) \tag{16}$$

where $H(\alpha)$ denotes the value of information entropy. The closer its value is to 8, the better the encryption effect is. α_i represents the gray value of the first pixel, and$P(\alpha_i)$ represents the probability of the gray level. Measure the entropy of the three images of Lena, House, Baboon and Peppers after encryption, and the results are illustrated in Table 2. Taking Lena image as an example, comparing the encryption method in this paper with the different encryption methods, the results are demonstrated in Table 3, which proves the superiority and the security of

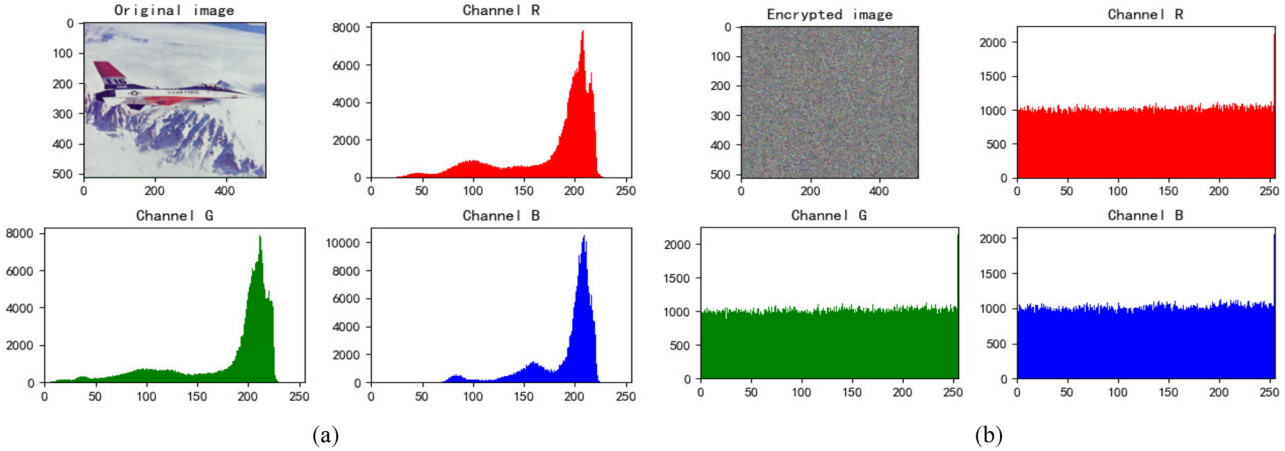

Figure 5. Jetplane's histogram. (**a**) Histogram of original Jetplane. (**b**) Histogram of encrypted Jetplane.

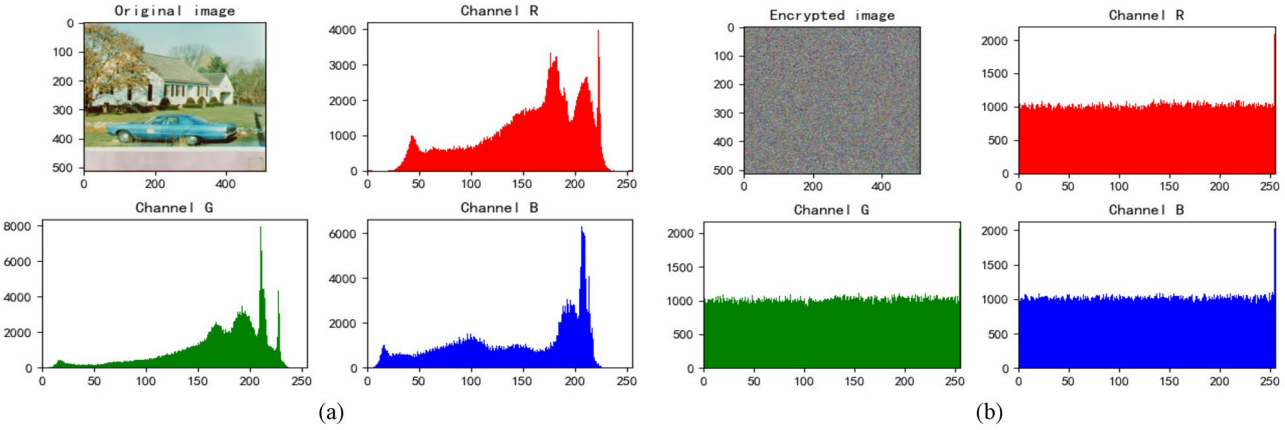

Figure 6. House's histogram. (**a**) Histogram of original House. (**b**) Histogram of encrypted House.

