Quantum Inf Process (2013) 12:3477–3493
DOI 10.1007/s11128-013-0612-y

Novel image encryption/decryption based on quantum Fourier transform and double phase encoding

Yu-Guang Yang · Juan Xia · Xin Jia · Hua Zhang

Received: 22 March 2013 / Accepted: 9 July 2013 / Published online: 19 July 2013

Abstract A novel gray-level image encryption/decryption scheme is proposed, which is based on quantum Fourier transform and double random-phase encoding technique. The biggest contribution of our work lies in that it is the first time that the double random-phase encoding technique is generalized to quantum scenarios. As the encryption keys, two phase coding operations are applied in the quantum image spatial domain and the Fourier transform domain respectively. Only applying the correct keys, the original image can be retrieved successfully. Because all operations in quantum computation must be invertible, decryption is the inverse of the encryption process. A detailed theoretical analysis is given to clarify its robustness, computational complexity and advantages over its classical counterparts. It paves the way for introducing more optical information processing techniques into quantum scenarios.

Keywords Image processing · Double random-phase encoding · Encryption · Decryption · Quantum Fourier transform

1 Introduction

Image is one of the most important information representation models and widely used in modern society. With the rapid development of Internet technology and digital signal processing technology, the secure transmission of image data is becoming a

Y.-G. Yang (✉) · J. Xia · X. Jia
College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
e-mail: yangyang7357@bjut.edu.cn

H. Zhang
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

most important problem. Thus, image encryption is of great significance but of difference from traditional text encryption due to some inherent features of the image, such as bulk data capacity, high redundancy and strong correlation among adjacent pixels. A variety of image encryption schemes have ever been proposed, based on scan patterns methodology [1], double random-phase encoding (DRPE) [2], iterative random encoding and gyrator transformation [3], vector quantization [4], quadtree compression [5,6], chaos maps with total shuffling [7], Kolmogorov flow [8] and so on.

Optical processing systems may be useful for security applications owing to their ability to operate with high speed and in parallel and the characteristics of having various attributes such as amplitude, phase, wavelength, polarization and so on. However, up to date, most optical encryption systems are far from satisfactory. This is because there exist two following reasons. On the one hand, optical elements via free space transmission have big size, weak operating flexibility and stability. For example, the DRPE scheme has skew alignment drawbacks [9,10] and the encryption results as the complex amplitude distributions are difficult to store and transmit. On the other hand, most optical encryption systems have vulnerabilities against attacks. For example, the security of the DRPE method has been thoroughly analyzed and a few weaknesses and attacks have started to appear, including known plaintext attack [11,12], chosen ciphertext attack [13] and chosen-plaintext attack [14] and so on. Therefore, optical encryption systems should be used cautiously in practice.

As we know, cryptography is the approach to protect data secrecy in public environment. The security of most classical cryptosystems is based on the assumption of computational complexity and might be susceptible to the strong ability of quantum computation [15,16]. Fortunately, this difficulty can be overcome by quantum cryptography [17,18], where the security is assured by quantum physical principles such as Heisenberg uncertainty principle, quantum no-cloning theorem and so on. With the advantage of higher security, quantum cryptography has attracted a great deal of attention now.

Processing images on classical computers have been studied extensively. With the development of quantum computation, classical image processing is naturally extended to the quantum scenario. Research on quantum image processing started with proposals on quantum image representations such as Qubit Lattice [19,20], Real Ket [21] and Flexible Representation of Quantum Images (FRQI) [22]. On the other hand, classical frequency domain transformations have been proposed to be implemented on quantum computers such as quantum Fourier transform (QFT) [23], quantum discrete cosine transform (QDCT) [24,25], quantum Wavelet transform (QWT) [26], quantum fractional Walsh transform (QFWT) [27] and quantum discrete Hartley transform (QDHT) [28,29]. These quantum transforms are more efficient than their classical counterparts [23]. For example, as shown in Ref. [23], the quantum circuit provides a $\Theta(n^2)$ algorithm for performing the QFT. In contrast, the best classical algorithms for computing the discrete Fourier transform on 2^n elements are algorithms such as the *Fast Fourier Transform* (*FFT*), which compute the discrete Fourier transform using $\Theta(n2^n)$ gates. That is, it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the QFT on a quantum computer. The similar conclusions can be drawn for other quantum transforms. Table 1 summarizes the classical and quantum algorithm complexities for some representative transforms and applications.

Table 1 Comparisons between classical and quantum algorithm complexities

	Fourier transform	Discrete cosine transform	Wavelet transform	Fractional Walsh transform	Discrete Hartley transform	Search algorithm	Prime factorization
C	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n)$	$\exp(\Theta(n^{1/3}\log^{2/3} n))$
Q	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n)$	$\Theta(n^2)$	$\Theta(\sqrt{n})$	$\Theta(n^2 \log n \log\log n)$

In the first column, C denotes classical algorithm complexity, and Q for quantum algorithm complexity

However, there are some special classical image processing operations that cannot be applied on quantum images, for example convolution and correlation [30], because all operations in quantum computation must be invertible. Quantum transforms have been used for images processing directly [22,31–34].

To solve the drawbacks of the optical encryption systems and combine the merits of quantum cryptography, we propose a novel image encryption and decryption scheme based on QFT and DRPE proposed by Refregier and Javidi [2]. Due to the properties of quantum parallel computation, the use of quantum transforms speeds up the image encryption and decryption procedures. A detailed theoretical analysis is given to clarify its robustness, computational complexity and advantages over its classical counterparts.

