

Least significant qubit algorithm for quantum images

Jianzhi Sang¹ · Shen Wang¹ · Qiong Li¹

Received: 29 April 2016 / Accepted: 1 August 2016 / Published online: 18 August 2016
© Springer Science+Business Media New York 2016

Abstract To study the feasibility of the classical image least significant bit (LSB) information hiding algorithm on quantum computer, a least significant qubit (LSQb) information hiding algorithm of quantum image is proposed. In this paper, we focus on a novel quantum representation for color digital images (NCQI). Firstly, by designing the three qubits comparator and unitary operators, the reasonability and feasibility of LSQb based on NCQI are presented. Then, the concrete LSQb information hiding algorithm is proposed, which can realize the aim of embedding the secret qubits into the least significant qubits of *RGB* channels of quantum cover image. Quantum circuit of the LSQb information hiding algorithm is also illustrated. Furthermore, the secrets extracting algorithm and circuit are illustrated through utilizing control-swap gates. The two merits of our algorithm are: (1) it is absolutely blind and (2) when extracting secret binary qubits, it does not need any quantum measurement operation or any other help from classical computer. Finally, simulation and comparative analysis show the performance of our algorithm.

Keywords Least significant qubit · Unitary operator · Color digital images

✉ Jianzhi Sang
768588166@qq.com

✉ Qiong Li
qiongli@hit.edu.cn

Shen Wang
shen.wang@hit.edu.cn

¹ Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, China

1 Introduction

Along with the bright prospect of quantum computers [1, 2], quantum image processing (QIP) has gained researchers' interest in recent years [3]. The first task in this direction is constructing the quantum image representation model to represent images on quantum computer.

A great number of research results concerning quantum image representations have been established for the need of storing image information in quantum states, i.e., Qubit Lattice [4], Entangled Image [5], Real Ket [6], Flexible Representation of Quantum Images (FRQI) [7], quantum representation for log-polar images [8], a novel enhanced quantum representation of digital images (NEQR) [9], the improved novel enhanced quantum representation (INEQR) [10], Multi-channel representation for quantum images (MCRQI) [11], and a novel quantum representation for color digital images (NCQI) [12].

Because of the particular properties of quantum computation, there are some quantum processing transformations which are more efficient than their corresponding classical versions: quantum Fourier transform [13], quantum wavelet transform [14], and quantum discrete cosine transform [15]. Many researchers also focus on some elementary processing algorithms on quantum images, such as the geometric transformations on quantum images (GTQI) [16], image scrambling [17, 18], image translation [19], image scaling [20, 21], pseudocolor coding [22] and quantum Boolean image denoising [23].

Except the above elementary quantum image processing algorithms, quantum image information hiding has become a hot topic. Based on restricted geometric transformation, a watermarking scheme is given [24]. A novel quantum image watermark scheme is proposed by embedding the secrets into the Taylor series coefficients [25] of color information. Several watermarking schemes based on FRQI are put forward [26–28]. Further, by using simple CNOT gate and small-scale quantum circuit, a watermarking scheme is projected in [29]. A novel quantum image steganography based on Moiré pattern is depicted [30]. A LSB algorithm based on NEQR has been given in [31]. Block LSB steganography algorithm has been given [32]. However, all existing quantum image steganography algorithms are derived from gray scale image. In fact, in quantum image processing, gray image processing algorithms cannot be directly applied into the color digital image. We have to design different methods for the realization of information hiding algorithm of color image on quantum computer. Also, the images in the real life are usually colorful, so the corresponding quantum steganography algorithms of color images should be researched.

This paper is concerned with the LSB information hiding algorithm based on NCQI. The following advantages of NCQI are suggested to make it suitable for quantum image LSB algorithm:

- (1) NCQI acquires three channels *RGB* information and their corresponding positions in an image into a normalized quantum state. Thus, quantum CNOT gates and other simple quantum gates are used to flexibly link color and position information, providing an easy way to process image for the user.

- (2) NCQI uses a binary qubit basis to encode position information. It is easy to design various unitary operators to act on the different position qubits, which achieves the aim of embedding the secret qubits into distinct positions of an image.
- (3) For NCQI, color information of RGB channels is stored into a binary quantum sequence which is similar to the representations of classical color digital images. This makes it relatively easy to transfer LSB information hiding algorithm from classical computer to quantum computer.

