International Journal of Theoretical Physics (2022) 61: 64
https://doi.org/10.1007/s10773-022-04979-1

Quantum Image Encryption Based on Baker Map and 2D Logistic Map

WanQing Wu[1,2] · Qiao Wang[1,2]

Received: 2 November 2021 / Accepted: 21 December 2021 / Published online: 10 March 2022

Abstract
This paper presents a quantum image encryption algorithm based on Baker map and 2D logistic map. The encrypted image is represented with NEQR model and the presented scheme adopts the strategy of selective encryption. Given a threshold value T, when $C'_{YX} \geq T (C'_{YX} < T)$, the proposed scheme performs $U_{\oplus k}(U_{\oplus A})$ on quantum state $|I'\rangle$. The final ciphertext quantum image is obtained through performing nine times quantum Baker map (QBM). The quantum circuits of encryption and decryption procedure are given. Multiple images were tested for security performance, including entropy, correlation coefficient (CC), Number of Pixel Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI). The best values of entropy, CC, NPCR and UACI are 7.9888, -0.0005, 99.58%, 33.17% respectively. Simulation results show that the proposed quantum image scheme has good performance in the aspect of security. By comparison with other schemes, the main indicators of the proposed scheme are roughly the same.

Keywords Quantum image encryption algorithm · NEQR · Baker map · 2D logistic map

1 Introduction

Feynman proposed the quantum computer model in 1982 [1]. The model uses the superposition and entanglement properties of quantum mechanics to store, process and transmit information. It has higher computing power compared to normal computers. Subsequently, Shor and Grover proposed quantum prime factorization algorithm [2] and quantum search algorithms [3] respectively. Therefore, the quantum computers began to appear in various fields of computer science. Such as quantum cryptography [4–6], quantum communication [7, 8], quantum image encryption and so on. Among them, quantum image encryption has

✉ WanQing Wu
wuwanqing8888@126.com

[1] School of Cyber Security and computer, Hebei University, Baoding 071002, Peoples Republic of China

[2] Key Laboratory on High Trusted Information System in Hebei Province, Hebei University, Baoding 071002, Peoples Republic of China

become more and more important in recent years because it is more secure and efficient than traditional image encryption [9].

However, the digital image is converted into a quantum image before performing the quantum processing. Thus there are some quantum image representation methods are proposed. In 2003 Bose proposed the Qubit Lattice representation method [10]. The image is considered as a matrix and each qubit stores only one pixel. In 2010, a flexible representation of quantum images (FRQI) was proposed [11], an algorithm that represents color information as an angle. For an image of size $2^n \times 2^n$, its horizontal and vertical coordinates are expressed in n qubits. However, FRQI uses only one qubit to represent the color information, so it is not easy to perform some complex color manipulation. To address this problem, the novel enhanced quantum representation (NEQR) [12] was proposed in 2013. The total number of qubits required in NEQR is $q + 2n$ for a gray range $0 \sim 2^q - 1$ image with size of $2^n \times 2^n$. Although it increases the use of qubits, it facilitates the handling of colors. It has also become a more widely used image representation model in quantum image processing. There are other quantum image representation models, such as the generalized quantum image representation (GNEQR) model [36], FRQIM [38] by slightly modifying FRQI, the normal arbitrary superposition state (NASS) model [13] and the multi-channel quantum image (MCQI) model [38], which improve the efficiency of specific applications.

According to the characteristics and convenience of various quantum image representation methods, NEQR and its improved method GNEQR are often used for time domain image encryption [15–17, 39], and FRQI and its improved method FRQIM are often used for frequency domain image encryption [19, 20, 40, 41]. Time-domain image encryption scheme generally encrypts images by scrambling pixel positions and changing pixel values. For example, in [15], a three-level quantum image encryption algorithm based on Arnold transform and logistic mapping is proposed, which performs block-level permutation, bit-level permutation and pixel-level diffusion respectively. The key space is increased by setting different block sizes as well as Arnold transform parameters. In 2019, Li et al. proposed a block image encryption algorithm based on GNEQR [16]. It is not only applicable to grey-scale and color images, but also can be used for rectangular images. The scheme uses both geometric and bit-plane transformations to change the position and pixel values of the image. Frequency-domain encryption are more complicated than the encryption algorithms over the time domain. Because they usually convert the image to the frequency domain for encryption while maintaining permutation and diffusion operations. There are some encryption schemes in frequency domain. For example, in [19], it proposes a quantum image encryption algorithm based on Arnold permutation and wavelet transform, which combines the time domain and frequency domain permutation to achieve good encryption results. The algorithm uses a modified FRQI model to represent the image. In [41], it uses Fibonacci transform and geometric transform to scramble the position and double random-phase encoding to encode the pixel information. There are some encryption schemes that only disturb the frequency domain characteristics of the image. For example, the algorithms in [18] use the double random phase encoding (DRPE) technique for quantum image encryption in the Fourier transform domain. Then the paper [18] is improved by Du, he makes the results of the double random phase coding as uniformly mixed as possible in [20].

In recent years, chaotic maps are often used to image encryption due to the features of sensitivity to initial values, a period and pseudo randomness [37]. Therefore, we propose a quantum image encryption method based on chaotic mapping and Fourier transform in time-frequency domain. Considering that most encryption operations are performed in the

time domain, we choose NEQR as the representation method of quantum images. We incorporate the idea of selective encryption [24] into it to equalize histogram of cipher image. Selective encryption first to block the image. Then, different operations are performed on the image block according to whether the correlation coefficient in the block is greater than the threshold. The main advantages of this scheme as follows: (1) Associate the key with the plain image. It can effectively resist chosen-plaintext attack. (2) Equalize histogram of encrypted image. It can remarkably resist statistical attack. (3) The introduction of QFT increases the complexity of the encryption scheme.

