Measurement 73 (2015) 352–359

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Least significant qubit (LSQb) information hiding algorithm for quantum image

Shen Wang [a,*], Jianzhi Sang [a], Xianhua Song [b], Xiamu Niu [a]

[a] School of Computer Science and Technology, Harbin Institute of Technology, China
[b] Department of Applied Mathematics, Harbin University of Science and Technology, China

ARTICLE INFO

Article history:
Received 22 March 2015
Received in revised form 14 May 2015
Accepted 29 May 2015
Available online 8 June 2015

Keywords:
Quantum computation
Quantum image information hiding
Least significant qubit (LSQb)
Quantum Fourier transform

ABSTRACT

Quantum computation has the ability to solve some problems that are considered inefficient in classical computer. Research on Quantum image processing has been extensively exploited in recent decades. Quantum image information hiding can be divided into quantum image digital watermarking, quantum image steganography, anonymity and other branches. Least significant bit (LSB) information hiding plays an important role in classical world because many information hiding algorithms are designed based on it. In this paper, based on novel enhanced quantum representation (NEQR), the concrete least significant qubit (LSQb) information hiding algorithm for quantum image is given firstly. Because information hiding located on the frequency domain of an image can increase the security, we further discuss the frequency domain LSQb information hiding algorithm for quantum image based on quantum Fourier transform. In our algorithms, the corresponding unitary transformations are designed to realize the aim of embedding the secret information to the least significant qubit representing color of the quantum cover image. Finally, we illustrate the procedure of extracting the secret information. Quantum image LSQb information hiding algorithm can be applied in many fields according to different needs.

1. Introduction

Quantum computation has been a novel topic in recent information science owing to the advantages of quantum mechanics [1] overcoming the limitations of classical computation. A series of quantum information processing algorithm have been proposed in recent decades, such as Shor's integer factoring algorithm [2], Grover's search algorithm [3].

Digital image processing plays an important role in practical applications [4], correspondingly, quantum image processing has been a hot topic in recent years. Quantum image processing is a branch of quantum information processing, and it has attracted many researchers' attention. Until now, most researches focus on the problems about quantum image representation, quantum image watermarking and quantum image encryption. Many quantum image representations have been proposed for the need of storing image information in quantum states, i.e., Qubit Lattice [5], Entangled Image [6], Real Ket [7], Flexible Representation of Quantum Images (FRQI) [8], Multi-Channel representation of quantum image (MCRQI) [9], quantum representation for log-polar images [10] and a new enhanced quantum image representation [11]. FRQI reduces the required number of qubits from $2^n \times 2^n$ of Qubit Lattice to $2n+1$ for $2^n \times 2^n$ image. Although the required qubits of NEQR increases to $2n+q$, it is good for image processing because the gray coding is very similar like the bit plane of classical image.

[*] Corresponding author.
E-mail address: shen.wang@hit.edu.cn (S. Wang).

http://dx.doi.org/10.1016/j.measurement.2015.05.038
0263-2241/© 2015 Elsevier Ltd. All rights reserved.

Watermarking and steganography are two parts of information hiding. Image watermarking, as one of branches of information hiding, has been researched deeply in classical computer. Quantum watermarking is the technique which embeds the invisible quantum signal such as the owner's identification into quantum multimedia data (such as audio, video and image) for copyright protection. Quantum image watermarking methods have been explored with many quantum image representations proposed. Based on FRQI, Iliyasu et al. proposed a secure, keyless, and blind watermarking and authentication strategy for quantum images based on restricted geometric transformations [14]. But the scheme can only be used to verify the identification of true owner of the carrier image. Then Zhang et al. designed a watermarking protocol [15] for quantum images. The scheme can be used to find out who is the real owner. Concrete quantum image watermarking method based on QFT has been proposed by Zhang et al. [16]. In their strategy, the watermark image is embedded into the Fourier coefficients of the quantum carrier image. Song et al. put forward a dynamic watermarking scheme for quantum images using quantum wavelet transform (QWT) [17] and quantum Hadamard transform [18], which has larger embedding capacity and good visual effect.

Information hiding embeds the additional secret information into media under the conditions of the carrier does not changing so much. Many information hiding methods for traditional images have been developed [19–21]. Classical LSB information hiding algorithm just substitutes the least significant bit of cover image using the secret information [22]. And LSB plays a significant part in digital image information hiding since many information hiding algorithms are based on it. Now the study of quantum image LSB information hiding algorithm is still in its infancy.