In this paper, a substantially different method for the quantum realization is proposed for LSQb information hiding algorithm of NCQI. In the proposed method, the reliance on using quantum measurement or classical computer is no longer necessary. The key idea is how to embed secret qubits information into the least significant qubits of RGB channels. A method of designing three qubits comparator and unitary operators to embed secret qubits is required. Specifically, LSQb hiding problem is solved by two steps. First, through the designed three qubits comparator, the secret qubits are compared with least significant qubits of RGB channels. Then, by the constructed unitary operators, the secret qubits are embedded into the least significant qubits of RGB channels. Theoretical analyses show two merits of our algorithm: (1) the algorithm is absolutely blind. The extracting procedure does not need the original cover image. (2) The whole procedure of information extraction does not need any quantum measurement operation or any other help from classical computer.

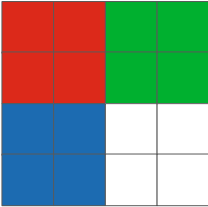
The contributions of this paper are summarized as follows: First, three qubits comparator is designed, which can establish the relationship between the secret qubits and least significant qubits of three channels. Second, the elaborated unitary operators are constructed to construct LSQb information hiding algorithm. Third, the control-swap gates are introduced to design the quantum secret information extraction circuit.

The rest of the paper is organized as follows. Section 2 briefly introduces the NCQI model. Also, the differences between FRQI, NEQR, and NCQI are depicted. In Sect. 3, the reasonability and feasibility of LSQb information hiding algorithm of NCQI are proven based on the designed three qubits comparator and the unitary operators. The proposed LSQb information hiding and extraction algorithms are depicted in Sect. 4. In addition, complexity and comparison analysis are also shown. Simulation examples and quantum measurement on the outcome are demonstrated in Sect. 5. The conclusion and future work are given in Sect. 6.

2 Related work

2.1 NCQI

Inspired by the NEQR [9], NCQI is present to store and process color digital images on quantum computer. The range of x and y is assumed to be $[0, 2^n - 1]$ and $[0, 2^n - 1]$, respectively. The value range of every channel (R, G, B) is $[0, 2^q - 1]$. Then, the quantum image representation model NCQI can be shown in the following equation:



$$\begin{aligned}
 |I(\theta)\rangle &= \frac{1}{\sqrt{2^4}} \left[\begin{aligned}
 &\left| \underbrace{11111111}_R \underbrace{00000000}_G \underbrace{00000000}_B \right\rangle \otimes (|0000\rangle + |0001\rangle + |0100\rangle + |0101\rangle) \\
 &+ \left| \underbrace{00000000}_R \underbrace{11111111}_G \underbrace{00000000}_B \right\rangle \otimes (|0010\rangle + |0011\rangle + |0110\rangle + |0111\rangle) \\
 &+ \left| \underbrace{00000000}_R \underbrace{00000000}_G \underbrace{11111111}_B \right\rangle \otimes (|1000\rangle + |1001\rangle + |1100\rangle + |1101\rangle) \\
 &+ \left| \underbrace{11111111}_R \underbrace{11111111}_G \underbrace{11111111}_B \right\rangle \otimes (|1010\rangle + |1011\rangle + |1110\rangle + |1111\rangle) \end{aligned} \right]
 \end{aligned}$$

Fig. 1 A 4×4 color image and its quantum representation expression of NCQI

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |c(y, x)\rangle \otimes |yx\rangle \tag{1}$$

where $|c(y, x)\rangle$ denotes the color value of the corresponding pixel and it can be encoded by the binary sequence $R_{q-1} \cdots R_0 G_{q-1} \cdots G_0 B_{q-1} \cdots B_0$.

$$|c(y, x)\rangle = \left| \underbrace{R_{q-1} \cdots R_0}_{Red} \underbrace{G_{q-1} \cdots G_0}_{Green} \underbrace{B_{q-1} \cdots B_0}_{Blue} \right\rangle \tag{2}$$

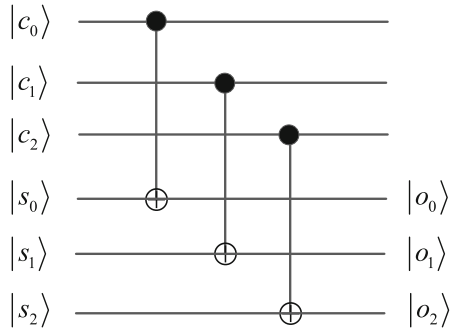
Equation (1) indicates that the whole NCQI model is stored into a normalized quantum superposition state. There are three parts i.e., the color information $c(y, x)$, the vertical position y and the horizontal position x to represent one pixel. The tensor product of these three qubits sequences constitutes the basis state of NCQI. Equation (2) implies that $|c(y, x)\rangle$ contains three channels information, i.e. R, G, B . There are $2n + 3q$ qubits being employed to store image information into a NCQI state for a $2^n \times 2^n$ color image with every channel R, G, B ranged $[0, 2^q - 1]$.