The remainder of this paper is organised as follows. Section 2 presents some preliminary knowledges. The proposed encryption and decryption schemes are presented in Section 3. Section 4 presents simulations and security evaluations of the scheme. Finally, the conclusion is presented in Section 5.

2 Preliminary

Before introducing the background, we agree on some symbols in Table 1.

2.1 NEQR representation and quantum computation model

In [28], Zhang et al. presented the NEQR representation of quantum image. The digital image I can be stored into a normalized superposition state $|I\rangle$, that is, the proposed NEQR model stores the gray-scale and position information of the image using the superposition of the qubit sequences.

The NEQR model of a quantum image $|I\rangle$ for a $2^n \times 2^n$ image can be written as

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_{YX}\rangle |YX\rangle, \tag{1}$$

where the gray-scale value of the corresponding pixel (Y, X) is

$$|C_{YX}\rangle = |C_{YX}^0 C_{YX}^1 \cdots |C_{YX}^q\rangle \in [0, 2^q - 1], C_{YX}^i \in \{0, 1\}.$$

While the vertical position Y and horizontal position X are represented with qubits $|YX\rangle$. Thus, in the representation of NEQR, a quantum image with the gray-scale 2^q and position information $2^n \times 2^n$ consists of $q + 2n$ qubits.

Next we introduce the quantum computation model. Quantum computation consists of a series of quantum logic gates and measurement results. It can accepts superposition states input and outputs corresponding superposition states. The special quantum computation model is as follow

$$U_f : |x, 0\rangle \rightarrow |x, f(x) \oplus 0\rangle, \tag{2}$$

where f is any function and U_f is a unitary operator [31].

Table 1 Notation Convention

$x \bigoplus y$	binary x and y perform bitwise XOR
$dec2bin(\cdot)$	Convert from decimal to binary
$bin2dec(\cdot)$	Convert from binary to decimal

2.2 Discrete Baker map (DBM) and quantum DBM

Baker mapping is a block scrambling method, and at the same time, selecting encryption requires dividing the image into blocks. That's why Baker mapping was chosen for scrambling. The classical Baker map $B(x, y)$, which maps the unit square $0 \leq x, y \leq 1$ onto itself, is a special chaotic map in [29]. Classical Baker map $B(x, y)$ is described as follows

$$B(x, y) = \begin{cases} (2x, \frac{y}{2}), & 0 \leq x < 1/2 \\ (2x-1, \frac{y+1}{2}), & 1/2 \leq x \leq 1, \end{cases} \tag{3}$$

where $y \in [0, 1]$. In other words, as shown in Fig. 1, the classical Baker map maps the left rectangle of the square $[0, \frac{1}{2}) \times [0, 1)$ to rectangle $[0, 1) \times [0, \frac{1}{2})$, and it transforms the right rectangle of the square $[\frac{1}{2}, 1) \times [0, 1)$ to rectangle $[0, 1) \times [\frac{1}{2}, 1)$.

The Baker map used for image encryption needs to be discretized because each image is composed of discrete pixel values. The Baker map can be discretized in the following.

Assume $n_i | N (i = 1, \cdots, k)$ and $n_1 + n_2 + ... + n_k = N$, $N \in Z^+$. The discrete Baker Map is defined as follows. Firstly, it divides the image $B_{N\times N}$ into N blocks, i.e.

$$B_{11}, \cdots, B_{1n_1}, B_{21}, \cdots, B_{2n_2}, \cdots, B_{k1}, \cdots, B_{kn_k}$$

where B_{ij} is a matrix of $\dfrac{N}{n_i}$ rows and n_i columns, $i = 1, \cdots, k$, $j = 1, \cdots, n_i$. Secondly, it performs matrix vec operator [30] on B_{ij} to obtain $B1_{N\times N}$, i.e.

$$B1_{N\times N} = \begin{bmatrix} vec^T(B_{11}) \\ \vdots \\ vec^T(B_{ij}) \\ \vdots \\ vec^T(B_{kn_k}) \end{bmatrix} = \begin{bmatrix} B1_{11} \\ \vdots \\ B1_{ij} \\ \vdots \\ B1_{kn_k} \end{bmatrix} \tag{4}$$

where $B1_{ij}$ is a matrix of 1 row and N columns. For example, let $N = 4, n_1 = 1, n_2 = 2, n_3 = 1$, the discrete Baker Map is as shown in Fig. 2.

For an example with $N = 4$ in Fig. 2, we give a concrete quantum circuit of the quantum Baker map. The quantum analogy of classical image $B_{N\times N}$ is $|I\rangle$, and its NEQR representation is expressed as

$$\begin{aligned} |I\rangle \ = \frac{1}{4}\Big(& |C_{0000}\rangle|0000\rangle + |C_{0100}\rangle|0100\rangle + |C_{1000}\rangle|1000\rangle + |C_{1100}\rangle|1100\rangle + \\ & |C_{0001}\rangle|0001\rangle + |C_{0101}\rangle|0101\rangle + |C_{1001}\rangle|1001\rangle + |C_{1101}\rangle|1101\rangle + \\ & |C_{0010}\rangle|0010\rangle + |C_{0110}\rangle|0110\rangle + |C_{1010}\rangle|1010\rangle + |C_{1110}\rangle|1110\rangle + \\ & |C_{0011}\rangle|0011\rangle + |C_{0111}\rangle|0111\rangle + |C_{1011}\rangle|1011\rangle + |C_{1111}\rangle|1111\rangle \Big). \end{aligned}$$