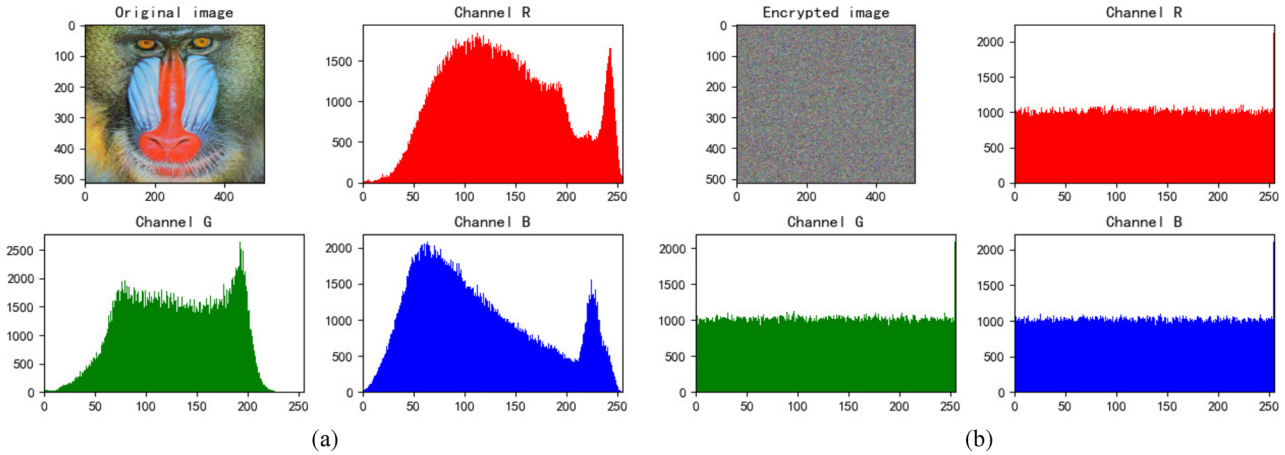

Figure 7. Baboon's histogram. (**a**) Histogram of original Baboon. (**b**) Histogram of encrypted Baboon.

the encryption method in this paper. The entropy value of the algorithm which put forward in this paper can reach 7.999, which is better than most encryption algorithms.

Correlation analysis. Correlation is a measurement standard for calculating the degree of correlation between two variables. Generally speaking, the degree of correlation between adjacent pixels of the image to be encrypted is high commonly, and a third party can infer the characteristics of the surrounding pixels through a

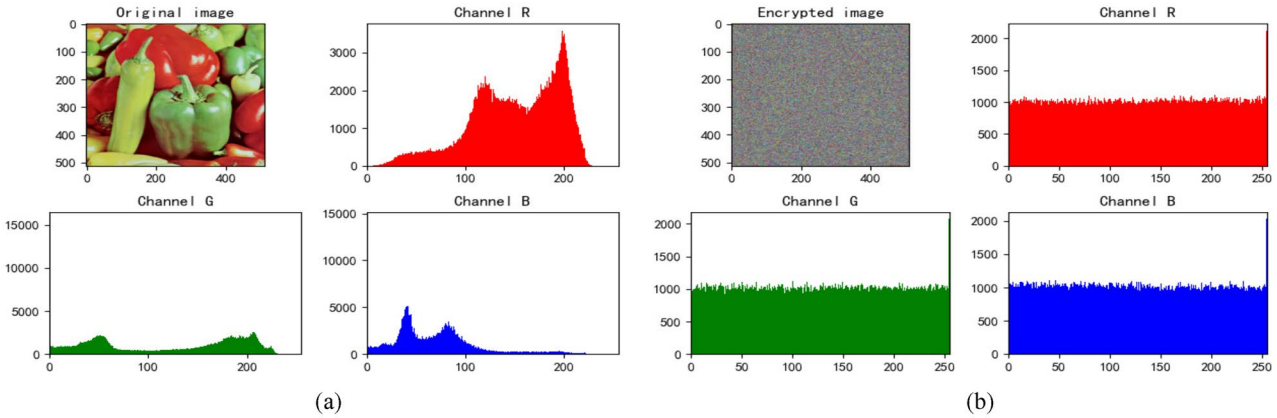

Figure 8. Peppers's histogram. (**a**) Histogram of original Peppers. (**b**) Histogram of encrypted Peppers.

Global	Jetplane	House	Baboon	Peppers
Channel R	7.9991	7.9992	7.9992	7.9992
Channel G	7.9991	7.9992	7.9993	7.9993
Channel B	7.9989	7.9994	7.9994	7.9994
Local	**Jetplane**	**House**	**Baboon**	**Peppers**
Channel R	7.8912	7.8985	7.8947	7.9002
Channel G	7.8986	7.8972	7.8847	7.9000
Channel B	7.9046	7.9005	7.9002	7.9040

Table 2. Global and local information entrop of three channels.

Information entrop	Proposed	Ref[29]	Ref[46]	Ref[16]	Ref[48]	Ref[49]
Jetplane	7.999	******	******	******	******	7.9971
House	7.9992	******	7.99704	7.9969	******	******
Baboon	7.9993	7.9974	7.99729	******	7.9993	7.9995
Peppers	7.9992	******	******	7.9851	7.9993	7.9989

Table 3. Information entrop of different encryption. * means no value.

pixel. Therefore, image encryption must decrease the correlation as much as possible. We calculate the correlation of encrypted images with using the formula (17). The value range of the correlation coefficient is $[-1, 1]$ that the absolute value of the correlation coefficient approaches 0, indicating that the correlation is smaller, and the attack is resisted. The stronger the ability is, the better the effect of image encryption is.