An example of a 4×4 color image with three channels R, G, B ranged $[0, 2^8 - 1]$, i.e., $n = 2, q = 8$ is shown in Fig. 1. Equation expressed in Fig. 1 depicts that the whole NCQI is stored into a normalized quantum superposition state, in which each basis represents one pixel.

Among numerous quantum image models, FRQI and NEQR are the two most important and convenient models in considering the way in which a gray image is encoded under rectangular coordinate system. The differences and relations between FRQI, NEQR and NCQI can be summarized as follows:

- (1) FRQI and NEQR are very important two quantum image models, but they cannot represent the color digital images on the quantum computer. NCQI can represent color digital images on the quantum computer, which meets the fact that the images in the real life are usually colorful.
- (2) The most obvious distinction between them lies in the color encoding form. Due to the different patterns of color encoding state, the preparation process for FRQI, NEQR and NCQI is distinct. FRQI is convenient to research quantum

Fig. 2 Three qubits comparator



gray image watermarking and frequency transform. However, for some binary qubit operation-based transforms, NEQR and NCQI may be more applicable.

- (3) NEQR is developed from FRQI. NCQI extends the NEQR model to the color digital image.

According to the above points, discussions about LSQb information hiding algorithm of color digital image is appropriate for NCQI.

3 Reasonability and feasibility of LSQb algorithm

In the following discussion, the original quantum image has the form described in Eq. (1) and the secret binary qubits stream has the form $|s_0\rangle, |s_1\rangle, \dots, |s_{3t-2}\rangle, |s_{3t-1}\rangle$, $t \leq 2^{2n}$. Before proving the feasibility of LSQb information hiding algorithm, one proposition is given.

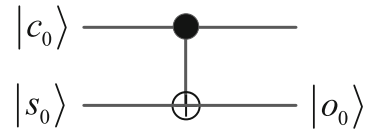
Proposition 1 *Using the novel designed three qubits comparator in Fig. 2, the aim of comparing the secret qubits with the least significant qubits of RGB channels can be realized.*

Proof Through analyzing the inputs and outputs of Fig. 2, the corresponding conclusion in proposition 1 can be obtained.

- (1) Firstly, as an example, CNOT gate is analyzed. In Fig. 3, the value of input qubits $|c_0s_0\rangle$ has four circumstances $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$. After the function of the CNOT gate, the corresponding values of the output qubit $|o_0\rangle$ are $|0\rangle, |1\rangle, |1\rangle, |0\rangle$. That is to say, when $|c_0s_0\rangle = |00\rangle$ or $|c_0s_0\rangle = |11\rangle$, the output qubit $|o_0\rangle = |0\rangle$; when $|c_0s_0\rangle = |01\rangle$ or $|c_0s_0\rangle = |10\rangle$, the output qubit $|o_0\rangle = |1\rangle$. So, the following conclusion can be acquired:
If $|o_0\rangle = |0\rangle$, then $|c_0\rangle = |s_0\rangle$; if $|o_0\rangle = |1\rangle$, then $|c_0\rangle \neq |s_0\rangle$.
- (2) For three qubits comparator in Fig. 2, there are three CNOT gates, which $|c_0\rangle, |c_1\rangle, |c_2\rangle, |s_0\rangle, |s_1\rangle$ and $|s_2\rangle$ are the input qubits and $|o_0\rangle, |o_1\rangle, |o_2\rangle$ are the output states. Following the case in (1), the following conclusion about Fig. 2 is established:

If $|o_0\rangle = |0\rangle$, then $|c_0\rangle = |s_0\rangle$; if $|o_0\rangle = |1\rangle$, then $|c_0\rangle \neq |s_0\rangle$;

Fig. 3 CNOT gate



If $|o_1\rangle = |0\rangle$, then $|c_1\rangle = |s_1\rangle$; if $|o_1\rangle = |1\rangle$, then $|c_1\rangle \neq |s_1\rangle$;
 If $|o_2\rangle = |0\rangle$, then $|c_2\rangle = |s_2\rangle$; if $|o_2\rangle = |1\rangle$, then $|c_2\rangle \neq |s_2\rangle$.

According to (1) and (2), proposition 1 is established. That is, when the corresponding output qubit is $|0\rangle$, the two qubits being compared are the same. When the corresponding output qubit is $|1\rangle$, the two qubits being compared are different. \square

Theorem 1 *LSQb information hiding algorithm is rational for NCQI.*

Proof To prove this theorem, there are two problems needing to be solved. \square

Problem 1 Before embedding secret qubits into the least significant qubits of *RGB* channels (i.e. $|R_0\rangle, |G_0\rangle, |B_0\rangle$), secret qubits and $|R_0\rangle, |G_0\rangle, |B_0\rangle$ should be compared.