Most researches for quantum image security are based on FRQI representation. FRQI uses a superposition quantum state to store all pixels in an image. Color information is encoded by one qubit, and some simple image processing algorithms have been designed based on FRQI [12,13]. Obviously, single qubit is not suitable for LSQb information hiding because of no least significant qubit. Therefore, when discussing LSB information hiding algorithms for quantum images, the color encoding should be in the form of the binary qubit. At this time, NEQR based on binary qubit is an ideal representation for quantum image.

In this paper, based on NEQR, we propose quantum image LSQb information hiding algorithm, and the LSQb information hiding algorithm in quantum Fourier transformed domain for quantum image. Owning to the color information and position information are entangled together in NEQR, so in the procedure of the algorithm, we design the unitary transformation acting on the quantum image state. Through the unitary operations, we can realize the aim of embedding the secret message into the quantum cover image.

The rest of the paper is organized as follows. A brief introduction about NEQR representation, Quantum Fourier Transform, two quantum bit comparator and Classical LSB information hiding algorithm is presented in Section 2. The LSQb information hiding algorithm based on NEQR representation is proposed in Section 3. Based on Quantum Fourier transform of quantum image information hiding algorithm is shown in Section 4. Experimental results are shown in Section 5. Finally, a conclusion is given in Section 6.

2. Preliminaries

2.1. Classical least significant bit (LSB) information hiding method

Information hiding can achieve the functions of covert communication and copyright protection and so on. LSB information hiding is one of the significant methods of information hiding. It is proposed firstly by Tirkel in 1993 [22]. It substitutes the least significant bit of cover image with the secret information. When extract the secret information, only need to operate the stego image (the embedded cover image). It has the merits of easy to operate. Meanwhile, the stego image not changed so much that naked eyes cannot detect the differences. An example of LSB of image pixel 193 is shown in Fig. 1.

2.2. NEQR image representation

A novel enhanced quantum representation (NEQR) for digital images was proposed by Zhang et al. [11]. In this new model, the classical image color information is represented by the basis states of the color qubit. Therefore, color information qubit sequence and the position information qubit sequence are entangled in NEQR representation to store the whole image. Suppose the gray range of the image is 2^q, that is $f(i) \in [0, 2^q - 1]$. Gray-scale value $f(i)$ of the corresponding pixel is encoded by binary sequence $c^i_{q-1}c^i_{q-2}\ldots c^i_0$, $c^i_m \in [0,1](m = 0, 1, \ldots q - 1)$. The new representation model of a quantum image for a $2^n \times 2^n$ image is described as follows:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n-1}}|f(i)\rangle|i\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c^i_{q-1}c^i_{q-2}\ldots c^i_0\rangle|i\rangle \tag{1}$$

Position information $|i\rangle$ includes the vertical information and the horizontal information.

$$|i\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2}\cdots y_0\rangle|x_{n-1}x_{n-2}\ldots x_0\rangle$$

$|y\rangle$ encodes the vertical information and $|x\rangle$ encodes the horizontal information. Now we give a concrete example for NEQR.

Fig. 2 shows a 2 × 2 gray-scale image and its representative expression in NEQR. Since the gray scale ranges between 0 and 255. Eight qubits are needed to encode the color information for the pixels. On the other hand,

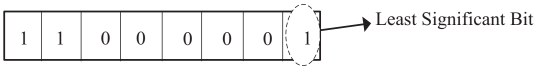
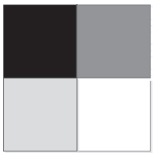


Fig. 1. Least significant bit of gray value 193.



$$|I\rangle = \frac{1}{2}\big(|0\rangle\otimes|00\rangle + |100\rangle\otimes|01\rangle + |200\rangle\otimes|10\rangle + |255\rangle\otimes|11\rangle\big)$$
$$= \frac{1}{2}\big(|00000000\rangle\otimes|00\rangle + |01100100\rangle\otimes|01\rangle + |11001000\rangle\otimes|10\rangle + |11111111\rangle\otimes|11\rangle\big)$$

Fig. 2. A 2 × 2 example image and its representative expression in NEQR.

we can see the difference between NEQR and classical image is only at the color information. When a NEQR image is changed into a classical image, we only need to convert its binary color information into an integer.

NEQR uses the basis qubit to store the gray-scale information for each pixel in an image, some digital image-processing operations, for example certain complex color operations, can be done on the basis of NEQR. And partial color operations and statistical color operations can be conveniently performed based on NEQR. The whole preparation of NEQR costs no more than $O(qn2^{2n})$ for a $2^n \times 2^n$ image with gray range 2^q [11].