$$R_{y,x} = \frac{\sum_{i=1}^{W} \big(y_i - E(y)\big)(x_i - E(x))}{W\sqrt{D(y)}\sqrt{D(x)}} \tag{17}$$

where $D(y) = \frac{1}{W}\sum_{i=1}^{W}\big(y_i - E(y)\big)^2$, $E(y) = \frac{1}{W}\sum_{i=1}^{W} y_i$. y and x are the adjacent pixels, and W is the total number of pixels in the image. We chose Lena, House and Baboon as the test images to measure the correlation between the original image and the encrypted image of the three images. Firstly, 3000 couples of pixels are selected for each image, and then the correlations in the horizontal, vertical, and diagonal lines are tested respectively. The test results are shown in Figs. 9, 10 and 11 and Table 4. It can be seen that the correlation of the original image is basically linear, while the distribution of the encrypted image is uniform and disorderly. Through the comparison of the two, we can conclude that the encrypted image is weakly correlated and this methods has sound effects.

Key space analysis. For an algorithm of image encryption, it's trustworthy to have a vast key space. So that external eavesdroppers cannot obtain information through brute force enumeration. The Rubik's Cube encryption scheme based on chaotic mapping has better security in some real-time confidential communications,however, the key space of traditional chaotic encryption is limited and there is still a risk of being cracked. The encryption scheme based on alternate quantum walk and Rubik's cube rotation which is put forward in this paper uses the

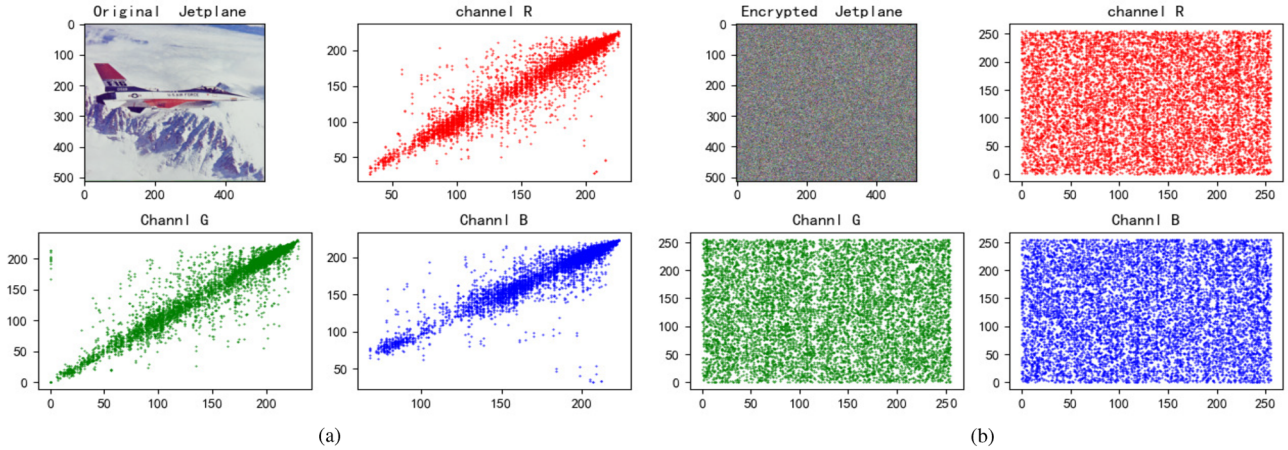

Figure 9. Jetplane's correlation. (**a**) Correlation of Jetplane and it's channels. (**b**) Correlation of encrypted Jetplane and it's channels.

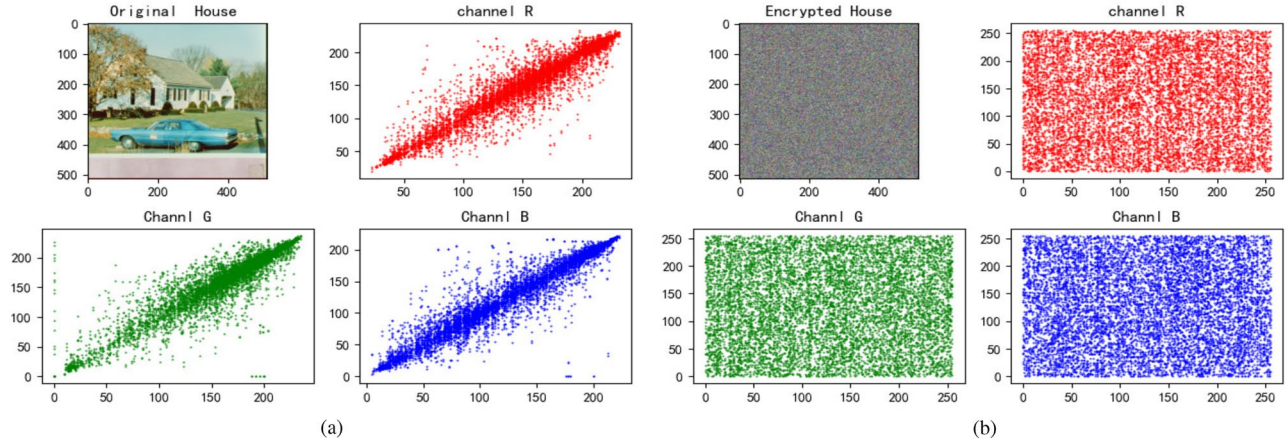

Figure 10. House's correlation. (**a**) Correlation of House and it's channels. (**b**) Correlation of encrypted House and it's channels.