Problem 2 The concrete unitary operators should be designed to realize the aim of embedding the secret qubits into $|R_0\rangle, |G_0\rangle, |B_0\rangle$ which are the least significant qubits of the relevant pixels in the cover image.

Solution for problem 1 Obviously, from proposition 1, utilizing three qubits comparator in Fig. 2, problem 1 has a perfect solution.

Concretely speaking, secret binary qubits $|s_i\rangle, i = 0, 1, 2$ and the qubits $|R_0\rangle, |G_0\rangle, |B_0\rangle$ of the first pixel in the cover image are taken as the inputs of the quantum comparator in Fig. 2. Three comparison results between $|s_0\rangle$ and $|R_0\rangle, |s_1\rangle$ and $|G_0\rangle, |s_2\rangle$ and $|B_0\rangle$ are obtained, which are denoted as $|o_0\rangle, |o_1\rangle, |o_2\rangle$. Through analyzing the results of the output qubits, the aim of comparing secret binary qubits $|s_i\rangle, i = 0, 1, 2$ and the qubits $|R_0\rangle, |G_0\rangle, |B_0\rangle$ is realized. Similarly, the comparisons between other secret qubits $|s_j\rangle, |s_{j+1}\rangle, |s_{j+2}\rangle, j = 3, 6, \dots, 3t - 3$ and $|R_0\rangle, |G_0\rangle, |B_0\rangle$ of other $t - 1$ relevant pixels in the cover image can also be achieved.

Solution for problem 2 New unitary operators can be designed to achieve the secrets embedding.

Unitary operators are designed according to the comparison results. Each of the comparison results $|o_i\rangle, i = 0, 1, \dots, 3t - 1$ has two cases, i.e. $|s_i\rangle = |c_0\rangle$ (the same, noted as S) and $|s_i\rangle \neq |c_0\rangle$ (the different, noted as D), $c = R, G, B$. There are $2 \times 2 \times 2 = 8$ cases for us to analyze.

(1) If the results are S, S, S, unitary transform U_0 is applied.

$$U_0 = I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0}^{2^n-1} |ji\rangle \langle ji| \right)$$

(2) If the results are S, S, D, unitary transform U_1 is applied.

$$U_1 = I^{\otimes 3q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(3) If the results are S, D, S, unitary transform U_2 is applied.

$$U_2 = I^{\otimes 2q-1} \otimes U \otimes I^{\otimes q} \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(4) If the results are D, S, S, then unitary transform U_3 is applied.

$$U_3 = I^{\otimes q-1} \otimes U \otimes I^{\otimes 2q} \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(5) If the results are S, D, D, then unitary transform U_4 is applied.

$$U_4 = I^{\otimes 2q-1} \otimes U \otimes I^{\otimes q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(6) If the results are D, D, S, then unitary transform U_5 is applied.

$$U_5 = I^{\otimes q-1} \otimes U \otimes I^{\otimes q-1} \otimes U \otimes I^{\otimes q} \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(7) If the results are D, S, D, then unitary transform U_6 is applied.

$$U_6 = I^{\otimes q-1} \otimes U \otimes I^{\otimes q} \otimes I^{\otimes q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

(8) If the results are D, D, D, then unitary transform U_7 is applied.

$$U_7 = I^{\otimes q-1} \otimes U \otimes I^{\otimes q-1} \otimes U \otimes I^{\otimes q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, i \neq j}^{2^n-1} |ji\rangle \langle ji| \right)$$

where $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Whether the above unitary operators truly realize the aim of hiding secret qubits should be proven. In the following proof, unitary operator U_1 corresponding to one of the result S, S, D is taken as an example to analyze.

$$\begin{aligned}
 &U_1(|I\rangle) \\
 &= I^{\otimes 3q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, ji \neq yx}^{2^n-1} |ji\rangle \langle ji| \right) (|I\rangle) \\
 &= I^{\otimes 3q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, ji \neq yx}^{2^n-1} |ji\rangle \langle ji| \right) \\
 &\quad \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |c(y, x)\rangle \otimes |yx\rangle \right) \\
 &= I^{\otimes 3q-1} \otimes U \otimes |yx\rangle \langle yx| + I^{\otimes 3q} \otimes \left(\sum_{j=0}^{2^n-1} \sum_{i=0, ji \neq yx}^{2^n-1} |ji\rangle \langle ji| \right) \\
 &\quad \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |R_{q-1} \cdots R_0 G_{q-1} \cdots G_0 B_{q-1} \cdots B_0\rangle \otimes |yx\rangle \right) \\
 &= \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0, ji \neq yx}^{2^n-1} |R_{q-1} \cdots R_0 G_{q-1} \cdots G_0 B_{q-1} \cdots B_0\rangle \otimes |ji\rangle \\
 &\quad + |R_{q-1} \cdots R_0 G_{q-1} \cdots G_0 B_{q-1} \cdots \overline{B_0}\rangle \otimes |yx\rangle \tag{3}
 \end{aligned}$$

where

$$\overline{|B_0\rangle} = \begin{cases} |1\rangle, & |B_0\rangle = |0\rangle \\ |0\rangle, & |B_0\rangle = |1\rangle \end{cases}$$