2.3. Quantum Fourier transform

In quantum theory, Quantum Fourier transform, whose computation time is $O(n^2)$ for n qubits inputs, is a unitary transform which mapped a set of orthogonal basis $|x\rangle$ into another orthogonal basis $|y\rangle$.

$$\mathrm{QFT}|x\rangle = \frac{1}{2^n}\sum_{y=0}^{2^{2n}-1} e^{2\pi jiy/2^{2n}}|y\rangle \tag{2}$$

Le defined the application of QFT on FRQI in [8]. It can be considered as the application of Fourier transform on the cosine part and sin part of the FRQI state. Suppose the quantum image state FRQI be the following form:

$$|J\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n-1}}(\cos\theta_i|0\rangle + \sin\theta_i|1\rangle)|i\rangle \tag{3}$$

Then the quantum Fourier transformed FRQI image is the following:

$$|J_1\rangle = \mathrm{QFT}(|J\rangle) = \frac{1}{2^n}\sum_{i=0}^{2^{2n-1}}(\cos\theta_i|0\rangle + \sin\theta_i|1\rangle)\otimes\mathrm{QFT}(|i\rangle) \tag{4}$$

In parallel, we can define Quantum Fourier Transform on the NEQR quantum image state as the following way.

$$|I_1\rangle = \mathrm{QFT}(|I\rangle) = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle\otimes\mathrm{QFT}(|i\rangle) \tag{5}$$

2.4. Two quantum bit comparator

Inspired by the idea of quantum comparator [23], we design two quantum bit comparator which can be seen just as in Fig. 3. The symbols '○', '●' and '⊕' in Fig. 3 represent zero control, one control and NOT operations, respectively. The circuit employs Two-qubit controlled NOT gate and realizes the goal of judging whether two qubits are same or not. In Fig. 3 $|a\rangle, |b\rangle$ are the input qubit and $|c\rangle, |d\rangle$ are the outputs of the corresponding state.

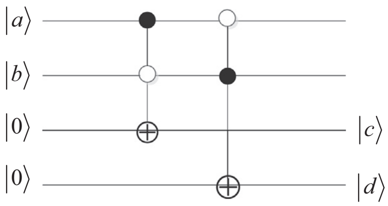


Fig. 3. Two qubit comparator.

If $|c\rangle|d\rangle = |1\rangle|0\rangle$ or $|c\rangle|d\rangle = |0\rangle|1\rangle$, then quantum state $|a\rangle$ is not equal to quantum state $|b\rangle$;

If $|c\rangle|d\rangle = |0\rangle|0\rangle$, then quantum state $|a\rangle$ is equal to quantum state $|b\rangle$.

Obviously, we can compare the secret qubit information with the last qubit of the cover image to judge is they are equal using the two quantum bit comparator.

3. Proposed quantum LSB image information hiding algorithm

Just like described in Section 2.1, the principle of classical LSB information hiding is embedding the secret message into the least significant bit of cover image. Appropriately, we can define quantum LSQb information hiding. Quantum LSQb information hiding can be described in this way: substituting the last qubit of cover image encoding color with the secret information. We must notice that no matter what kind of the secret information is, it can be encoded into a binary qubit stream.

3.1. Quantum image LSQb information hiding algorithm

Next we describe the specific procedure of quantum image LSQb information hiding algorithm in the following steps:

(1) Comparing the qubit of secret information $|c_{m0}\rangle$ with the last qubit color encoding cover image color encoding information $|c_0\rangle$ in Eq. (1) using the quantum comparator in Fig. 3. Obviously, secret image color encoding $|c_{m0}\rangle$ just needs one qubit, $|c_{m0}\rangle = |0\rangle or|1\rangle$, while cover image color encoding $|c\rangle$ needs q qubit $|c\rangle = |c_{q-1}c_{q-2}\cdots c_1c_0\rangle$ when implementing the above steps. We use the quantum comparator in Fig. 3 and we can see that in order to use quantum comparator to compare $|c_{m0}\rangle$ and $|c_0\rangle$, the first qubit of cover image color encoding c_0 and the

secret image color encoding c_{m0} can be taken as the input of the quantum comparator. Then, according to the output of the quantum comparator circuit, we can decide which unitary transform will be acted on the quantum state.