The outline of this work is as follows. In Sect. 2, a novel and flexible quantum representation for gray-level images (FQRGI) is introduced. Section 3 introduces the proposed quantum encryption and decryption scheme. Section 4 is devoted to classical simulation and performance comparison. Finally, the conclusion is drawn in Sect. 5.

2 Flexible quantum representation for gray-level images (FQRGI)

The properties of gray information and position are extracted from the gray-level image to generate a representation of image in quantum states as follows,

$$|I(\theta)\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes |j\rangle, \tag{1}$$

$$|c_j\rangle = \left(|0\rangle + e^{i\theta_j}|1\rangle\right), \tag{2}$$

where $\theta_j \in \left[0, \frac{\pi}{2}\right]$, $j = 0, 1, \ldots, 2^{2n}-1$, $|0\rangle$, $|1\rangle$ are two dimensional computational basis quantum states, $(\theta_0, \theta_1, \ldots, \theta_{2^{2n}-1})$ is the vector of phases encoding information about gray-level information, and $|j\rangle$, for $j = 0, 1, \ldots, 2^{2n}-1$ are 2^{2n} dimensional computational basis quantum states. There are two parts in the quantum image representation: $|c_j\rangle$ and $|j\rangle$ which encode gray-level information and their corresponding positions in the image, respectively. To perform operation on gray-level information, a phase gate $U = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\psi_j} \end{bmatrix}$ can be performed on $|c_j\rangle$.

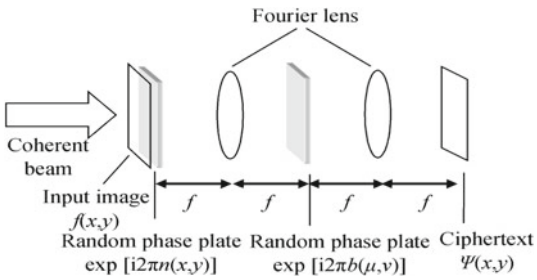

Fig. 1 Encoding procedure

For two dimensional images, the location information encoded in the position qubit $|j\rangle$ includes two parts; the vertical and horizontal co-ordinates. In $2n$-qubit systems for preparing quantum images, or n-sized images, the vector

$$|j\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2}\dots y_0\rangle|x_{n-1}x_{n-2}\dots x_0\rangle, \quad x_j, y_j \in \{0, 1\}$$

for every $j = 0, 1, \dots, 2^{2n} - 1$ encodes the first n-qubit $y_{n-1}y_{n-2}\cdots y_0$ along the vertical location and the second n-qubit $x_{n-1}x_{n-2}\cdots x_0$ along the horizontal axis.

3 Quantum image encryption and decryption scheme

In this section, we will first review the DRPE technique [2]. Then we will introduce its idea into our quantum encryption and decryption strategies.

3.1 DRPE technique

The DRPE technique was proposed by Refregier and Javidi in 1995 [2]. This method allows one to encode a primary image into a stationary white noise, which has been receiving much interest because of its high-level data security. The encoding procedure is given by the following steps and can be shown in Fig. 1.

Assume $f(x, y)$ is the plaintext image and the size is $M \times N$, $\varphi(x, y)$ is the cipher image. The formulas of the encoding and decoding procedures are given respectively as follows:

$$\varphi(x, y) = FT^{-1}\{FT\{f(x, y)\exp[j2\pi n(x, y)]\}\exp[j2\pi b(\xi, \eta)]\}, \tag{3}$$
$$f(x, y) = FT^{-1}\{FT\{\varphi(x, y)\}\exp[-j2\pi b(\xi, \eta)]\}\exp[-j2\pi n(x, y)], \tag{4}$$

where $n(x, y)$ and $b(\xi, \eta)$ are the two random-phase functions in spatial domain and frequency domain, respectively, which are uniformly distributed in [0; 1]. FT and FT^{-1} represent the Fourier transform and its inverse Fourier transform, respectively. $f(x, y)$ denotes the plaintext image, which is a complex image.

The basic principle of this technique is as follows. Two unrelated random phase marks (RPM, i.e. $\exp[j2\pi n(x, y)]$ and $\exp[j2\pi b(\xi, \eta)]$) act as the keys to be applied on the input plane and Fourier spectrum plane respectively, as shown in Fig. 1. The

input image is encrypted to get the encrypted image on the output plane. The encrypted image is complex-amplitude stationary white noise. The cipher image cannot be decrypted successfully by any unauthorized people without keys, thus the security of the image is protected well. If only the first RPM is used to encrypt the original image, the encrypted image is white but nonstationary and not encoded. If one only uses the second RPM on the Fourier spectrum plane to encrypt image, the encrypted image can easily be deciphered.

To learn the DRPE technique further, refer to Ref. [2] for details. There is no spectrum apodization in the Fourier domain, and this method leads to a robust reconstruction of the primary image as well as to high optical efficiency and robustness against blind deconvolution. This is an attractive optical technique for high-security applications. However, as mentioned above, the DRPE scheme is far from satisfactory because of its skew alignment drawbacks and the difficulty of storing and transmitting the encryption results as the complex amplitude distributions. In addition, the security of the DRPE scheme has been thoroughly analyzed and been found a few weaknesses and attacks mentioned above [11–14]. Therefore, there exists the difficulty in practical use for the DRPE scheme.