Obviously, from the above result, the function of the unitary operator U_1 is just changing least significant blue qubit $|B_0\rangle$ of the relevant pixel $|yx\rangle$ into $\overline{|B_0\rangle}$. It does not change color information of other pixels. Again, the other two secret qubits are respectively equal to $|R_0\rangle$ and $|G_0\rangle$, so they can also be regarded as being embedded into the least significant qubits $|R_0\rangle$ and $|G_0\rangle$ of the cover image. Other cases can also be proven in a similar way. From the above explanations, problem 2 is solved.

Once solving problem 1 and problem 2, theorem 1 is established. Since in order to realize the aim of embedding $3t$ secret qubits, it just needs to divide the secret qubits into t groups, then execute t times comparator and t times unitary operator.

Note 1 It should be noted that when executing comparator once, three secret qubits are compared.

Note 2 We should note that when performing unitary operator once, three secret qubits are embedded into cover image.

4 LSQb information hiding method of NCQI

In this section, LSQb algorithm of NCQI is proposed by employing the three qubits comparator and unitary operators proposed in Sect. 3, which hides the secret qubits stream into the LSQb of *RGB* channels in the cover image.

4.1 LSQb information hiding algorithm

LSQb information hiding method rooted in NCQI is described in details as in the following steps.

Step 1 Comparing the secret qubits s_0, s_1, s_2 with the three least significant qubits R_0, G_0, B_0 of the first pixel in the original cover image. Utilizing the three qubits comparator in Fig. 2, secret qubits s_0, s_1, s_2 and the last three qubits R_0, G_0, B_0 is compared sequentially. Comparison results from the comparator are denoted as o_0, o_1, o_2 , respectively.

Step 2 LSQb information hiding. According to the values of o_0, o_1 and o_2 , one of the unitary operators from the set $\{U_0, U_1, U_2, U_3, U_4, U_5, U_6, U_7\}$ is chosen to operate on the original cover image state $|I\rangle$ to realize the aim of embedding the first three secret qubits.

Step 3 Repeating Step 1 and Step 2 t times. In the beginning, the length of the secret binary qubits $s_0, s_1 \cdots s_{3t-2}, s_{3t-1}$ is supposed as $3t$. In order to complete the task of embedding all secret binary qubits, it is necessary to repeat Step 1 t times to execute $3t$ times comparison and step 2 t times to hide $3t$ secret qubits. Since the secret qubits have been divided into t groups and every group has 3 qubits. Obviously, in this process, t relevant pixels in the cover image are used. Applying unitary transform $\prod_{i=1}^t T_i$ on the state $|I\rangle$ can realize the goal of information hiding. Operator T_i , which is in the set $\{U_0, U_1, U_2, U_3, U_4, U_5, U_6, U_7\}$, is decided by the output values of the comparator.

Note 3 The length of secret binary qubits can always be supposed as $3t, t \leq 2^{2n}$. If secret binary qubits' length is less than $3t$, it can be increased to $3t$ by using the same least significant color qubits of relevant pixels in the original image.

Figure 4 shows the quantum circuit of LSQb information hiding algorithm. It can be seen that after the function of the unitary operators $T_i, i = 1 \cdots t$, the LSQb-embedded quantum image is obtained.

4.2 LSQb information extraction algorithm

Secret binary qubits stream can be accurately extracted by using control-swap gates.

Step 1 Separately extracting the last qubits of three channels *R, G, B* corresponding to t relevant pixels. All the extracted qubits constitute sequentially the secret binary qubits stream.