(2) LSQb information hiding. The output two values from quantum comparator are same, then we will do nothing about the color information, however, if the return two values are different, we can define the following unitary transformation to act on the quantum cover image state.

$$U_i = I^{\otimes q-1} \otimes U \otimes |i\rangle\langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle\langle j| \right) \tag{6}$$

where

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Obviously, this unitary transform is the CNOT gate. And the secret information needs to embed all the positions of cover image. So each operation U_i corresponding to each position $i = 0, 1, \ldots 2^{2n} - 1$. Next we will give the concrete derivation process. We suppose all the returning values are different. If some locations returned the same value, we use the following unitary transform.

$$U_j = I^{\otimes q} \otimes \left(\sum_{j=0}^{2^{2n}-1} |j\rangle\langle j| \right) \tag{7}$$

$$\begin{aligned}
U_i(|I\rangle) &= \left(I^{\otimes q-1} \otimes U \otimes |i\rangle\langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle\langle j| \right) \right) \left(\frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} \left| c_{q-1}^i c_{q-2}^i \cdots c_0^i \right\rangle |i\rangle \right) \\
&= \frac{1}{2^n} \left(I^{\otimes q-1} \otimes U \otimes |i\rangle\langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle\langle j| \right) \right) (|c_{q-1}^i c_{q-2}^i \cdots c_0^i\rangle |i\rangle) \\
&\quad + \frac{1}{2^n} \left(I^{\otimes q-1} \otimes U \otimes |i\rangle\langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle\langle j| \right) \right) \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |c_{q-1}^j c_{q-2}^j \cdots c_0^j\rangle |j\rangle \right) \\
&= \frac{1}{2^n} (I^{\otimes q-1} \otimes U \otimes |i\rangle\langle i|)(|c_{q-1}^i c_{q-2}^i \cdots c_0^i\rangle |i\rangle) \\
&\quad + \frac{1}{2^n} \left(I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle\langle j| \right) \right) \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |c_{q-1}^j c_{q-2}^j \cdots c_0^j\rangle |j\rangle \right) \\
&= \frac{1}{2^n} |c_{q-1}^i c_{q-2}^i \cdots c_1^i\rangle U |c_0^i\rangle |i\rangle + \frac{1}{2^n} \sum_{j=0, j\neq i}^{2^{2n}-1} |c_{q-1}^j c_{q-2}^j \cdots c_0^j\rangle |j\rangle \\
&= \frac{1}{2^n} |c_{q-1}^i c_{q-2}^i \cdots c_1^i\rangle |\tilde{c}_0^i\rangle |i\rangle + \frac{1}{2^n} \sum_{j=0, j\neq i}^{2^{2n}-1} |c_{q-1}^j c_{q-2}^j \cdots c_0^j\rangle |j\rangle
\end{aligned}$$

where

$$|\tilde{c}_0^i\rangle = \begin{cases} |\bar{c}_0^i\rangle, & |c_{m0}\rangle \neq |c_0\rangle \\ |c_0^i\rangle, & |c_{m0}\rangle = |c_0\rangle \end{cases}$$

$|\bar{c}_0^i\rangle$ is the complement of $|c_0^i\rangle$.

$$|\bar{c}_0^i\rangle = \begin{cases} |1\rangle, & |c_0^i\rangle = |0\rangle \\ |0\rangle, & |c_0^i\rangle = |1\rangle \end{cases}$$

From the above deriving process, we see that the operation only change the last qubit of color information encoding of the corresponding position. If we apply the operation $\prod_{i=0}^{2^{2n-1}} U_i$ to the quantum cover image $|I\rangle$, we can realize the aim of hiding the secret information to the cover quantum image state and get the following embedded image.

$$|I'\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |c_{q-1}^i c_{q-2}^i \cdots c_1^i\rangle |\tilde{c}_0^i\rangle |i\rangle \tag{8}$$

Note 1: In the above algorithms, if some positions such as position $|j\rangle$ return the same value, the transform U_j in $\prod_{i=0}^{2^{2n-1}} U_i$ should be in the form of $U_j = I^{\otimes q} \otimes \left(\sum_{j=0}^{2^{2n}-1} |j\rangle\langle j| \right)$.

Note 2: In the above two steps, we must notice that if the length of secret information did not equal the cover image position. We should set the length of secret information equal to the length of cover image color. We just need to use the same last qubit of cover image to fill the secret information.

Note 3: If we want to embed the same secret information in some positions of cover image. We can design the corresponding unitary transformation. For example, if we want to hide the secret information to the position i_1 and i_2, and suppose that color information of cover image in positions i_1 and i_2 is different from the secret information. Then the following unitary transform can be taken.

$$U_i = I^{\otimes q-1} \otimes U \otimes (|i_1\rangle\langle i_1| + |i_2\rangle\langle i_2|) + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i_1, j\neq i_2}^{2^{2n}-1} |j\rangle\langle j| \right) \tag{9}$$

3.2. Secret information extraction procedure

For the process of extracting secret information, just need to extract the last qubit of color encoding of the stego image (embedded quantum cover image). Next we describe the concrete procedure.