3.2 Quantum image encryption

As shown in Sect. 2, we just take the gray-level information of quantum image into consideration. A quantum image is written as $|I(\theta)\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle \otimes |j\rangle$, where $|c_j\rangle$ represents the vectors in color space. Assume the plaintext quantum image is $|\mathrm{O}\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|c_j\rangle \otimes |j\rangle$, the keys for spatial and QFT domain are phase operations $U_{K_1} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\psi_j} \end{bmatrix}$ and $U_{K_2} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\upsilon_j} \end{bmatrix}$, respectively. Here ψ_j, υ_j are real numbers and distributed uniformly between 0 and 2π.

Step 1. Encode the original plaintext image in spatial domain to get $|M\rangle$ using the key K_1.

$$\begin{aligned} |M\rangle &= K_1|\mathrm{O}\rangle = U_{K_1} \otimes I_{2^{2n}}|\mathrm{O}\rangle \\ &= U_{K_1} \otimes I_{2^{2n}} \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |c_j\rangle \otimes |j\rangle \\ &= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} U_{K_1}|c_j\rangle \otimes |j\rangle \\ &= \frac{1}{2^n} \sum_{j=0}^{2^{2n}-1} |d_j\rangle \otimes |j\rangle. \end{aligned} \tag{5}$$

Here, $|d_j\rangle = \left(|0\rangle + e^{i(\theta_j+\psi_j)}|1\rangle\right)$.

Step 2. Execute QFT on $|M\rangle$ to get its QFT $QFT\,(|M\rangle)$ shown as follows.

$$QFT\,(|M\rangle) = QFT\left(\frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|d_j\rangle \otimes |j\rangle\right). \tag{6}$$

Here, the QFT on an orthonormal basis $|0\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$QFT : |j\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle. \tag{7}$$

Step 3. Encrypt $QFT\,(|M\rangle)$ using the key K_2, and get $|M_1\rangle$.

$$\begin{aligned}|M_1\rangle &= K_2 QFT\,(|M\rangle)\\ &= U_{K_2} \otimes I_{2^{2n}} QFT\,(|M\rangle)\\ &= U_{K_2} \otimes I_{2^{2n}} QFT\left(\frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|d_j\rangle \otimes |j\rangle\right)\\ &= \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} U_{K_2} QFT\left(|d_j\rangle \otimes |j\rangle\right).\end{aligned} \tag{8}$$

Step 4. Execute the inverse QFT to get the quantum cipher image $|C\rangle$ what we expect as follows.

$$\begin{aligned}|C\rangle &= inQFT\,(|M_1\rangle)\\ &= inQFT\left(\frac{1}{2^n}\sum_{j=0}^{2^{2n}-1} U_{K_2} QFT\left(|d_j\rangle \otimes |j\rangle\right)\right).\end{aligned} \tag{9}$$

Here the inverse QFT is the implementation of the quantum circuit of QFT in the reverse order.

The quantum image encryption procedures can be implemented by the following quantum circuit, as shown in Fig. 2.

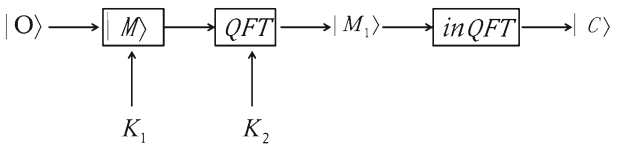

Fig. 2 The quantum image encryption circuit

3.3 Quantum image decryption

In this phase, only two keys are needed to decrypt the cipher image, i.e. the phase operations U_{K_1} and U_{K_2}. Because all the transformations used in quantum computation are unitary transformations, the encryption procedure is completely reversible. Our decrypting procedure is as follows.

Step 1. Execute QFT on $|C\rangle$, and get $QFT\,(|C\rangle)$ shown as follows.

$$QFT\,(|C\rangle) = QFT\,(inQFT\,(|M_1\rangle)) = |M_1\rangle. \tag{10}$$

Step 2. Perform the decryption operation on $|M_1\rangle$ using the key K_2 shown as follows.

$$\begin{aligned} K_2^{-1}|M_1\rangle &= U_{K_2}^{+} \otimes I_{2^{2n}}|M_1\rangle \\ &= U_{K_2}^{+} \otimes I_{2^{2n}} K_2 QFT\,(|M\rangle) \\ &= (U_{K_2}^{+} \otimes I_{2^{2n}})(U_{K_2} \otimes I_{2^{2n}})QFT\,(|M\rangle) \\ &= U_{K_2}^{+}U_{K_2} \otimes I_{2^{2n}} QFT\,(|M\rangle) \\ &= QFT\,(|M\rangle)\,. \end{aligned} \tag{11}$$

Step 3. Execute the inverse QFT to get $|M\rangle$ shown as follows.

$$inQFT\,(QFT\,(|M\rangle)) = |M\rangle. \tag{12}$$

Step 4. Perform the inverse operation on $|M\rangle$ using the key K_1 to get the quantum plaintext image $|\mathrm{O}\rangle$ as follows.

$$\begin{aligned} K_1^{-1}|M\rangle &= U_{K_1}^{+} \otimes I_{2^{2n}}|M\rangle \\ &= U_{K_1}^{+} \otimes I_{2^{2n}} K_1|\mathrm{O}\rangle \\ &= (U_{K_1}^{+} \otimes I_{2^{2n}})(U_{K_1} \otimes I_{2^{2n}})|\mathrm{O}\rangle \\ &= U_{K_1}^{+}U_{K_1} \otimes I_{2^{2n}}|\mathrm{O}\rangle \\ &= |\mathrm{O}\rangle. \end{aligned} \tag{13}$$

4 Numerical simulation

We will give a detailed theoretical analysis to clarify its robustness, computational complexity and advantages over its classical counterparts.