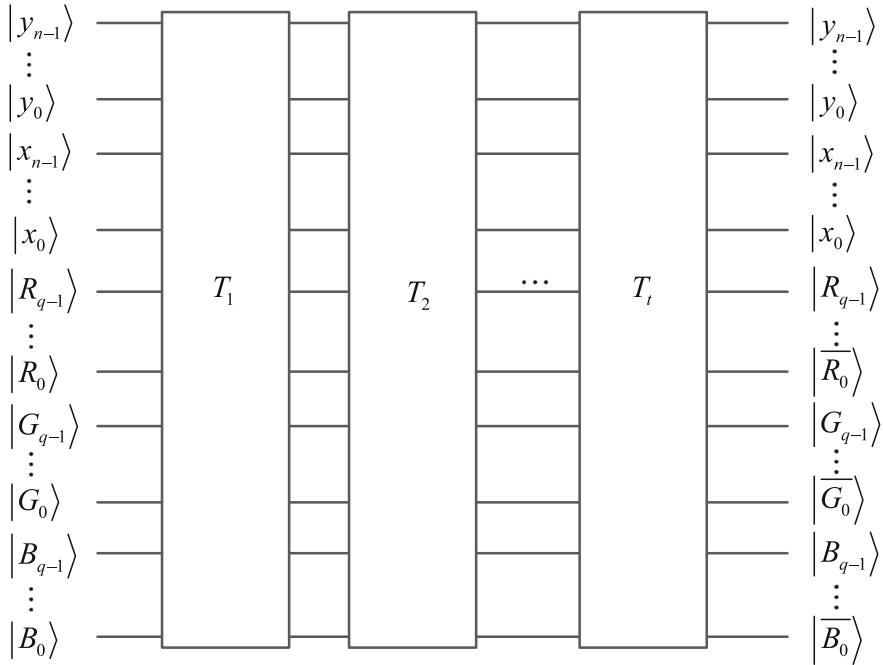


Fig. 4 Quantum circuit of information hiding algorithm

Figure 5 describes the quantum circuit of extracting the secret qubits stream. When extracting the secrets, the extraction order in terms of cover image is from left to right and from top to bottom. That is, the control qubits in Fig. 5 is set from the natural number 0 until the beginning of coding sequence of natural number $t - 1$.

Original quantum image can also be recovered in a lossless manner. Applying $\prod_{i=1}^t T_i^\dagger$ on the embedded image, the original quantum image $|I\rangle$ can be recovered accurately, where T_i^\dagger is the conjugate transpose of T_i . Obviously, all transforms T_i , $i = 1, \dots, t$ used in information hiding algorithm are reversible, so T_i^\dagger is meaningful. Figure 6 describes the quantum circuit of recovering the original quantum cover image.

In all, LSQb information hiding algorithm is designed based on the three qubits comparator and the unitary operator. Obviously, the algorithm is absolutely blind because the extraction procedure does not need the original cover image. The whole procedure of information extracting, which only needs control-swap gates, does not need any quantum measurement operation or any other help from classical computer. Figure 7 describes the whole framework of LSQb information hiding algorithm.

4.3 Computational complexity

In quantum image processing, the circuit’s complexity depends on what is considered to be an elementary gate. Generally, CNOT gate is chosen as a basic unit. For the LSQb information hiding algorithm, due to the properties of quantum parallel computation,

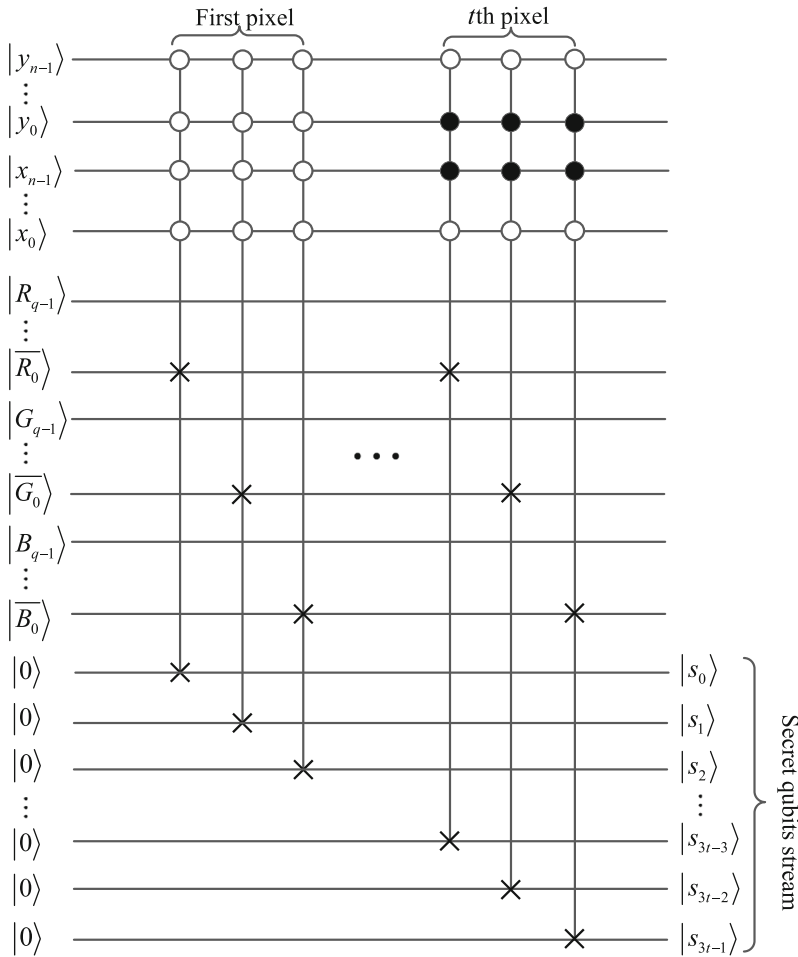


Fig. 5 Quantum circuit of extracting secret qubits stream

the utilization of quantum transforms speeds up the information hiding and extraction. The computational complexity of the information hiding algorithm depends on three qubits comparator and unitary operator T_i .