(1) Owing to LSQb stego image is a complex vector in Hilbert space which the size is 2^{q+2n}. So we decompose the vector into the direct product of color and correspondingly position. For example: the size of the cover image is $2^2 \times 2^2$, and the LSQb stego image vector is X. Then we ought to disintegration X as the following form:

$$X = C_1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + C_2 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + C_3 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + C_4 \otimes \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Obviously this step can be realized because the vector X and the binary encoding of position are known.

(2) Convert every first part of the direct product (color information) to binary data. The number of binary bit is equivalent to the number of bits of cover images' color encoding. In the above example, that means converting C_1, C_2, C_3, C_4 to the appropriate binary data C_{1_b}, C_{2_b}, C_{3_b}, C_{4_b}. This transform can be guaranteed by the operations in quantum computation.

(3) Extract the last bit of every binary data. These bits form a binary code stream which is the secret information. That is to extract the last bit of C_{1_b}, C_{2_b}, C_{3_b}, C_{4_b} and arrange these bits as the secret information.

Obviously, the embedding rate of the LSQb information hiding algorithm is $1/q$ and the embedding capacity is 1 qubits/pixel.

4. Quantum image LSQb steganography algorithm in frequency domain

Researches on frequency domain of classical image LSB information hiding algorithm are meaningful. Correspondingly, we can define the quantum image frequency domain LSQb information hiding algorithm. It embeds the secret message to frequency domain of the quantum image. Next we will give the example quantum image LSQb information hiding algorithm in the QFT frequency domain.

4.1. Quantum image LSQb information hiding algorithm in quantum Fourier transformed domain

Firstly, we describe the concrete procedure of quantum image LSQb information hiding algorithm just as the following steps:

(1) Execute QFT on the cover image $|I\rangle$, getting its Fourier form shown as follows

$$|T_1\rangle = \mathrm{QFT}|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle \otimes \left(\frac{1}{2^n}\sum_{y=0}^{2^{2n}-1}e^{2\pi jiy/2^{2n}}|y\rangle\right) \tag{10}$$

Obviously, when executed quantum Fourier transform, the color encoding information does not changed according to the definition of quantum Fourier transform in (5). The only difference is that the position qubit becomes the superposition state of basis.

(2) Comparing the qubit of secret image color encoding information $|c_{m0}\rangle$ with the last qubit color encoding information $|c_0\rangle$ of the Quantum Fourier transformed cover image $|T_1\rangle$ in (10) using the two qubit quantum comparator in Fig. 3. Just like the Quantum LSQb algorithm in III, the first qubit of color encoding c_0 of $|T_1\rangle$ and the secret image color encoding c_{m0} can be taken as the input of the quantum comparator. Then according to the output of the quantum comparator circuit, we can decide which unitary transform will be acted on the quantum state.

(3) LSQb information hiding. If the return two values are different, we can define the following unitary transformation to act on the Quantum Fourier transformed cover image state $|T_1\rangle$ in (10).

$$U'_i = I^{\otimes q-1}\otimes U\otimes \mathrm{QFT}|i\rangle\langle i|\mathrm{QFT}^{-1} + I^{\otimes q}\otimes \mathrm{QFT}\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1} \tag{11}$$

where

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

If the two values are same, then we apply the following unitary equation

$$U'_j = I^{\otimes q}\otimes \mathrm{QFT}\left(\sum_{j=0}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1} \tag{12}$$

And the secret information needs to embed all the positions of Quantum Fourier transformed cover image. So each operation U'_i corresponding to each positions $i = 0, 1, \ldots 2^{2n}-1$. In the above steps, we must notice that if the length of secret information is not equal to the cover image position. We should set the length of secret information equal to the length of cover image color. Next we will give the specific derivation procedure.