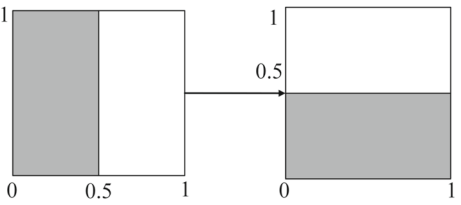

Fig. 1 Baker Map

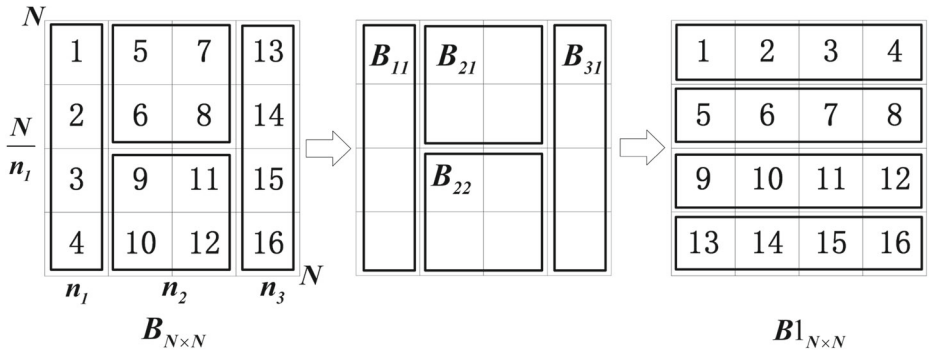

Fig. 2 Discrete Baker Map

Apply the quantum Baker map on quantum image $|I\rangle$, and we obtain the new quantum image $|I'\rangle$. That is,

$$\begin{aligned}|I'\rangle = U_{QBM}|I\rangle = \frac{1}{4}\Big(&|C_{0000}\rangle|0000\rangle + |C_{0001}\rangle|0100\rangle + |C_{0010}\rangle|1000\rangle + |C_{0011}\rangle|1100\rangle\\ &+|C_{0100}\rangle|0001\rangle + |C_{0101}\rangle|0101\rangle + |C_{1000}\rangle|1001\rangle + |C_{1001}\rangle|1101\rangle\\ &+|C_{0110}\rangle|0010\rangle + |C_{0111}\rangle|0110\rangle + |C_{1010}\rangle|1010\rangle + |C_{1011}\rangle|1110\rangle\\ &+|C_{1100}\rangle|0011\rangle + |C_{1101}\rangle|0111\rangle + |C_{1110}\rangle|1011\rangle + |C_{1111}\rangle|1111\rangle\Big),\end{aligned}$$

and its quantum circuit is shown in Fig. 3.

2.3 2D Logistic Map

The 2D Logistic Map [32] is defined as follows

$$\begin{cases} x_1(n+1) = \mu_1 x_1(n)(1 - x_1(n)) + \gamma_1 x_2^2(n) \\ x_2(n+1) = \mu_2 x_2(n)(1 - x_2(n)) + \gamma_2 (x_1(n) + x_1(n)x_2(n)) \end{cases} \tag{5}$$

where $x_1(n), x_2(n) \in (0, 1)$ and $2.75 < \mu_1 \leq 3.4$, $2.7 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$, $0.13 < \gamma_2 \leq 0.15$. The 2D Logistic Map can ensure the keyspace larger and the encryption system more complex since there are two quadratic terms in the 2D Logistic Map.

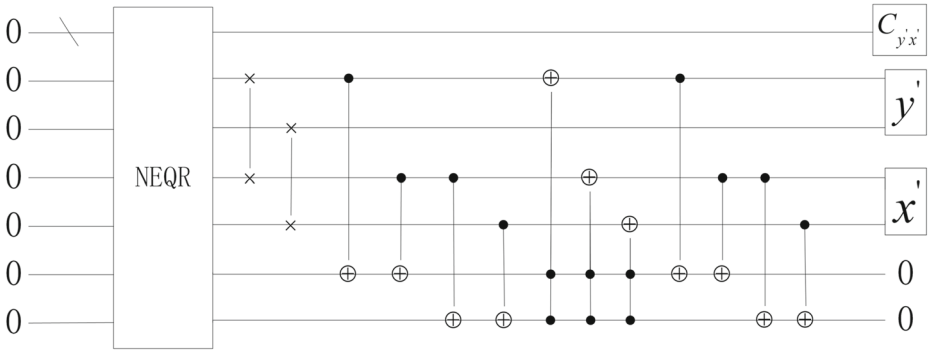

Fig. 3 Quantum circuit of QBM

3 Quantum image encryption scheme

In this section, the quantum image encryption scheme based on Baker map, 2D logistic map and quantum Fourier transform is presented in detail. The whole quantum image scheme has three main parts including key generation, encryption process and decryption process. More details can be introduced in the following subsections.

3.1 Key generation

Let the original classical image with size $2^8 \times 2^8$ be denoted as I. We use 2D logistic map to generate pseudo-random numbers with good cryptographic characteristics as the key. The specific steps are as follows.

Step 1. Caculate *offset*

a) Apply the discrete Baker map $B(x, y)$ on classical image I, then it obtains a new image I' denoted as $I' = B1_{N\times N}$ through equation (4).

b) Let $B1_{11} = (b_{11}, \cdots, b_{1N})$ be a vector from $B1_{N\times N}$, where $b_{1k} \in [0, 255], k = 1, \cdots, N$. Apply operation $dec2bin(\cdot)$ on b_{1k} of $B1_{11}$, and it has $dec2bin(b_{1k}) = (b_{1k})_2 = (e_{k1}, \cdots, e_{kl})^T$, where $e_{kl} \in \{0, 1\}$ and $l = 1, \cdots, 8$. Thus we obtain a $8 \times N$ binary matrix $BM = ((b_{11})_2^T, \cdots, (b_{1N})_2^T)$.

c) Perform bitwise XOR operation on each row of BM, i.e., $\alpha_l = \bigoplus_{k=1}^{N} e_{kl}, \alpha_l \in 0, 1, l = 1, \ldots, 8$. Then, it obtains $E = (\alpha_1, \cdots, \alpha_8)^T$.

d) Perform $bin2dec(\cdot)$ operation on E, and it obtains $bin2dec(E) = E_{10} = \alpha_7 \times 2^7 + \cdots + \alpha_1 \times 2^0$ and denotes E_{10} as the *offset* $\in [0, 255]$.