Since a practical and useful quantum computer is unavailable, we cannot clearly say what the hardware will be like. Nevertheless, we can assume that any practical quantum computer will have an in-built error correction mechanism to protect the

quantum information from errors due to uncontrolled interactions with the environment, or due to imperfect implementations of the quantum logical operations [23,35]. It may be possible to incorporate intrinsic fault tolerance into the design of quantum computing hardware.

The simulations are based on linear algebraic constructions. To simulate the quantum effects such as quantum entanglement or superposition, the complex vectors are used, and the image processing operations are simulated by the unitary matrices. The final step in these simulations is the measurement, which converts the quantum information into the classical information in form of probability distributions. Extracting and analyzing these distributions gives information for retrieving the transformed images [22,36].

MATLAB is a mathematical software. It facilitates the representation and manipulation of large arrays of vectors and matrices which makes it a good tool for simulating quantum states (such as our images) and their transformations. In particular, by treating the quantum images as large matrices the required simulation of their transformation using linear algebraic constructions equivalent to the quantum circuit elements is possible. MATLAB's Image Processing Toolbox provides a set of graphical tools for image processing, analysis, visualization, and algorithm development using which these images and circuit to manipulate them, can be effectively simulated. The results reported in this section are based on classical simulation experiments using a dataset of five different images.

In this section, the simulations are analyzed from two aspects. Firstly, in order to understand the encryption algorithm and prove that our scheme is reliable and secure, we give a classical numerical simulation. Secondly, we make a comparison between optical image encryption based on DRPE technique and our scheme in terms of security, robustness and computational complexity to demonstrate the advantage of the proposed quantum encryption scheme.

4.1 Evaluation of the proposed scheme

Classical numerical simulation has been implemented on a plaintext image, which consists of 256×256 pixels. Experiments are performed on a laptop with Intel(R) Core(TM) 2 Duo CPU P7450 2.13 GHz 1.99 GB RAM equipped with the MATLAB R2012a environment.

The plaintext image is shown in Fig. 3a, and the corresponding cipher image is shown in Fig. 3b.

An ideal encryption scheme should resist against all kinds of attacks such as statistical attacks, brute-force attacks, differential attacks, cipher only attacks and the known plaintext attacks, etc. According to the basic principles of cryptology, a desirable encryption scheme requires sensitivity to cipher keys, that is, the cipher should have close correlation with the keys. In this section, the key sensitivity analysis and statistical analysis on the proposed image encryption scheme are discussed. All the analyses show that the proposed image encryption scheme is highly secure thanks to its large key space and satisfactory permutation–diffusion architecture.

Fig. 3 **a** The plaintext image, **b** the cipher image

4.1.1 Key sensitivity analysis

A good image encryption algorithm should be sensitive to the cipher key, and the key space should be sufficiently large to make brute-force attack ineffective. It is recommended in Ref. [37] that the ideal key space should be larger than 2^{100} while considering the current computer computation speed. In our cryptosystem, the key space is as large as the plaintext image, and the keys are two independent white sequence uniformly distributed in [0, 1], which represent the key of spatial domain and QFT frequency domain, respectively.

Key sensitivity is an essential property for any good cryptosystem, which ensures the security of the cryptosystem against the brute-force attack. The key sensitivity of a cryptosystem can be observed from two aspects: (i) the attacker employs slightly different keys to decrypt the cipher image so that the decryption will fail to obtain the plaintext image; (ii) the cipher image produced by the cryptosystem should be sensitive to the secret key, i.e., if the attacker uses two slightly different keys to encrypt the same plaintext image, then the two cipher images should be completely independent to each other.

We will use the following three kinds of keys to decrypt the cipher image in order to analyze the keys' sensitivity: (i) the spatial and frequency domain keys are all right; (ii) the right frequency domain key while the spatial domain key is wrong; and (iii) the right spatial domain key with the wrong frequency domain key. The results of the simulations are shown in Fig. 4. From the results, we can clearly see that the keys decide the results. We can get the absolutely correct plaintext image when the spatial and frequency domain key are all right, which is shown in the left of Fig. 4. With a similar spatial domain key and the right frequency domain key, we get another independent white sequence uniformly distributed in [0, 1], which is shown in the middle of Fig. 4. From the results we can still see the outline of the plaintext image, but very blurry. Finally, we use the right spatial domain key and generate a similar random matrix as the wrong frequency domain key so that the decrypted image is a random noise, which is shown in the right of Fig. 4.

Obviously, the decryption using a very similar key completely fails to obtain the plaintext image. Because the key distribution is unknown for a large key space, the

Fig. 4 Results for tests of keys' sensitivity

plaintext image cannot be recovered even though there is a slight difference between the encryption keys and the decryption keys, which ensures the double random phase encryption to have high security.

4.1.2 Statistical analyses

The statistical analyses on the cipher image are of crucial importance for a cryptosystem. An ideal cryptosystem should be robust against any statistical attacks. In order to prove the security of the proposed encryption scheme, the adjacent pixel correlation analysis and the histogram analysis on the proposed image encryption scheme are discussed in this section.

4.1.2.1 Correlation among adjacent pixels

Each pixel in the plaintext image is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. An ideal encryption design should produce the cipher images with no such correlation in the adjacent pixels. We have computed the correlation coefficients for horizontally, vertically and diagonally adjacent pixels, respectively. The formulas of correlation coefficients are given as:

$$cov(x, y) = E\{(x - E(x))(y - E(y))\}, \tag{14}$$

$$C_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}}, \tag{15}$$

where x and y are gray-level values of two adjacent pixels in the image. $E(x) = \frac{1}{N}\sum_{i=1}^{N} xi$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$. Then the same operations are performed along the vertical and the diagonal directions.