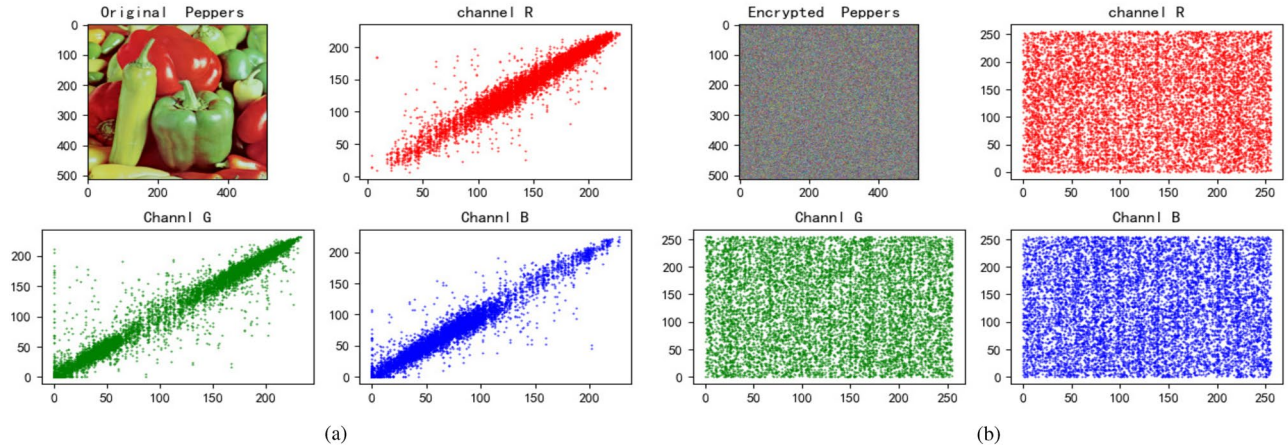

Figure 11. Baboon's correlation. (**a**) Correlation of Baboon and it's channels. (**b**) Correlation of encrypted Baboon and it's channels.

Correlation	Horizontal	Vertical	Diagonal
Original image: Jetplane	0.9685	0.9507	0.9275
Encrypted image: Jetplane	0.0125	0.0134	0.0071
Original image: House	0.9574	0.9620	0.9266
Encrypted image: House	0.0122	0.0098	0.0083
Original image: Baboon	0.9000	0.8349	0.8069
Encrypted image: Baboon	0.0143	0.0103	0.0103

Table 4. Correlation of the original images and encrypted images.

Image	NPCR/%	UACI/%
Lena	99.5991	33.4537
House	99.5670	33.3913
Baboon	99.6181	33.4429
Peppers	99.6073	33.4508
Ref[29]	99.5850	28.6210
Ref[16]Baboon	99.61935	*****
Ref[16]	99.765	*****
Ref[48]	99.61	33.47
Ref[49]Baboon	99.6045	33.4457

Table 5. NPCR and UACI between encrypted images with different key parameters.

characteristics of alternate quantum walk. While quantum walk are sensitive to the initial state and non-periodic to generate a theoretically infinite space key. Assuming that the initial state of quantum walk is $|\psi_0\rangle$, after the unitary operation of N steps, the final state is $|\psi_N\rangle$:

$$|\psi_N\rangle = \hat{U}^N|\psi_0\rangle \tag{18}$$

The probability of getting a walker at position (y, x) is:

$$P_{Y,X} = \sum \left|\left\langle y, x_3 0\middle|\hat{U}^N\middle|\psi_0\right\rangle\right|^2 + \sum \left|\left\langle y, x, 1\middle|\hat{U}^N\middle|\psi_0\right\rangle\right|^2 \tag{19}$$

Since the possibility of determining an initial state and decomposing a sum of squares is almost zero, there is endless possibility in the key space. In the conventional computer simulation quantum environment, that is, the precision is 10^{-16}, the parameters of the quantum random walk consist of four numbers, two of which are obtained by calculating the hash value of the image, and the space size is 2^{256}, the space size of the other two parameters is $(10^{16})^2$, so the key space of the encryption scheme is $2^{256} \times 10^{32}$. Thus, in the case that the initial state cannot be obtained, the randomness and unpredictability of the key sequence make the eavesdropper unable to obtain any information, which effectively prevents the information from being cracked and eavesdropped.

Key sensitivity analysis. In order to obtain the key sensitivity of the algorithm, we change a parameter of the key for encryption, and test the change pixel rate NPCR and the average change intensity UACI between it and the correct key. The closer the NPCR is to 99.6094% and the UACI to 33.4635%, the stronger the key sensitivity is. The test results of NPCR and UACI are demonstrated in Table 5.

Analysis of PSNR. PSNR is used to measure the robustness of encrypted images in the field of image encryption. The smaller the value of PSNR is, the greater the difference between the encrypted image and the original image is. Hence, the encryption effect is better. For the original image $\mathcal{I}$ and encrypted image I_{en}. The calculation formula of PSNR is:

$$PSNR = 10\log_{10}\frac{(2^n-1)^2 ab}{\sum_{i=1}^{a}\sum_{j=1}^{b}(I_{en}(i,j)-\mathcal{I}(i,j))^2} \tag{20}$$

where a is the width of image, b is the height of the image, and n is the number of pixels. We tested the PSNR values of Lena, House, Baboon, and House, and the test results are shown in Table 6 below. The test results indicate that encryption method which put forward has better robustness.