Three qubits comparator consists of three CNOT gates. So the quantum comparator’s complexity is no more than $O(3)$. Unitary operator T_i can be regarded as almost a $2n$ -control-NOT gate. Reference [33] has pointed out that a t -control-qubit-NOT gate is equivalent to $2(t - 1)$ Toffoli gates + 1 CNOT gate. Again, one Toffoli gate can be constructed by 6 CNOT gates. So the complexity of the unitary operator T_i is $O(2(2n - 1) \cdot 6 + 1)$, i.e. $O(24n - 11)$.

In step 1, quantum comparator is carried out one time, so its complexity is $O(3)$. In step 2, unitary transform T_i is operated on the original quantum image, so the complexity is near $O(24n - 11)$. In step 3, step 1 and step 2 are repeated t times.

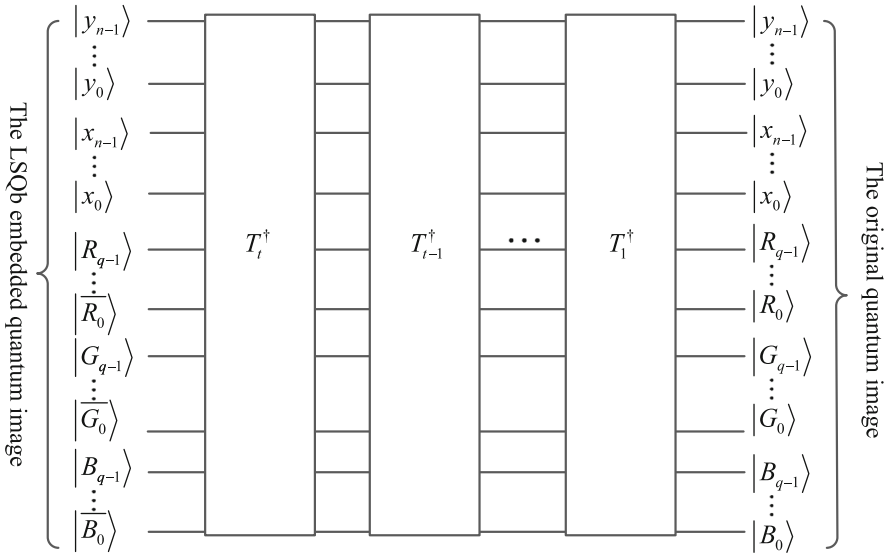


Fig. 6 Quantum circuit of recovering the cover image

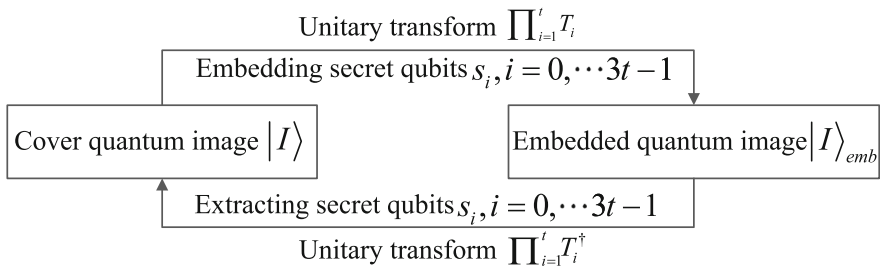


Fig. 7 Framework of information hiding algorithm

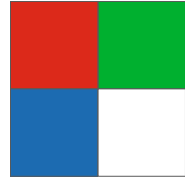
So the complexity of our algorithm is $O((24n - 8)t)$. The complexity is linear to the length $3t$ of the secret binary qubits stream ($(24n - 8)t = \frac{24n - 8}{3} \cdot 3t$), which to some extent shows the feasibility of the proposed LSQb information hiding scheme.

4.4 Example

In order to understand LSQb scheme clearly, one specific circuit is given as another application example of our presented idea.

For example, there is a color digital image sized 2×2 , which is shown in Fig. 8. The NCQI representation of Fig. 8 can be expressed as the following form $|I(\theta)\rangle$.