For example, let $N = 8$, the above calculation process of *offset* is shown in Fig. 4.

Step 2. Update the initial values of the 2D logistic map.

Suppose the initial values of the 2D logistic map are $x_1(0)', x_2(0)'$. The *offset* that is obtain in Step 1 will be mapped to (0, 1) by equation $\delta(s, offset)$. The $\delta(s, offset)$ is defined as follows

$$\delta(s, offset) = \lfloor \frac{10^s \times offset}{257} \rfloor \times 10^{-s}, offset \in [0, 255] \tag{6}$$

where symbol $\lfloor \cdot \rfloor$ is a floor function and s is a given value. In this paper, we convention $s = 4$.

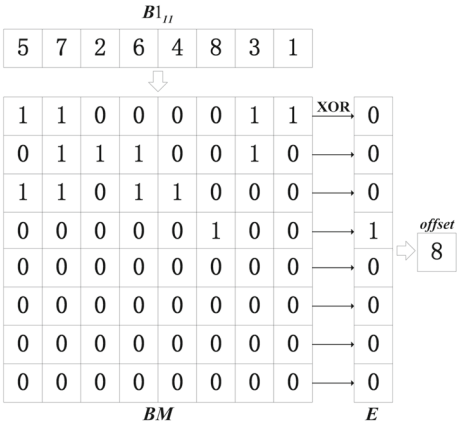

Fig. 4 Block binary XOR

Add the result of $\delta(s, offset)$ to $x_1(0)', x_2(0)'$, and obtain the modified initial values $x_1(0), x_2(0)$ i.e.,

$$\begin{cases} x_1(0) = \{x_1(0)' + \delta(s, offset)\} \\ x_2(0) = \{x_2(0)' + \delta(s, offset)\} \end{cases} \tag{7}$$

where $x_1(0)', x_2(0)'$ are given initial values and $\{x\}$ is the fractional part of x.

Step 3. Generate key

Modified initial values will be used to generate the key. Substituting $x_1(0), x_2(0)$ into equation (5), the equation yields two chaotic sequences $x_1 = (x_1(1), \cdots, x_1(N/2))$ and $x_2 = (x_2(1), \cdots, x_2(N/2))$. The chaotic sequences x_1, x_2 are mapped to [1, 255] using the equation as follows

$$g(u) = floor(255u) + 1 \tag{8}$$

where $u \in (x_1(1), \cdots, x_1(N/2), x_2(1), \cdots, x_2(N/2))$.

The mapped values $g(u)$ are considered as

$$k = \Big(g(x_1(1)), \ldots, g(x_1(N/2)), \cdots, g(x_2(1)), \ldots, g(x_2(N/2))\Big).$$

It shorted by $k = (k_1, \ldots, k_N)$.

Finally, after performing the $dec2bin(\cdot)$ function on k, we obtain the classical information $k_2 = dec2bin(k_1) \oplus \cdots \oplus dec2bin(k_N)$ as the encryption key.

3.2 Encryption process

Alice and Bob secretly transmit image information using quantum technology. The encryption process involves the following steps.

Step 1. Let $C_{Y'X'}$ be the corresponding discrete pixel values of image I'. Alice calculates $A = floor(\frac{1}{N^2}\sum_{Y',X'} C_{Y'X'})$ from I' and selects a random number $T \in [0, 255]$. Alice sends the binary sequence $(k_2, dec2bin(A))$ to Bob through quantum key distribution protocol such as $BB84$ protocol.

Step 2. Initialization of the quantum state.

After performing the quantum Baker map (QBM) on I, and Alice obtains quantum image with size $2^8 \times 2^8$ denoted as $|I'\rangle$, and its NEQR representation is expressed as

$$\begin{aligned} |I'\rangle &= |T\rangle U_{QBM}|I\rangle \\ &= \frac{1}{2^n}\sum_{Y'=0}^{2^n-1}\sum_{X'=0}^{2^n-1}|C_{Y'X'}\rangle|Y'X'\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_{Y'X'}\rangle|y'_0y'_1\cdots y'_{n-1}\rangle|x'_0x'_1\cdots x'_{n-1}\rangle. \end{aligned}$$

Step 3. Alice computes $C_{Y'X'} - T$ and stores the result on a auxiliary qubit $|0\rangle_a$. If $C_{Y'X'} \geq T (C_{Y'X'} < T)$, the auxiliary qubit $|0\rangle_a = |1\rangle (|0\rangle_a = |0\rangle)$.

Step 4. If $|0\rangle_a = |1\rangle (|0\rangle_a = |0\rangle)$, then Alice performs the unitary operation $U_{\oplus k}(U_{\oplus A})$ on quantum states $|I'\rangle$ and sequentially performs quantum Fourier transform (QFT) on it.

Step 5. Alice iterates the quantum Baker Map (QBM) nine times and obtains cipher image $|C\rangle = |0\rangle_a|T\rangle|C'_{YX}\rangle|YX\rangle$. After at least nine iterations, the original adjacent pixels will be distributed to the entire scrambled image [29]. That's the reason for the nine iterations of QBM.

The flowchart of the proposed quantum image encryption is demonstrated in Fig. 5, and the corresponding quantum circuit in Fig. 6.