Different attack analysis. In the process of network transmission, the transmission of image information will inevitably be affected and destroyed by various factors, resulting in image degradation and pollution, which

PSNR	Jetplane	House	Baboon	Peppers
Channel R	8.206	8.713	8.766	9.127
Channel G	7.915	8.348	9.226	7.65
Channel B	8.006	8.356	8.356	7.648

Table 6. PSNR of three channels.

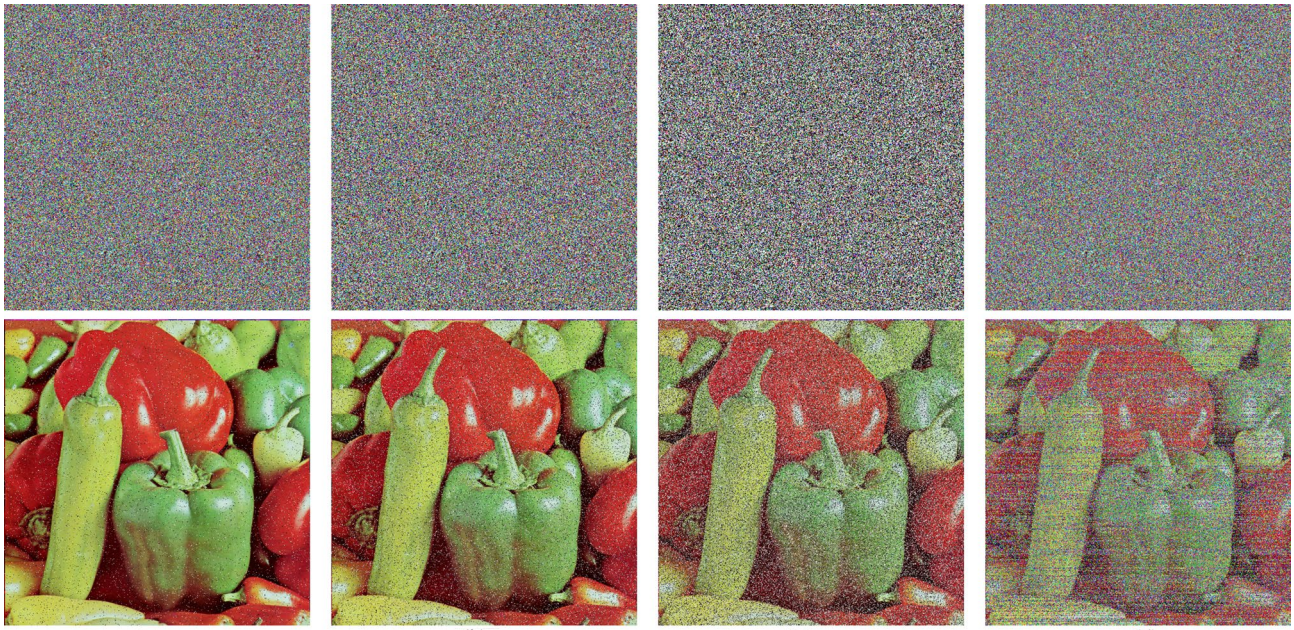

Figure 12. Noise attack. (**a–c**) Pictures which add different degrees of salt and pepper noise, and (**d**) is that adds Gaussian noise.

has a great impact on image decryption. In order to further study and analyze the robustness of the algorithm, this paper validates the common interference and attacks. We add different degrees of salt and pepper noise and Gaussian noise to the image, and the experimental results are shown in Fig. 12; we also crop the image to varying degrees, and the results are shown in Fig. 13. The experimental results show that no matter under the influence of noise or cropping, the algorithm can solve the image with visual information and is robust.

Differential attack analysis. As a kind of selective plaintext attack, differential attack can effectively test the security of encryption algorithm and the sensitivity of image. By making minor changes to the original plaintext image and analyzing the encrypted image with the unchanged image, the attacker obtains certain relations and rules, and uses them to decrypt other encrypted images to obtain information. Some of the parameters of the quantum random walk of the key generated in this scheme are obtained by calculating the hash value of the image, that is to say, the scheme is sensitive to the image, that is, when the image changes slightly, the encryption result of the image will be very different. In order to confirm this idea, we change one pixel value to the original image, and compare the encrypted image with the encrypted image before the change. The experimental results are shown in the Table 7. Through the data in the table, we find that when the image changes slightly, the encrypted image is very different, especially in the pixel change rate of the two encrypted images. Therefore, the scheme has the ability to resist selective plaintext attack.

Time and space complexity analysis. In this scheme, the pixels of the image are traversed many times in different steps, and the size of the color image is assumed to be $N * N * 3$. For the algorithm mentioned in the previous chapter, it is considered that the key generated by the alternating quantum random walk and the random sequence are a common part, and the time complexity is $O(N * N)$. Then it takes about $O(N * N * 3)$ to extract the pixel information to construct the Rubik's cube, and $O(\frac{1}{6} * 9 * N * N * 3)$ to complete the scrambling operation for the Rubik's cube rotation. Finally, the complex time is $O(N * N * 3)$ after bitwise XOR diffusion processing. Therefore, the time complexity of this scheme is about $O(11N^2)$.