The visual test of the correlation of adjacent pixels can be done by plotting the distribution of the adjacent pixels in the plaintext image and its corresponding cipher image. We select 10,000 pairs of adjacent pixels in each direction from the plaintext image and its cipher image randomly. We have shown the distribution of horizontally, vertically and diagonally adjacent pixels in the plaintext image 'Lena' and its corresponding cipher image in Figs. 5, 6 and 7, respectively. The correlation coefficients

Table 2 The correlation coefficients results of the plaintext image 'Lena' and its cipher image

The plaintext image (Lena)			The cipher image		
Horizontally	Vertically	Diagonally	Horizontally	Vertically	Diagonally
0.9660	0.9660	0.8908	−0.0165	−0.0165	0.0297

results in horizontally, vertically and diagonally adjacent pixels of plaintext image 'Lena' and its corresponding cipher image are shown in Table 2. It is clear that the correlation coefficients for the test cases are very small (or approximately zero) and hence no correlation between the plaintext image and its corresponding cipher image exists. From Figs. 5, 6, and 7, we can clearly know that the plaintext image has strong correlation, while the correlation of the corresponding cipher image is random.

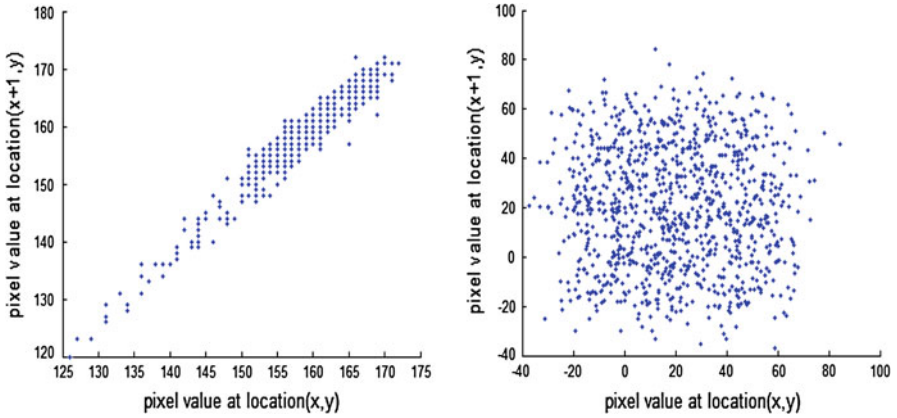

Fig. 5 The *left* is the distribution of horizontally adjacent pixels in the plaintext image and the *right* is the distribution of horizontally adjacent pixels in the corresponding cipher image

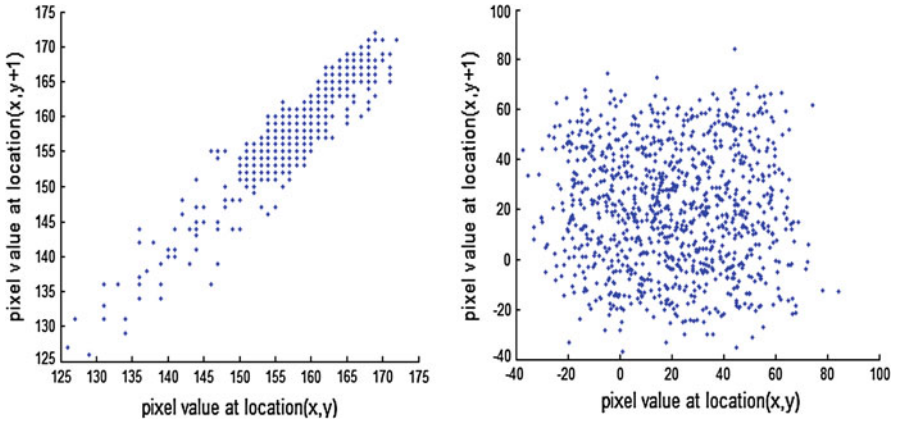

Fig. 6 The *left* is the distribution of vertically adjacent pixels in the plaintext image and the *right* is the distribution of vertically adjacent pixels in the corresponding cipher image

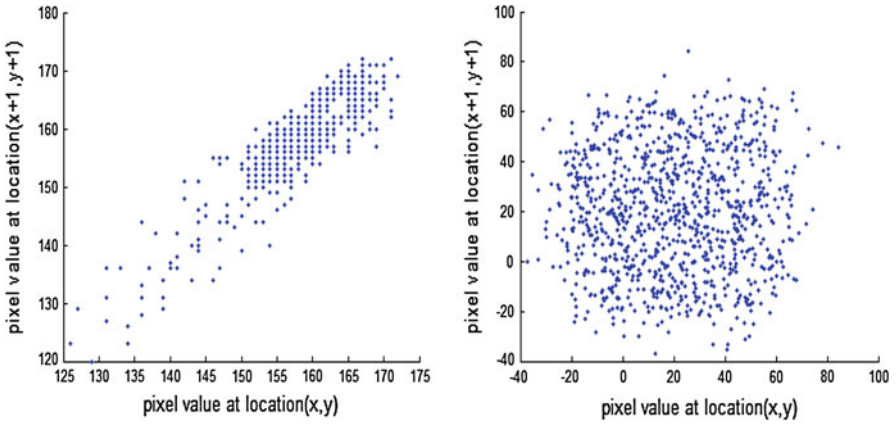

Fig. 7 The *left* is the distribution of diagonally adjacent pixels in the plaintext image and the *right* is the distribution of diagonally adjacent pixels in the corresponding cipher image

4.1.2.2 Histogram

Gray histogram is one of the simplest tools extensively used in digital image processing. It describes an image's gray content. An image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each gray level. An image histogram includes considerable information. Some types of images can be completely described by the histogram. The distribution of the cipher is of much importance. More specifically, it should hide the redundancy of the plaintext and should not leak any information about the plaintext or the relationship between the plaintext and its cipher.