$$\begin{aligned}
|T_2\rangle &= U'_i(|T_1\rangle) = U'_i(\mathrm{QFT}|I\rangle)\\
&= \Bigg(I^{\otimes q-1}\otimes U\otimes \mathrm{QFT}|i\rangle\langle i|\mathrm{QFT}^{-1}\\
&\quad + I^{\otimes q}\otimes \mathrm{QFT}\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1}\Bigg)\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle\otimes \mathrm{QFT}(|i\rangle)\right)\\
&= \left(I^{\otimes q-1}\otimes U\otimes \mathrm{QFT}|i\rangle\langle i|\mathrm{QFT}^{-1} + I^{\otimes q}\otimes \mathrm{QFT}\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1}\right)\\
&\quad \times\left(\tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle\otimes \mathrm{QFT}(|i\rangle)+\tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}(|j\rangle)\right)\\
&= I^{\otimes q-1}\otimes U\otimes \mathrm{QFT}|i\rangle\langle i|\mathrm{QFT}^{-1}\\
&\quad \left(\tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle\otimes \mathrm{QFT}(|i\rangle)+\tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}(|j\rangle)\right)\\
&\quad + I^{\otimes q}\otimes \mathrm{QFT}\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1}\\
&\quad \times\left(\tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle\otimes \mathrm{QFT}(|i\rangle)+\tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}(|j\rangle)\right)\\
&= \tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle U|c^i_0\rangle\otimes \mathrm{QFT}|i\rangle\langle i|\mathrm{QFT}^{-1}(\mathrm{QFT}(|i\rangle))\\
&\quad + \tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1}\mathrm{QFT}(|j\rangle)\\
&= \tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle U|c^i_0\rangle\otimes \mathrm{QFT}|i\rangle + \tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}(|j\rangle)\\
&= \tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle U|c^i_0\rangle\otimes \mathrm{QFT}|i\rangle + \tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}((|j\rangle))\\
&= \tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\cdots c^i_0\rangle|\tilde{c}^i_0\rangle\otimes \mathrm{QFT}|i\rangle + \tfrac{1}{2^n}\sum_{j=0,j\neq i}^{2^{2n}-1}|c^j_{q-1}c^j_{q-2}\cdots c^j_0\rangle\otimes \mathrm{QFT}((|j\rangle))
\end{aligned}$$

Then according to the definition of Quantum Fourier transform, we can rewrite the above equation as the following quantum state:

$$\begin{aligned}
|T_2\rangle &= \tfrac{1}{2^n}|c^i_{q-1}c^i_{q-2}\ldots c^i_0\rangle|\tilde{c}^i_0\rangle\left(\tfrac{1}{2^n}\sum_{y=0}^{2^{2n}-1}e^{2\pi jiy/2^{2n}}|y\rangle\right)\\
&\quad + \tfrac{1}{2^n}\sum_{l=0,l\neq i}^{2^{2n}-1}|c^l_{q-1}c^l_{q-2}\cdots c^l_0\rangle\left(\tfrac{1}{2^n}\sum_{y=0}^{2^{2n}-1}e^{2\pi jly/2^{2n}}|y\rangle\right)
\end{aligned} \tag{13}$$

So we can see that the aim of embedding the secret information to the Quantum Fourier transformed image is achieved.

Where

$$|\tilde{c}_0^i\rangle = \begin{cases} |\bar{c}_0^i\rangle, & |c_{m0}\rangle \neq |c_0\rangle \\ |c_0^i\rangle, & |c_{m0}\rangle = |c_0\rangle \end{cases}$$

$|\bar{c}_0^i\rangle$ is the complement of $|c_0^i\rangle$. We also suppose every return value of comparator is different. That is to say in our derivation process, the first case occurs.

From the above deriving process, we see that the operation only change the color information of the corresponding position. If we apply the operation $\prod_{i=0}^{2^{2n-1}} U'_i$ to the Quantum Fourier transformed cover image $|T_1\rangle$, which U'_i is decided by the comparator return value of position $|i\rangle$. we can realize the aim of hiding the secret information to the quantum Fourier transformed cover image. That is we can get the following image:

$$|T_2\rangle = \frac{1}{2^n}|c_{q-1}^i c_{q-2}^i \cdots c_1^i\rangle|\tilde{c}_0^i\rangle\left(\frac{1}{2^n}\sum_{y=0}^{2^{2n}-1} e^{(2\pi jiy)/2^{2n}}|y\rangle\right) \tag{14}$$

Note 4: In the above algorithms, if some positions such as position $|j\rangle$ return the same value, the transform U'_j in $\prod_{i=0}^{2^{2n-1}} U'_i$ should be in the form of $U'_j = I^{\otimes q} \otimes \mathrm{QFT}\left(\sum_{j=0}^{2^{2n}-1}|j\rangle\langle j|\right)\mathrm{QFT}^{-1}$.

4.2. Quantum image LSQb information hiding extracting algorithm in quantum Fourier transformed domain

For the process of extracting secret information, it is just like the discussion in III. The aim is that we extract the last qubit of color encoding information of Fourier transformed image as the secret message.