The space complexity of the scheme is $O(N^2)$. The step space of alternating quantum random walk to generate key is $O(N * N)$. The space occupied by space scrambling is the space occupied by image segmentation, Rubik's cube and rotation scrambling and spreading recovery, that is, $O(N * N) + O(1) + O(1) + O(N * N) = O(N * N)$,

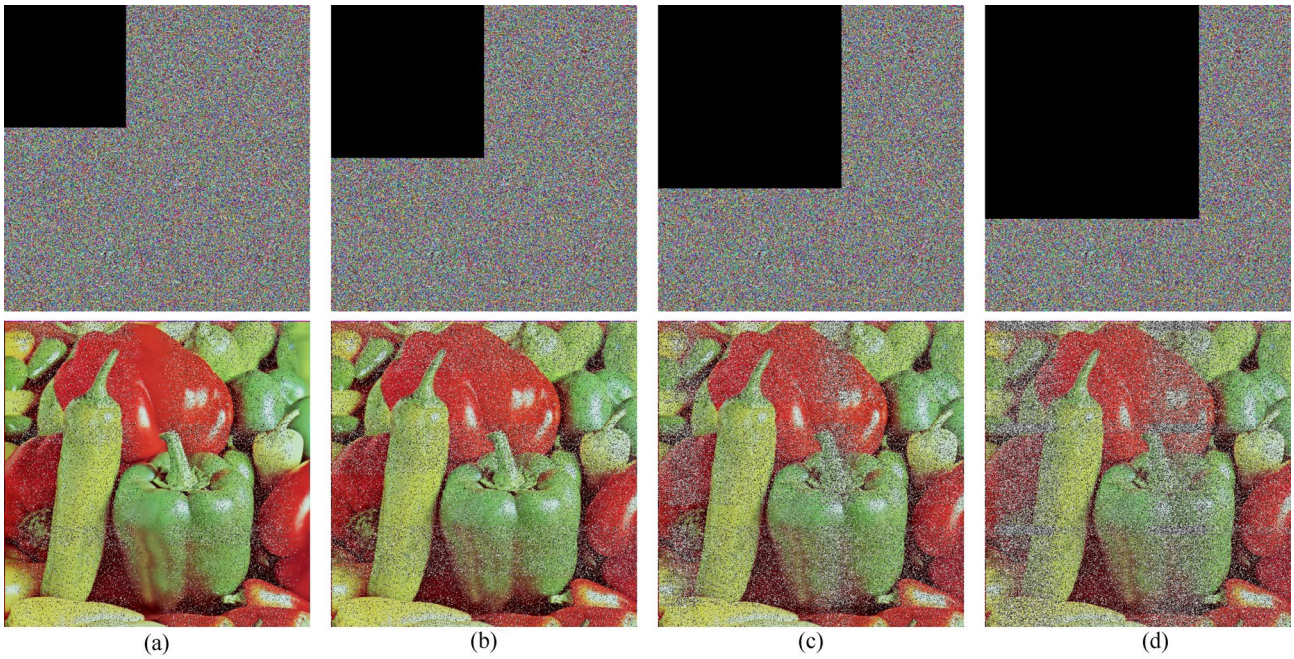

Figure 13. Clipping attack. (**A–D**) The experimental results of 16%, 25%, 36% and 49% of the cut images, respectively.

Image	NPCR/%	UACI/%
Jetplane	99.6116	33.5955
House	99.6134	33.662
Baboon	99.612	33.6651

Table 7. NPCR and UACI between encrypted images.

and the space occupied by diffusion encryption step is $O(N * N)$. To sum up, the space complexity of the scheme is $O(N^2) + O(N^2) = O(N^2)$.

NIST test analysis. NIST Statistical Test[50](version NIST SP 800-22 National Institute of Standards and Technology) is suitable for testing the randomness of sequences. The test consists of 15 items that reflect the random performance of the sequence. Table 8 shows the NIST test results of this scheme. It has been mentioned in reference[50] that when P-Value is greater than or equal to 0.01, this group of data is random, and the result shows that it is passed. The average pass rate of this scheme is 98.9%, and the lowest pass rate is 97%, which is acceptable.

Summary and prospect

Based on alternate quantum walk and Rubik's cube transforme, this paper has put forward a novel color image encryption scheme. The core algorithm of this scheme is to generate random sequence through quantum random walk, extract image pixels to form a third-order Rubik's Cube. Then we control rotation of Rubik's Cube by using random sequences to realize image scrambling. Through experiments, it is found that proposed scheme has a sound encryption effect. The histogram of encrypted image is evenly distributed, the entropy value is about 7.999, the degree of correlation is low, so it can effectively resist statistical attacks. The algorithm has a vast key space and strong key sensitivity, which can effectively resist brute force attacks. The NPCR of encrypted images is around 99.5978%, and the UACI is around 33.4317%, which can effectively resist differential attacks. The PSNR of the encrypted image is low, and it has better robustness.At present and in the future, we will vigorously promote the combination of quantum walk and classical algorithms, and further apply it to image information encryption in medicine, military and other directions.