Here we plot the histograms of the plaintext image and the corresponding cipher image as shown in Figs. 8 and 9, respectively. It is clearly seen that the histogram of the cipher image is fairly uniform and significantly different from that of the plaintext image so that it does not provide any clue to statistical attacks.

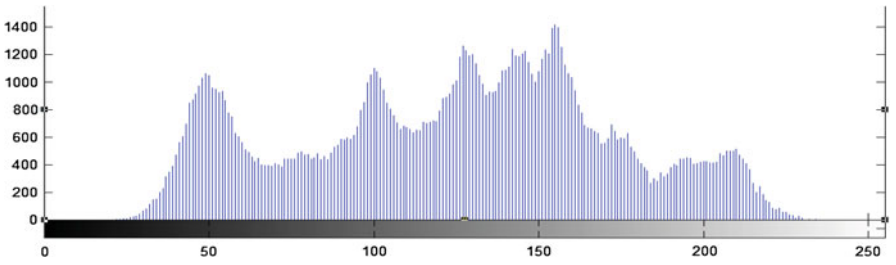

Fig. 8 The histogram of the plaintext image

4.2 Comparison with the classical image encryption based on DRPE technique

4.2.1 Comparison in terms of statistical analyses

We have proposed many parameters when analyzing the performance of image-encryption techniques. From those parameters, the criteria adopted for measuring the performance of our scheme are summarized below.

- Key space: An ideal encryption scheme should have a large key space to make brute-force attack infeasible.
- Security: An ideal encryption scheme should well resist various kinds of attacks like statistical attack, differential attack, etc.
- High sensitivity: A desirable encryption scheme requires high sensitivity to cipher keys, i.e., the cipher text should have a close correlation with the keys.

These parameters are somewhat dependent on each other. However, our comparison will be focused on them separately. Results of simulation experiments using the proposed image encryption scheme as reported in the preceding section will be used as the basis of our comparison with the optical method using DRPE technique. The reason of selecting the method based on DRPE technique for performance comparison is that because our proposed quantum encryption scheme is the generalization of the method based on DRPE technique to quantum scenarios, it can demonstrate representatively the advantage of the proposed quantum encoding scheme.

We will explain how classical numerical simulation can demonstrate the advantage of the proposed quantum encoding scheme. First, we easily find that the proposed quantum encryption scheme has a large key space. This is because ψ_j and υ_j are real numbers and distributed uniformly between 0 and 2π, which implies a very large key space.

At last, let us make a comparison between correlation of the quantum scheme and the method using the DRPE technique for six images, as shown in Table 3.

From Table 3, we can easily see that our quantum encryption scheme has a better performance than the method using the DRPE technique for six images as experiments. For example, for the image canoe, horizontal correlation using the method based on the DRPE technique is -0.0663, while it is -0.0157 in the proposed quantum encryption scheme; diagonal correlation using the method based on the DRPE technique is -0.0450, while it is -0.0355 in the proposed quantum encryption scheme; vertical

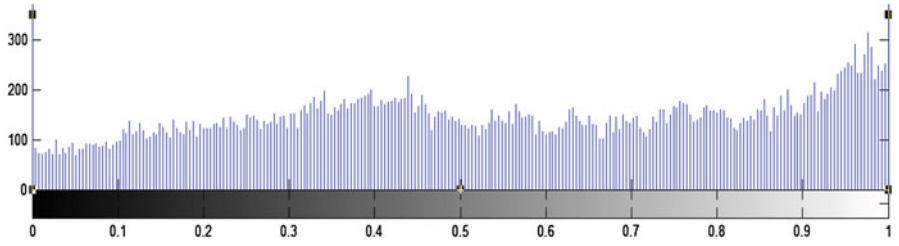

Fig. 9 The histogram of the cipher image

Table 3 Comparisons between correlation of quantum scheme and the method using the DRPE technique for six images

Encrypted images	Horizontal correlation		Diagonal correlation		Vertical correlation	
	DRPE	Quantum	DRPE	Quantum	DRPE	Quantum
canoe.jpg	−0.0663	−0.0157	−0.0450	−0.0355	0.0703	−0.0373
pepper.jpg	−0.0261	−0.0057	0.0302	0.0275	0.0048	−0.0377
football.jpg	−0.0374	0.0136	−0.0162	0.0341	−0.0060	0.0227
pears.jpg	0.0035	−0.0194	0.0136	0.0030	0.0205	−0.0481
lena.jpg	−0.0071	−0.0070	0.0421	−0.0633	−0.0199	−0.0232
baboon.jpg	0.0161	0.0344	0.0149	−0.0164	−0.0039	−0.0015

correlation using the method based on the DRPE technique is 0.0703, while it is −0.0373 in the proposed quantum encryption scheme.