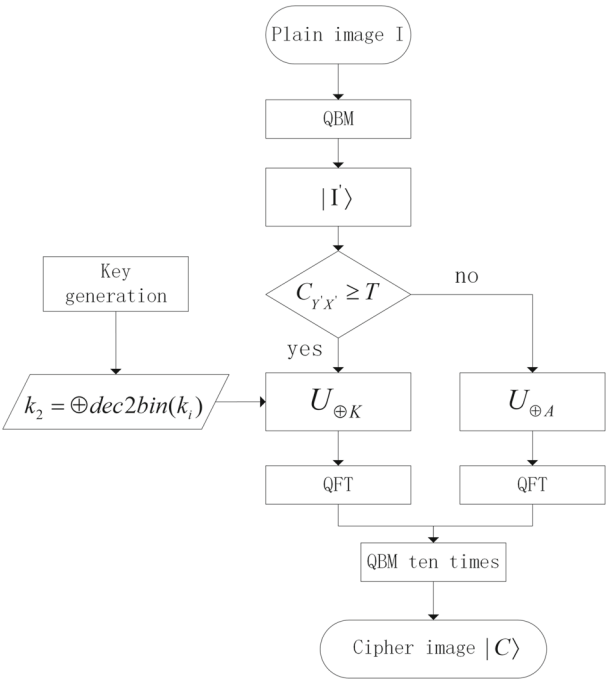

Fig. 5 Encryption process

Note that the unitary operation U denotes as an inverse quantum adder operation in Fig. 6.

3.3 Decryption process

Step 1. Iterate discrete inverse quantum Baker Map (IQBM) on the entire cipher image $|C\rangle$ ten times, and the transformed image is still denoted as $|C\rangle$.

Step 2. Bob performs the inverse quantum Fourier transform (IQFT) on $|C\rangle$.

Step 3. Bob applies the control unitary operation $C-U$ on plain image. If the control qubit is $|1\rangle(|0\rangle)$, then the $C-U$ is equivalent to $C-U_{\oplus k}(C-U_{\oplus A})$.

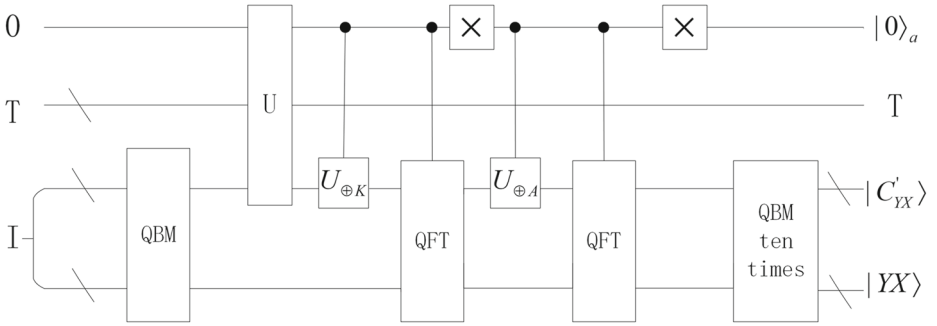

Fig. 6 Quantum circuit of encryption process

Step 4. Bob performs the inverse quantum Baker Map (IQBM) and obtains plain image I.

The flowchart of quantum image decryption is demonstrated in Fig. 7, and the corresponding quantum circuit in Fig. 8.

Note that the unitary operation U^{-1} denotes as the quantum adder operation in Fig. 8.

4 Simulation Results

The experiments are performed on MATLAB R2018a. We use 256 × 256 images Cameraman, Peppers, Baboon, Lake and Lena to test the security performance of the encryption scheme. The security performance indicators include visual inspection, keyspace, entropy, encryption quality, histogram and differential analysis. The key of the encryption scheme is composed of $(n_1, \cdots, n_k; x_1(0), x_2(0), \mu_1, \mu_2, \gamma_1, \gamma_2)$. Set the key to (64, 32, 4, 8, 4, 16, 32, 64, 16, 16; 0.5, 0.5, 3, 3, 0.2, 0.14) during the experiment.

4.1 Visual Inspection

In evaluating the ciphered image, visual inspection is the easiest and most remarkable factor. The five original images and their corresponding encrypted images are shown in Fig. 9, there is a big difference between the original images and the ciphers. Thus the proposed scheme can hide the main information of the original images.

4.2 Keyspace

In the permutation stage, the key relies on the width (height) of the image to be encrypted due to the scrambling phenomenon of the chaotic Baker map. Thus, the keyspace of size

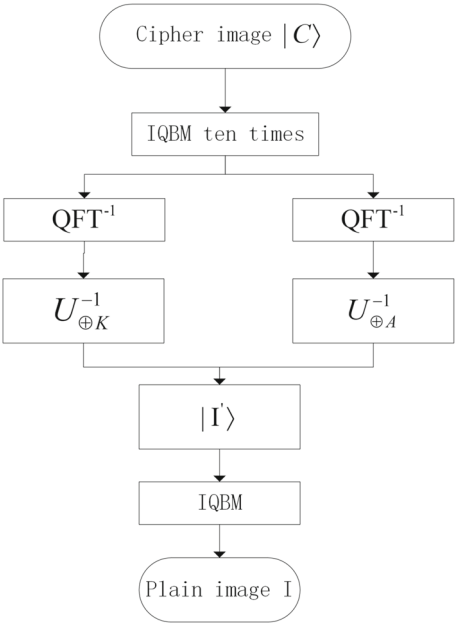

Fig. 7 Decryption process

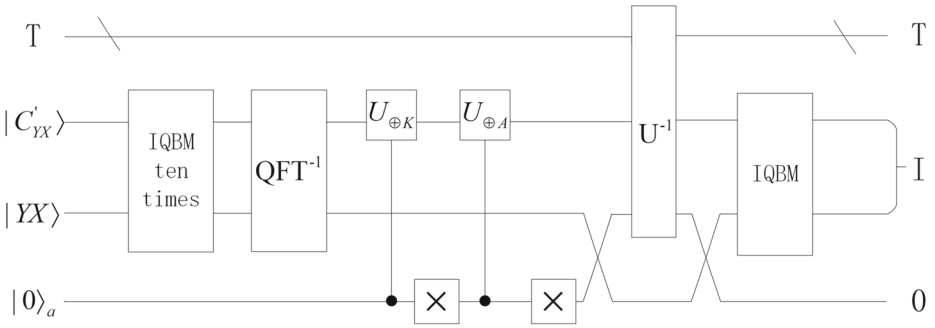

Fig. 8 Quantum circuit of decryption process

256×256 is equal to 10^{63} [23]. In the substitution stage, every parameter of the logistic map is a double precision number [23]. Thus, the keyspace in this stage is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{84}$. Such a large keyspace is enough to resist brute-force attacks.