Statixtical test	P-value	Proportion
Frequence	0.637119	100/100
BlockFrequence	0.401199	100/100
CumulativeSums	0.779188	99/100
CumulativeSums	0.304126	100/100
Runs	0.202268	97/100
LongestRun	0.883171	99/100
Rank	0.040108	99/100
FFT	0.085587	98/100
NonOverlappingTemplate	0.505671	98/100
ApproximateEntropy	–	98/100
Serial	0.779188	99/100
Serial	0.946308	100/100
LinearComplexity	0.816537	99/100
RandomExcursions	0.40783	2/2
RandomExcursionsVariant	0.340435	2/2
Universal	0.449653	2/2

Table 8. Result of NIST test for encrypted image.

Received: 26 December 2021; Accepted: 4 August 2022
Published online: 22 August 2022

References

1. Ma, Y., Li, N., Zhang, W., Wang, S. & Ma, H. Image encryption scheme based on alternate quantum walks and discrete cosine transform. *Opt. Exp.* **29**(18), 28338–28351 (2021).
2. Xi, S. *et al.* Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram. *Opt. Exp.* **25**(7), 8212–8222 (2017).
3. Su, Y. *et al.* Optical encryption scheme for multiple color images using complete trinary tree structure. *Opt. Lasers Eng.* **98**, 46–55 (2017).
4. Tao, S., Tang, C., Shen, Y. & Lei, Z. Optical image encryption based on biometric keys and singular value decomposition. *Appl. Opt* **59**(8), 2422–2430 (2020).
5. Fu, C. *et al.* A chaos-based digital image encryption scheme with an improved diffusion strategy. *Opt. Exp.* **20**(3), 2363–78 (2012).
6. Liansheng, S., Bei, Z., Xiaojuan, N. & Ailing, T. Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain. *Opt. Exp.* **24**(1), 499–515 (2016).
7. Wu, T. *et al.* Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission. *Opt. Exp.* **29**(3), 3669–3684 (2021).
8. Sui, L., Duan, K., Liang, J. & Hei, X. Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps. *Opt. Exp.* **22**(9), 10605–10621 (2014).
9. Zhong, Z., Qin, H., Liu, L., Zhang, Y. & Shan, M. Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain. *Opt. Exp.* **25**(6), 6974–6982 (2017).
10. Tao, R., Xin, Y. & Wang, Y. Double image encryption based on random phase encoding in the fractional Fourier domain. *Opt. Exp.* **15**(24), 16067–16079 (2007).
11. Shi, X. & Zhao, D. Color image hiding based on the phase retrieval technique and Arnold transform. *Appl. Opt.* **50**(14), 2134–2139 (2011).
12. Chen, W., Quan, C. & Tay, C. J. Optical color image encryption based on Arnold transform and interference method. *Opt. Commun.* **282**(18), 3680–3685 (2009).
13. Wu, L., Zhang, J., Deng, W. & He, D. Arnold transformation algorithm and anti-Arnold transformation algorithm. in *2009 First International Conference on Information Science and Engineering*. 1164–1167. (IEEE, 2009).
14. Liu, Z. *et al.* Image encryption by using gyrator transform and Arnold transform. *J. Electron. Imaging* **20**(1), 013020 (2011).
15. Subramanyan, B., Chhabria, V. M. & Babu, T. G. S. Image encryption based on AES key expansion. in *2011 Second International Conference on Emerging Applications of Information Technology*. 217–220. (IEEE, 2011).
16. Zhang, Q. & Ding, Q. Digital image encryption based on advanced encryption standard (AES). in *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*. 1218–1221. (IEEE, 2015).
17. Singh, A., Agarwal, P. & Chand, M. Image encryption and analysis using dynamic AES. in *2019 5th International Conference on Optimization and Applications (ICOA)*. 1–6. (IEEE, 2019).
18. Arab, A., Rostami, M. J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J. Supercomput.* **75**(10), 6663–6682 (2019).
19. Wang, Y. N., Song, Z. Y., Ma, Y. L., Hua, N. & Ma, H. Y. Color image encryption algorithm based on DNA coding and alternating quantum random walk [J/OL]. *Acta Phys. Sin.* 1–21 (2021).
20. Wang, X. & Liu, C. A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimed. Tools Appl.* **76**(5), 6229 (2017).
21. Chai, X., Chen, Y. & Broyde, L. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt. Lasers Eng.* **88**, 197–213 (2017).
22. Enayatifar, R., Abdullah, A. H. & Isnin, I. F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Opt. Lasers Eng.* **56**, 83–93 (2014).
23. Liu, H. & Wang, X. Image encryption using DNA complementary rule and chaotic maps. *Appl. Soft Comput.* **12**(5), 1457–1466 (2012).
24. Wang, X. Y., Zhang, Y. Q. & Bao, X. M. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **73**, 53–61 (2015).