4.2.2 Comparison in terms of robustness

Maybe the numerical simulations above are not enough to show the claims and supposed benefits of the proposed quantum image encryption/decryption scheme. Now from the basic principles of quantum mechanics we will explain why the proposed quantum encryption scheme is secure and robust. As we know, the reason why classical encryption technique is useful in modern society is that it can safeguard the classical data from unauthorized modification and eavesdropping. Classical data cannot change irreversibly whether the adversary adopts any active or passive attack strategy. Therefore, even if the classical data have suffered the attack, the legitimate parties cannot detect this fact. In contrast, because of the quantum no-cloning theorem, it is impossible to directly copy the information encoded in an unknown quantum state. Moreover, according to the quantum uncertainty of the quantum measurement theory, if one measures an unknown quantum state, it will collapse irreversibly. If the adversary wants to obtain the information about the quantum state, he has to measure it, which will make the quantum state collapse randomly into an eigenstate of the measurement operators irreversibly. Therefore, the principles of quantum mechanics ensure the security and robustness of the proposed quantum encryption scheme.

In contrast, the DRPE scheme is far from satisfactory because of its skew alignment drawbacks and the difficulty of storing and transmitting the encryption results as the complex amplitude distributions. Moreover, the security of the DRPE scheme has been thoroughly analyzed and been found a few weaknesses and attacks mentioned above [11–14]. Therefore, there exists the difficulty in practical use for the DRPE scheme.

4.2.3 Comparison in terms of computational complexity

Now let us first compute the computational complexity of the classical algorithm. According to Eq. (3), $\varphi(x, y) = FT^{-1}\{FT\{f(x, y)\exp[j2\pi n(x, y)]\}\exp[j2\pi b(\xi, \eta)]\}$, FT and FT^{-1} represent the Fourier transform and its inverse

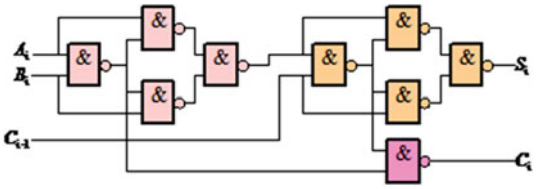

Fig. 10 The logic diagram of a full adder

Fourier transform, respectively. $f(x, y)$ denotes the $M \times N$ plaintext image. For simplicity, let $M = N$. There are N^2 pixels in a plaintext image. How many operations does this encryption use? We start by doing N^2 multiplications of $f(x, y)$ and $\exp[j2\pi n(x, y)]$. Then we perform a Fourier transform on $f(x, y) \exp[j2\pi n(x, y)]$, using N^4 complex multiplication operations. Next we further do N^2 multiplications of $FT\{f(x, y) \exp[j2\pi n(x, y)]\}$ and $\exp[j2\pi b(\xi, \eta)]$. At last we perform an inverse Fourier transform on $FT\{f(x, y) \exp[j2\pi n(x, y)]\} \exp[j2\pi b(\xi, \eta)]$. Because the computational complexity is same for Fourier transform and its inverse, computing an inverse Fourier transform on $FT\{f(x, y) \exp[j2\pi n(x, y)]\} \exp[j2\pi b(\xi, \eta)]$ needs N^4 complex multiplication operations. We see that to realize the encryption algorithm the total operations $N^2+N^4+N^2+N^4 = 2N^2(N^2+1)$ are required. Assume $f(x, y)$ is a 256×256 plaintext image, i.e., $N = 256$, the number of the total operations is $2 \times 256^2(256^2 + 1) \approx 8589934592$. For an $n \times n$ multiplier, $n(n - 1)$ full adders and n^2 AND gates are required. Figure 10 is the logic diagram of a full adder. To realize a full adder, 9 AND gates and 9 NOT gates are required.

It is obviously seen that the gates used by the classical algorithm is huge amazingly. Therefore, the classical algorithm has a computational complexity of $\Theta(N^8)$ gates.

Next let us compute the computational complexity of the quantum encryption algorithm. We start by doing a phase operation U_{K_1} on the first qubit. This is followed by a QFT operation on the $(2n + 1)$ qubits. As we know [13], the quantum circuit provides a $\Theta(n^2)$ algorithm for performing the QFT. Then another phase operation U_{K_2} is done on the first qubit. At last, an inverse QFT is performed on the $(2n + 1)$ qubits. Therefore, the quantum encryption algorithm has a computational complexity of $\Theta(n^2)$ gates.

It is easily seen that the computational complexity of the two encryption schemes depends on that of the Fourier transform. Even if we use the best classical *FFT* algorithm to compute the discrete Fourier transform on 2^n elements, it computes the discrete Fourier transform using $\Theta(n2^n)$ gates. In contrast, the quantum circuit provides a $\Theta(n^2)$ algorithm for performing the QFT. That is, it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the QFT on a quantum computer. This implies that the proposed quantum encryption scheme takes advantage over its classical counterparts in terms of security, robustness and computational complexity.

5 Conclusion

In this paper, we have proposed a novel image encryption and decryption scheme based on QFT and DRPE. We uses one phase coding in the quantum image domain and another phase coding in the QFT domain to perform double quantum image encryption. The two random-phase encodings are used as the keys to enhance the security of the proposed scheme. Because all operations in quantum computation must be invertible, decryption is the inverse of the encryption process. Numerical simulations and theoretical analyses are given to clarify its robustness, computational complexity and advantages over its classical counterparts. It paves the way for introducing more optical information processing techniques into quantum scenarios.

Acknowledgments We thank the anonymous reviewer for his constructive suggestions. This work is supported by the National Natural Science Foundation of China (Grant No. 61003290); Beijing Natural Science Foundation (Grant No. 4122008); Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality (No. CIT&TCD201304039).