4.3 Entropy

Entropy is an unpredictability measurement of structural characteristics for a cipher image x. The formula is defined as [22]

$$E(x) = -\sum_{i=0}^{2^N-1} P(x_i) \log_2 P(x_i) \tag{9}$$

where N is the number of bits for the pixel value x_i. In this paper, let $N = 8$. $P(x_i)$ is the proportion of pixel value $x_i \in [0, 255]$ in the encrypted image x. To attach high-level security, the entropy $E(x)$ should be close to 8. The entropy values of the cipher image corresponding to Cameraman, Peppers, Baboon, Lake and Lena are 7.983, 7.9854, 7.9812, 7.9888 and 7.9812 respectively as shown in Table 2. It shows that the proposed scheme has the unpredictability of structural characteristics.

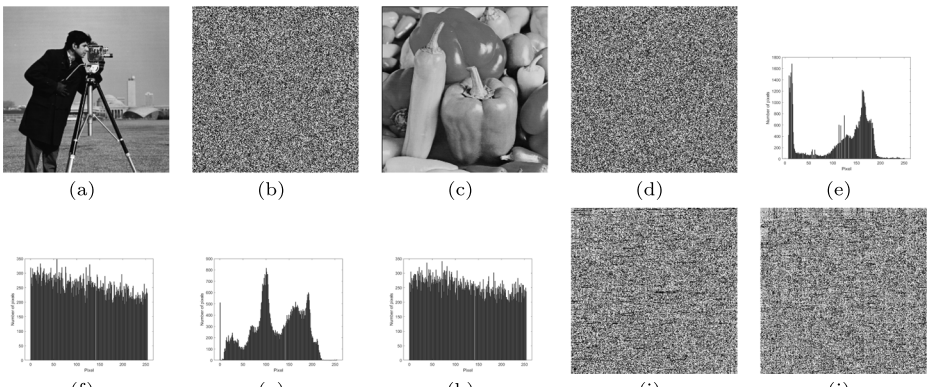

Fig. 9 Encryption result. a: original Cameraman. b: original Peppers. c: original Baboon. d: cipher Lake. e: cipher Lena. f: cipher Cameraman. g: cipher Peppers. h:cipher Baboon. i:cipher Lake. j:cipher Lena

Table 2 Entropy of encrypted images

Image	Entropy
Cameraman	7.983
Peppers	7.9854
Baboon	7.9812
Lake	7.9888
Lena	7.9812

4.4 Encryption Quality

In this section, correlation coefficient(CC), histogram deviation(HD), and irregular deviation(ID) have been calculated to evaluate the encryption quality.

CC is used to evaluate the correlation between plain image and cipher image. The value of CC is $[-1, 1]$. If the absolute value of CC equals to 1 that means the two images are the same. Thus, the lower absolute value of CC is, the better. The CC is measured by [22]

$$CC(x, y) = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \tag{10}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, N defines the pixel count in the image, and x, y are the pixel values of the plain image and encrypted image respectively.

The histogram deviation(HD) calculates the gap between the histogram of the original image and the histogram of the encrypted image and it can be defined as [22]

$$HD = \frac{\sum_{i=0}^{255}|h_1(i) - h_2(i)|}{W \times H} \tag{11}$$

where W(Width) and H(Height) are the size of the image, and $h_1(i), h_2(i)$ define the histogram of original image and enciphered image at value i respectively. The higher the HD value is, the better.

The histogram of an ideal encrypted image should keep each pixel level containing the same pixels. For example, for a 512×512 encrypted image, each pixel level should contain $512 \times 512/256 = 1024$ pixels. The irregular deviation(ID) measures the gap between the histogram of the cipher image and the histogram of the ideal encrypted image. The equation is [22]

$$ID = \frac{\sum_{i=0}^{255}(|h(i) - M|)}{W \times H} \tag{12}$$

Table 3 CC, HD and ID of encrypted images

Image	CC	HD	ID
Cameramen	0.0025	1.008	0.1074
Peppers	-0.0005	0.6144	0.1074
Baboon	-0.0024	0.8303	0.1350
Lake	-0.0020	0.9616	0.1035
Lena	-0.0061	0.6735	0.1413

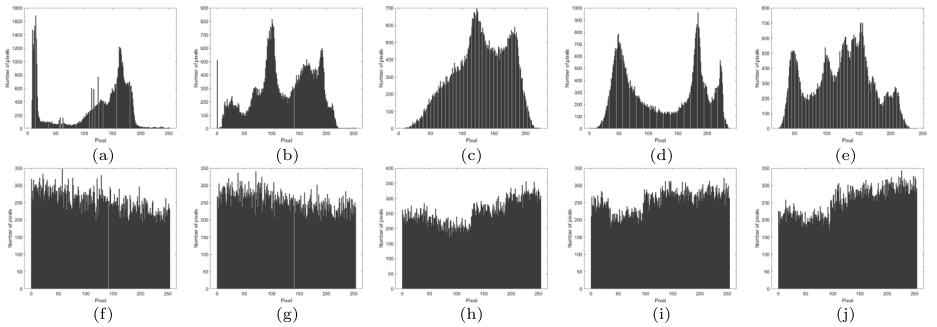

Fig. 10 Histograms of original images and cipher images. a: original Cameraman. b: original Peppers. c: original Baboon. d: cipher Lake. e: cipher Lena. f: cipher Cameraman. g: cipher Peppers. h:cipher Baboon. i:cipher Lake. j:cipher Lena

where $h(i)$ is enciphered image histogram at value i, and M is the average of an ideal enciphered image histogram. Given an image of size 256×256, M is set to 256. The smaller the ID value, the histogram of the encrypted image is closer to the histogram of the ideal encrypted image. Thus, the target is to attach the lower value of ID.