(1) Because LSQb stego image in quantum Fourier frequency domain is also a complex vector in Hilbert space which the size is $2 \wedge (q + 2n)$, we can decomposition this vector into the direct product of color and correspondingly position. There is a different from the first step of LSQb algorithm in III. The position basis vector should be acted by quantum Fourier transform. We also use an example to explain this step. Suppose the size of the cover image is $2^2 \times 2^2$, and the vector of LSQb stego image in the quantum Fourier transform vector is Y. Then we ought to disintegration Y as the following form:

$$Y = D_1 \otimes \mathrm{QFT}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + D_2 \otimes \mathrm{QFT}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + D_3 \otimes \mathrm{QFT}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + D_4 \otimes \mathrm{QFT}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Obviously the above equation can be realized because the vector Y and the vector of quantum Fourier transform acted on the position basis are known.

Then the next steps just like the description of LSQb algorithm.

(2) Convert every first part of the direct product (color information) to binary data. The number of binary bit is equivalent to the number of bits of cover images' color encoding. In the above example, that is to say, convert D_1, D_2, D_3, D_4 to the appropriate binary data D_{1_b}, D_{2_b}, D_{3_b}, D_{4_b}. This transform can be guaranteed by the operations in quantum computation.

(3) Extract the last bit of every binary data. These bits form a binary code stream which is the secret information. That is to extract the last bit of D_{1_b}, D_{2_b}, D_{3_b}, D_{4_b} and arrange these bits as the secret information.

The same as the LSQb information hiding algorithm, the embedding rate of the algorithm in QFT domain is still $1/q$.

5. Experimental results

There are some difference between quantum image and classical image. And until now, there is no concrete evaluation index for quantum image's visual quality. But we can change quantum image to the classical image to evaluate. Just like section B described, when NEQR image changes into classical image, only need to turn its binary color information qubit into an integer. In classical LSB algorithm, we use PSNR to evaluate its hidden effect. Here, we also use PSNR to evaluate the visual effect of the image.

Next we give some simulation-based experiments and analysis of the results and performance of the proposed

Fig. 4. (a) Original Lena image and (b) the hidden image Lena.

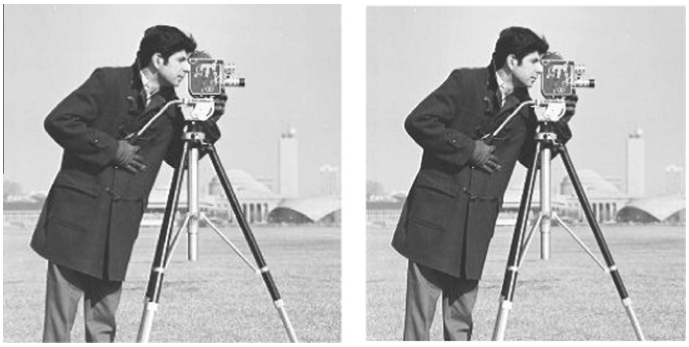


Fig. 5. (a) Original Cameraman image and (b) the hidden Cameraman image.

Table 1
PSNR value of the experiment.

Images	Lena	Cameraman
PSNR\db	64.9738	65.8034

LSQB information hiding algorithm. All experiments are simulated on the MATLAB 7.11.0. We use 256 × 256 Lena.bmp as our cover image and randomly produce binary qubit as our secret information.

PSNR (Peak Signal-to-Noise Ratio) is applied to display the accuracy of proposed information hiding algorithm. Assuming there are two $2^n \times 2^n$ images I and J, $I(y,x)$, $J(y,x)$ representing the pixel values of pixel (y,x). MSE (Mean Squared Error) is defined as Eqs. (15) and (16).

$$\mathrm{MSE} = \frac{1}{mn}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}[I(y,x) - J(y,x)]^2 \tag{15}$$

$$\mathrm{PSNR} = 20 \times \log_{10}\left(\frac{2^q - 1}{\sqrt{\mathrm{MSE}}}\right) \tag{16}$$

The following Figs. 4 and 5 describes experimental results of our algorithm of LSQB information hiding algorithm and Table 1 gives the PSNR value between the original quantum image and the hidden image.

Obviously, from Figs. 4 and 5, human eyes cannot detect the difference between hidden image and original carrier image. From the Table 1, we can see that the PSNR values are high enough. So we can conclude that LSQB information hiding algorithm has a good visual effect.

6. Conclusion

In this paper, based on NEQR, firstly, we designed the concrete quantum image LSQb information hiding algorithm. LSQb information hiding embedded the secret message qubit stream in the last qubit of color of quantum cover image. Moreover, information hiding is researched on the frequency domain which can increase the security of quantum cover image. Concretely, we also discuss the quantum image Fourier frequency domain LSQb information hiding algorithm. In algorithms, the corresponding unitary transformations are designed to realize the aim of embedding the secret information to the last qubit of color of quantum cover image. Quantum image LSQb information hiding algorithm can be applied on the basis of different needs.