References

1. Bourbakis, N., Alexopoulos, C.: Picture data encryption using SCAN pattern. Pattern Recognit. **25**(6), 567–581 (1992)
2. Refregier, R., Javidi, B.: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20**(7), 767–769 (1995)
3. Liu, Z., Guo, Q., Xu, L., Ahmad, M.A., Liu, S.: Double image encryption by using iterative random binary encoding in gyrator domains. Opt. Exp. **18**(11), 12033–12043 (2010)
4. Chang, C.C., Hwang, M.S., Chen, T.S.: A new encryption algorithm for image cryptosystems. J. Syst. Softw. **58**(7), 83–91 (2001)
5. Chang, H.K.L., Liu, J.L.: A linear quad tree compression scheme for image encryption. Signal Process. **10**(4), 279–290 (1997)
6. Cheng, H., Li, X.B.: Partial encryption of compressed image and videos. IEEE Trans. Signal Process. **48**(8), 2439–2451 (2000)
7. Zhang, G., Liu, Q.: A novel image encryption method based on total shuffling scheme. Opt. Commun. **284**(12), 2775–2780 (2011)
8. Scharinger, J.: Fast encryption of image data using chaotic Kolmogorov flow. J. Electron. Eng. **7**(2), 318–325 (1998)
9. Wang, B., Sun, C.-C., Su, W.-C.: Shift-tolerance property of an optical double-random phase-encoding encryption system. Appl. Opt. **39**(26), 4788–4793 (2000)
10. Bahram, J., Arnaud, S., Guanshen, Z., et al.: Fault tolerance properties of a double phase encoding encryption technique. Opt. Eng. **36**(4), 992–998 (1997)
11. Frauel, Y., Castro, A., Naughton, T., et al.: Resistance of the double random phase encryption against various attacks. Opt. Exp. **15**(16), 10253–10265 (2007)
12. Peng, X., Zhang, P., Wei, H., et al.: Known-plaintext attack on optical encryption scheme based on double random phase keys. Opt. Lett. **31**(8), 1044–1046 (2006)
13. Carnicer, A., Montes-Usategui, M., Arcos, S., et al.: Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. Opt. Lett. **30**(13), 1644–1646 (2005)
14. Peng, X., Wei, H., Zhang, P.: Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. Opt. Lett. **31**(22), 3261–3263 (2006)
15. Shor, P.W.: In Proceedings of 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mex-ico, p. 124 (1994)
16. Grover, L.K.: In Proceedings of 28th Annual ACM Symposium on Theory of Computing, New York, p. 212 (1996)
17. Bennett, C.H., Brassard, G.: In Proceedings of IEEE International Conference on Computers, Systems and Signal, Bangalore, India, p.175 (1984)

18. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002)
19. Venegas-Andraca, S.E., Ball, J.L.: Processing images in entangled quantum systems. Quantum Inf. Process. **9**(1), 1–11 (2010)
20. Venegas-Andraca, S.E., Bose, S.: Storing, processing and retrieving an image using quantum mechanics. In: Proceedings of the SPIE Conference Quantum Information and Computation, pp. 137–147 (2003)
21. Latorre, J.I.: Image compression and entanglement, arXiv:quant-ph/0510031(2005)
22. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**(1), 63–84 (2011)
23. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, New York (2000)
24. Klappenecker, A., Rotteler, M.: Discrete cosine transforms on quantum computers. In: Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis, pp. 464–468 (2001)
25. Tseng, C.C., Hwang, T.M.: Quantum circuit design of 8×8 discrete cosine transforms using its fast computation on graph. In: Proceedings of ISCAS 2005, pp. 828–831 (2005)
26. Fijany, A., Williams, C.P.: Quantum wavelet transform: fast algorithm and complete circuits, URL: arXiv:quantph/9809004 (1998)
27. Labunets, V., Labunets-Rundblad, E., Egiazarian, K., Astola, J.: Fast classical and quantum fractional Walsh transforms. In: Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis, pp. 558–563 (2001)
28. Tseng, C.C., Hwang, T.M.: Quantum circuit design of 8×8 discrete Hartley transform. ISCAS **III**, 397–400 (2004)
29. Tseng, C.C., Hwang, T.M.: Quantum circuit design of discrete Hartley transform using recursive decomposition formula. ISCAS **1–6**, 824–827 (2005)
30. Lomont, C.: Quantum convolution and quantum correlation algorithms are physically impossible, arXiv:quantph/0309070 (2003)
31. Iliyasu, A.M., et al.: Watermarking and authentication of quantum images based on restricted geometric transformations. Inf. Sci. **186**(1), 126–149 (2012)
32. Zhang, W.-W., Gao, F., Liu, B., Wen, Q.-Y., Chen, H.: A watermark strategy for quantum images based on quantum Fourier transform. Quantum Inf. Process. **12**(2), 793–803 (2013)
33. Zhou, R.G., Wu, Q., Zhang, M.Q., Shen, C.Y.: Quantum image encryption and decryption algorithms based on quantum image Geometric transformations. Int. J. Theor. Phys. **52**(6), 1802–1817 (2012)
34. Yang, Y.G., Jia, X., Xu, P., Tian, J.: Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform. Quantum Inf. Process. doi:10.1007/s11128-013-0561-5 (2013)
35. Gaitan, F.: Quantum Error Correction and Fault Tolerant Quantum Computing. CRC Press, Taylor and Francis Group, UK (2008)
36. Yan, F., Le, P.Q., Iliyasu, A.M., Sun, B., Garcia, J.A., Dong, F., Hirota, K.: Assessing the similarity of quantum images based on probability measurements. In 2012 IEEE World Congress on Computational Intelligence, Brisbane, 10–15 June 2012, pp. 1–6 (2012)
37. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcat. Chaos **16**(8), 2129–2151 (2006)