As shown in Table 3, the CC value of the encrypted Cameramen, Peppers, Baboon, Lake, Lena are 0.0025, -0.0005, -0.0024, -0.002 and -0.0061 respectively. It shows that the plain images and cipher images with a low correlation. The mean of HD is 0.8175. It shows that the difference between plain images and cipher images encrypted by the proposed scheme is large. The histograms of the cipher images are close to ideal histogram due to the ID values of five encrypted images are near to 0.1.

4.5 Histogram Analysis

The histograms of the plain images and cipher images are shown in Fig. 10. It proves that the histograms of the cipher images are different from the plain one. The cipher images have a uniformed histogram due to change the pixel value in time domain, which can resist statistical attacks better. The proposed scheme hides the histogram features well.

4.6 Differential Analysis

In order to resist differential attacks, a good encryption scheme should be sensitive to small changes in the key. There are two parameters used for differential analysis, namely Number

Table 4 NPCR and UACI of encrypted images

Image	NPCR(%)	UACI(%)
Cameramen	92.65	30.73
Peppers	99.58	33.17
Baboon	90.59	29.80
Lake	92.13	30.17
Lena	92.49	28.70

Table 5 The estimated entropy and others results of the proposed scheme and the related schemes in [15, 33–35]

Scheme	Entropy	CC	NPCR	UACI
Proposed	7.9854	-0.0005	99.58	33.17
[33]	7.9993	-0.0085	···	···
[34]	7.9973	0.0153	99.5300	33.5291
[15]	7.9969	-0.0062	···	···
[35]	7.9993	-0.0005	99.6213	33.4925

of Pixel Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI), described as follows [22]

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{13}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{E_1(i,j) - E_2(i,j)}{255}\right] \times 100\% \tag{14}$$

where E_1 and E_2 are two different cipher images of size $W \times H$. If the pixel values of E_1 and E_2 at position (i, j) are different, that is, $E_1(i, j) \neq E_2(i, j)$, then $D(i, j) = 1$. There will be a big gap between E_1 and E_2 if the values of NPCR and UACI are big and it shows that the proposed scheme is sensitive to key. The original key is used to encrypt the original image to obtain cipher image E_1. After that we exchange the position of the key n_2 and n_3, and keep other parameters unchanged. Then, the changed key is used to encrypt the original image to obtain cipher image E_2.

The results of NPCR and UACI are shown in Table 4. We observe that the values of NPCR are above 90%. For a 256 gray level image, the expected UACI value is 33% and the UACI value of the Peppers is 33.17%. It means our scheme can resist differential attacks well.

4.7 Comparative Analysis

To verify the safety of the proposed scheme, various experiments have been carried out to compare the security based on entropy, CC, NPCR and UACI.

The comparative study between the proposed quantum image encryption scheme and other similar quantum image encryption schemes is performed based on the image Peppers. The values of entropy, CC, NPCR and UACI are listed in Table 5 for the proposed and other schemes in [15, 33–35]. One can see that the image encrypted by the proposed scheme has the lowest CC value, that is, the correlation of the encrypted image is the lowest. In addition, the results of the experiment indicate that the other key indicators are approximately comparable to those of other scheme.

5 Conclusion

This paper proposed an image encryption scheme based on QFT and two chaotic maps. The proposed cryptographic system use the selecting encryption method to equalize histogram. If $C'_{YX} \geq T$ ($C'_{YX} < T$), it performs $U_{\oplus k}(U_{\oplus A})$ transformation, where the k and A are associated with the plain image. Then use QFT to transform the image to the frequency domain. Finally, we use a QBM to scramble the entire image. From the simulation results,

the keyspace of two chaotic maps is enough to resist brute-force attacks. The mean values of CC, HD and ID are 0.0027, 0.8175, 0,1189, which have been demonstrated the security of the proposed scheme. Change the pixel values in the time domain makes the histogram uniform. The key related to the plain image can effectively resist plaintext attacks. The values of NRCR are all above 90%, and the highest is 99.58%. The values of UACI are all around 30%, and the highest is 33.17%. That shows the proposed scheme is sensitive to key. However, this scheme still has some shortcomings, that is, the histogram of the encrypted image is not balanced enough. In the future, the encryption scheme can be optimized to obtain a more evenly distributed histogram.

Supplementary Information The online version contains supplementary material available at doi:10.1007/s10773-022-04979-1.

Acknowledgements The authors are supported by the Science and Technology Research Project of Higher Education of Hebei Province Nos. ZD2021011.