25. Wang, X. Y., Zhang, J. J., Zhang, F. C. & Cao, G. H. New chaotical image encryption algorithm based on Fisher-Yatess scrambling and DNA coding. *Chin. Phys. B* **28**(4), 040504 (2019).
26. Cao, Y., Gao, F., & Li, D. D. *et al.* Side information -driven quantum composite control for protecting a qubit (2019).
27. Hong-Yang, M. *et al.* Quantum private query based on stable error correcting code in the case of noise. *Int. J. Theor. Phys.* **58**(12), 4241–4248 (2019).
28. Zhong, P.-G. *et al.* Quantum phase transitions triggered by a four-level atomic system in dissipative environments. *Phys. Rev. A.* **2019**(4) (2019).
29. Ma, H., He, Z., Xu, P., Dong, Y. & Fan, X. A Quantum Richardson-Lucy image restoration algorithm based on controlled rotation operation and Hamiltonian evolution. *Quantum Inf. Process.* **19**(8), 1–14 (2020).
30. Gao, F., Qin, S. J., Huang, W. & Wen, Q. Y. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China* (2019).
31. Xu, P., He, Z., Qiu, T. & Ma, H. Quantum image processing algorithm using edge extraction based on Kirsch operator. *Opt. Exp.* **28**(9), 12508–12517 (2020).
32. Zhang, M., Zhou, L., Zhong, W. & Sheng, Y.-B. Direct measurement of the concurrence of hybrid entangled state based on parity check measurements. *Chin. Phys. B* (2019).
33. Ma, Y., Ma, H. & Chu, P. Demonstration of quantum image edge extration enhancement through improved Sobel operator. *IEEE Access* **8**, 210277–210285 (2020).
34. Liu, F., Zhang, X., Xu, P. A., He, Z. X. & Ma, H. Y. A quantum dialogue protocol in discrete-time quantum walk based on hyper-entangled states. *Int. J. Theor. Phys.* **59**(11), 3491–3507 (2020).
35. Ryan, C. A., Laforest, M., Boileau, J. C. & Laflamme, R. Experimental implementation of a discrete-time quantum random walk on an NMR quantum-information processor. *Phys. Rev. A* **72**(6), 062317 (2005).
36. Panahiyan, S. & Fritzsche, S. Controlling quantum random walk with a step-dependent coin. *New J. Phys.* **20**(8), 083028 (2018).
37. Summy, G. & Wimberger, S. Quantum random walk of a Bose–Einstein condensate in momentum space. *Phys. Rev. A* **93**(2), 023638 (2016).
38. Kemp, G., Sinayskiy, I. & Petruccione, F. Lazy open quantum walks. *Phys. Rev. A* **102**(1), 012220 (2020).
39. Abd-El-Atty, B., Iliyasu, A. M., Alanezi, A. & El-latif, A. Optical image encryption based on quantum walks. *Opt. Lasers Eng.* **138**, 106403 (2021).
40. Abdullatif, A. A., Abdullatif, F. A. & Naji, S. A. An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques. *Period. Eng. Nat. Sci. (PEN)* **7**(4), 1607–1617 (2019).
41. Zhang, L., Tian, X. & Xia, S. A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence. in *2011 International Conference on Multimedia and Signal Processing*. Vol.1. 312–315. (IEEE, 2011).
42. Pan, P., Pan, Y., Wang, Z. & Wang, L. Provably secure encryption schemes with zero setup and linear speed by using Rubik's Cubes. *IEEE Access* **8**, 122251–122258 (2020).
43. Loukhaoukha, K., Chouinard, J. Y. & Berdai, A. A secure image encryption algorithm based on Rubik's cube principle. *J. Electr. Comput. Eng.* **2012**, (2012).
44. Vidhya, R. & Brindha, M. A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF). *J. King Saud Univ. Comput. Inf. Sci.* (2020).
45. Abd-El-Atty, B., Iliyasu, A. M., El-Latif, A. & Ahmed, A. A multi-image cryptosystem using quantum Walks and Chebyshev map. *Complexity* **2021** (2021).
46. El-Latif, A., Ahmed, A., Abd-El-Atty, B., Amin, M. & Iliyasu, A. M. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. *Sci. Rep.* **10**(1), 1–16 (2020).
47. El-Latif, A. A. A., Iliyasu, A. M. & Abd-El-Atty, B. An efficient visually meaningful quantum Walks-based encryption scheme for secure data transmission on IoT and smart applications. *Mathematics* **9**(23), 3131 (2021).
48. Xu, C., Sun, J. & Wang, C. An image encryption algorithm based on random walk and hyperchaotic systems. *Int. J. Bifurc. Chaos* (2020).
49. Shahna, K. U. & Mohamed, A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map[J]. *Appl. Soft Comput.* **90**, 106162 (2020).
50. Rukhin, A. *et al. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (NIST Special Publication, 2010).

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No.11975132,61772295), the Natural Science Foundation of Shandong Province, China (No.ZR2019YQ01), the Project of Shandong Province Higher Education Science and Technology Program(No.J18KZ012), Shandong Provincial Natural Fund Project(No.ZR2021MF049) Qingdao Municipality Livelihood Plan Project (No.22-3-7-xdny-18-nsh).

Author contributions

J.Z. and T.Z. conceived the scheme, T.Z. and J.J. conducted the experiment(s), H.M., J.J. and T.F. analysed the results. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to H.M.