Acknowledgment

This work is supported by the National Science Foundation of China (61301099, 61361166006 and 61471141).

References

[1] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. Roy. Soc. Lond. A400 (1985) 97–117.

[2] P.W. Shor, Algorithms for quantum computation discrete logarithms and factoring, in: S. Goldwasser (Ed.), Pro of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Science, quantum ph/9508027.

[3] L.K. Grove, Quantum computers can search arbitrarily large databases by a single query, Phys. Rev. Lett. 79 (23) (1977) 47094712.

[4] R.C. Gozalez, R.E. Woods, S.L. Eddins, Digital Image Processing, Publishing House of Electronics Industry, Beijing, 2002.

[5] S.E. Venegas-Andraca, S. Bose, Storing, processing and retrieving an image using quantum mechanics, Proc. SPIE Conf. Quantum Inf. Comput. 5105 (2003) 137–147.

[6] S.E. Venegas-Andraca, J.L. Ball, K. Burnett, S. Bose, Processing images in entangled quantum systems, Quantum Inf. Process. 9 (2010) 1–11.

[7] J.I. Latorre, Image compression and entanglement. arXiv: quant-ph/0510031, 2005.

[8] P.Q. Le, F. Dong, K. Hirota, A flexible representation of quantum images for polynomial preparation, image compression and processing operations, Quantum Inf. Process. 10 (1) (2010) 63–84.

[9] B. Sun, P.Q. Le, A.M. Iliyasu, J. Adrian Garcia, F. Yan, J.F. Dong, K. Hirota, A multi-channel representation for images on quantum computers using the RGB α color space, in: Proceedings of the IEEE 7th International Symposium on Intelligent Signal Processing, 2011, pp. 160–165.

[10] Y. Zhang, K. Lu, Y.H. Gao, K. Xu, A novel quantum representation for log-polar images, Quantum Inf. Process (2013) 1–24.

[11] Y. Zhang, K. Lu, Y.H. Gao, M. Wang, NEQR: a novel enhanced quantum representation of digital images, Quantum Inf. Process (2013) 1–28.

[12] C.C. Tseng, T.M. Hwang, Quantum digital image processing algorithms, in: 16th IPPR Conference on Computer Vision, Graphics and Image Processing, 2003, pp. 827–834c.

[13] X.W. Fu, M.Y. Ding, A new quantum edge detection algorithm for medical images, in: Proceeding of Medical Imaging, Parallel Processing of Images and Optimization Techniques, SPIE, vol. 7497, 2009.

[14] A.M. Iliyasu, L.Q. Phuc, F. Dong, K. Hirota, Watermarking and authentication of quantum images based on restricted geometric transformation, Inform. Sci. 186 (2011) 126–149.

[15] W.W. Zhang, F. Gao, B. Liu, H.Y. Jia, Q. Wen, H. Chen, A quantum watermark protocol, Int. J. Theor. Phys. 52 (2) (2013) 504–513.

[16] W.W. Zhang, F. Gao, B. Liu, Q. Wen, H. Chen, A watermark strategy for quantum images based on quantum Fourier transform, Quantum Inf. Process. (2012), http://dx.doi.org/10.1007/s11128-012-0423-6.

[17] X.H. Song, S. Wang, S. Liu, A.A. El-Latif, X.M. Niu, A dynamic watermarking scheme for quantum images using quantum wavelet transform, Quantum Inf. Process 12 (12) (2013) 3689–3706.

[18] X.H. Song, S. Wang, S. Liu, A.A. El-Latif, X.M. Niu, Dynamic watermarking scheme for quantum images based on Hadamard transform, Multimedia Syst. 20 (4) (2014) 379–388.

[19] H.C. Huang, F.C. Chang, Hierarchy-based reversible data hiding, Expert Syst. Appl. 40 (1) (2013) 34–43.

[20] H.C. Huang, W.C. Fang, Authenticity preservation with histogram-based reversible data hiding and quadtree concepts, Sensors 11 (10) (2011) 9717–9731.

[21] C.F. Lee, C.C. Chang, P.Y. Pai, C.M. Liu, An adjustable and reversible data hiding method based on multiple-base notational system without location map, J. Inform. Hiding Multimedia Signal Process. 6 (1) (2015) 1–28.

[22] G. Shailender, A.G. Bhushan, Information hiding least significant bit steganography and cryptography, Int. J. Educ. Comput. Sci. 6 (2012) 27–34.

[23] D. Wang, Z.H. Liu, W.N. Zhu, S.Z. Li, Design of quantum comparator based on extended general Toffoli gates with multiple targets, Comput. Sci. 39 (9) (2012) 302–306.