References

1. Feynman, R.P.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6), 467–488 (1982)
2. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. Inproceedings of 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 124-134" (1994)
3. Grover, L.K.: A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp 212–219 (1996)
4. Feng, H., Liu, B.J., Li, D., et al.: Traceable ring signatures: general framework and post-quantum security. Des. Codes Crypt., pp 1–35 (2021)
5. Wu, W.Q., Ma, X.X.: Quantum private comparison protocol without a third party. Int. J. Theor. Phys. **59**(6), 1854–1865 (2020)
6. Wu, W.Q., Zhao, Y.X.: Quantum private comparison of size using d-level Bell states with a semi-honest third party. Quantum information process **20**(4), 155 (2021)
7. Song, S.Y., Wang, C.: Recent development in quantum communication. Chin. Sci. Bull. **57**(36), 4694–4700 (2012)
8. Pirandola, S.: Bounds for multi-end communication over quantum networks. Quantum Science and Technology **4**(4), 045006 (2019)
9. Wang, Z., Xu, M., Zhang, Y.: Review of quantum image processing. Archives of Computational Methods in Engineering, pp 1–25 (2021)
10. Venegas-Andr, S.E., Storing, B.S.: Processing, and retrieving an image using quantum mechanics. The International Society for Optical Engineering **5105**, 137–147 (2003)
11. Le, P.Q., Iliyasu, A.M., Dong, F., et al.: A flexible representation of quantum images for polynomial preparation, image compression and processing operations. Quantum Inf. Process **10**(1), 63–84 (2011)
12. Zhang, Y., Kai, L., Gao, Y., et al.: NEQR: A novel enhanced quantum representation of digital images. Quantum Inf. Process **12**(8), 2833–2860 (2013)
13. Li, H.S., Zhu, Q., Zhou, R.G., et al.: Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. Quantum Inf. Process **13**(4), 991–1011 (2014)
14. Li, H.S., Song, S.X., Fan, P., et al.: Quantum vision representations and multi-dimensional quantum transforms. Inform. Sci. **502**, 42–58 (2019)
15. Liu, X.B., Xiao, D., Liu, C.: Three-level quantum image encryption based on Arnold transform and logistic map. Quantum Inf. Process **20**(1), 1–22 (2021)
16. Li, H.S., Chen, X., Song, S.X., et al.: A block-based quantum image scrambling for GNEQR. IEEE Access **7**, 138233–138243 (2019)
17. Luo, Y.L., Tang, S.B., Liu, J.X., et al.: Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt. Lasers Eng. **124**, 105836 (2020)
18. Yang, Y.G., Xia, J., Jia, X., et al.: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf. Process **12**(11), 3477–3493 (2013)

19. Hu, W.W., Zhou, R.G., et al.: Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. Quantum Inf. Process **19**(3), 1–29 (2020)
20. Du, S.P., Qiu, D.W., Mateus, P., et al.: Enhanced double random phase encryption of quantum images. Results in Physics **13**, 102161 (2019)
21. Musanna, F., Kumar, S.: Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quantum Inf. Process **19**(8), 220 (2020)
22. Allah, O., Afifi, A., ElShafai, W., et al.: Investigation of Chaotic Image Encryption in Spatial and frFT Domains for Cybersecurity Applications. IEEE Access **3**(99), 195–208 (2020)
23. Ramadan, N., Ahmed, H., ElKhamy, S.E., et al.: Permutation-substitution image encryption scheme based on a modified chaotic map in transform domain. J. Cent. South Univ. **24**(9), 2049–2057 (2017)
24. Sher, K.J., Jawad, A.: Chaos based efficient selective image encryption. Multidim. Syst. Sign. Process. **30**, 943–961 (2019)
25. Fridrich, J.iri.: Symmetric ciphers based on Two-Dimensional chaotic maps. International Journal of Bifurcation and Chaos **8**(06), 1259–1284 (1998)
26. Wang, X., Crisis, S.h.i.Q.: New type hysteresis and fractal in coupled logistic map. Chinese Journal of Applied Mechanics **22**, 501–506 (2005)
27. Henderson, H.V., Searle, S.R.: Vec and vech operators for matrices, with some uses in Jacobians and multivariate statistics. Canadian Journal of Statistics **7**(1), 65–81 (1979)
28. Zhang, Y., Kai, L., Gao, Y., et al.: NEQR: A novel enhanced quantum representation of digital images. Quantum Inf. Process **12**(8), 2833–2860 (2013)
29. Jiri, F.: Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos **8**(06), 1259–1284 (1998)
30. Henderson, H.V., Searle, S.: Vec and vech operators for matrices, with some uses in jacobians and multivariate statistics. Canadian Journal of Statistics **7**(1), 65–81 (1979)
31. Kashefi, E., Kent, A., Vedral, V., et al.: A comparison of quantum oracles. Phys. Rev. A **65**(5), 882–886 (2001)
32. Wang, X.Y., Shi, Q.J.: New type crisis: hysteresis and fractal in coupled logistic map. Chinese Journal of Applied Mechanics **22**(4), 501–505 (2005)
33. Gong, L.H., He, X.T., Cheng, S., et al.: Quantum image encryption algorithm based on quantum image XOR operations. Int. J. Theor. Phys. **55**, 3234–3250 (2016)
34. Liu, X.B., Xiao, D., Liu, C.: Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. Quantum Inf. Process **19**(8), 239 (2020)
35. Ye, G.D., Jiao, K.X., Huang, X.L., et al.: An image encryption scheme based on public key cryptosystem and quantum logistic map. Sci. Rep. **10**, 21044 (2020)
36. Li, H.S., Ping, F., Xia, H.Y., et al.: Quantum implementation circuits of quantum signal representation and type conversion. IEEE Transactions on Circuits Systems I Regular Papers **1**, 1–14 (2018)
37. Wang, X., Zhang, J., Cao, G.: An image encryption algorithm based on ZigZag transform and LL compound chaotic system Optics Laser Technology, 119:105581-105591 (2019)
38. Li, H.S., Song, S.X., Ping, F., et al.: Quantum vision representations and multi-dimensional quantum transforms. Inform. Sci. **502**, 42–58 (2019)
39. Liu, X.B., Xiao, D., Xiang, Y.P.: Quantum image encryption using intra and inter bit permutation based on logistic map. IEEE Access **7**, 6937–6946 (2018)
40. Zhou, N.R., Hua, T.X., Gong, L.H., et al.: Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process **14**, 1193–1213 (2015)
41. Wang, H., Wang, J., Geng, Y.C.: Quantum image encryption based on iterative framework of frequency-spatial domain transforms. Int. J. Theor. Phys. **56**, 3029–3049 (2017)