Fig. 8 A 2×2 color digital image



$$\begin{aligned}
 |I(\theta)\rangle &= \frac{1}{\sqrt{2^2}} \left[\left| \underbrace{11111111}_R \underbrace{00000000}_G \underbrace{00000000}_B \right\rangle \otimes |00\rangle \right. \\
 &+ \left. \left| \underbrace{00000000}_R \underbrace{11111111}_G \underbrace{00000000}_B \right\rangle \otimes |01\rangle \right. \\
 &+ \left. \left| \underbrace{00000000}_R \underbrace{00000000}_G \underbrace{11111111}_B \right\rangle \otimes |10\rangle \right. \\
 &+ \left. \left| \underbrace{11111111}_R \underbrace{11111111}_G \underbrace{11111111}_B \right\rangle \otimes |11\rangle \right]
 \end{aligned}$$

Suppose the binary secret qubits stream has the form 000011100110. Obviously, the least significant qubits of three channels are 100010001111. Then we have:

$$\begin{aligned}
 s_0 &\neq c_0, s_1 = c_1, s_2 = c_2, s_3 = c_3, s_4 = c_4, s_5 \neq c_5, \\
 s_6 &\neq c_6, s_7 \neq c_7, s_8 = c_8, s_9 = c_9, s_{10} = c_{10}, s_{11} \neq c_{11}
 \end{aligned}$$

Qubits s_i and $c_i, i = 0, \dots, 11$ are corresponding to secret qubits and least significant qubits, respectively.

Following the proposed algorithm, the unitary operators U_1, U_2, U_3 and U_4 are designed as the following form.

$$U_1 = I^{\otimes 7} \otimes U \otimes I^{\otimes 16} \otimes |00\rangle \langle 00| + I^{\otimes 24} \otimes \sum_{j=0}^1 \sum_{i=0, ji \neq 00}^1 |ji\rangle \langle ji|$$

$$U_2 = I^{\otimes 23} \otimes U \otimes |01\rangle \langle 01| + I^{\otimes 24} \otimes \sum_{j=0}^1 \sum_{i=0, ji \neq 01}^1 |ji\rangle \langle ji|$$

$$U_3 = I^{\otimes 7} \otimes U \otimes I^{\otimes 7} \otimes U \otimes I^{\otimes 8} \otimes |10\rangle \langle 10| + I^{\otimes 24} \otimes \sum_{j=0}^1 \sum_{i=0, ji \neq 10}^1 |ji\rangle \langle ji|$$

$$U_4 = I^{\otimes 23} \otimes U \otimes |11\rangle \langle 11| + I^{\otimes 24} \otimes \sum_{j=0}^1 \sum_{i=0, ji \neq 11}^1 |ji\rangle \langle ji|$$

After the function of the operators U_1, U_2, U_3 and U_4 , the original quantum cover image evolves into the quantum image $|I(\theta)\rangle_{emb}$.

$$\begin{aligned}
 & |I(\theta)\rangle_{emb} \\
 &= \frac{1}{\sqrt{2^2}} \left[\left| \underbrace{11111110}_R \underbrace{00000000}_G \underbrace{00000000}_B \right\rangle \otimes |00\rangle \right. \\
 & \quad + \left| \underbrace{00000000}_R \underbrace{11111111}_G \underbrace{00000001}_B \right\rangle \otimes |01\rangle \\
 & \quad + \left| \underbrace{00000001}_R \underbrace{00000000}_G \underbrace{11111110}_B \right\rangle \otimes |10\rangle \\
 & \quad \left. + \left| \underbrace{11111111}_R \underbrace{11111111}_G \underbrace{11111110}_B \right\rangle \otimes |11\rangle \right]
 \end{aligned}$$

Obviously, from the form $|I(\theta)\rangle_{emb}$, it can be seen that the secret qubits have been embedded into the cover image. Also, the extracting quantum circuit can be depicted in Fig. 9 according to the proposed algorithm.

5 Simulation and analysis

In this section, several analysis in terms of visual quality, capacity, comparison with other works and quantum measurement on the outcome are introduced. Since a practical and useful quantum computer is unavailable, the simulations of the quantum circuit and algorithm are executed on a classical computer equipped with software MATLAB. Simulations are based on the MATLAB 7.12.

5.1 Visual quality

The peak-signal-to-noise (PSNR) is one of the most used indicator for comparing the fidelity of a stego-image with its original version. PSNR is defined as the following form

$$\begin{aligned}
 PSNR &= 20 \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \\
 MSE &= \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - J(i, j)]^2
 \end{aligned}$$

where I and J are two different gray images, MAX_I is the maximum pixel of image I . In our algorithm, I and J correspond to the original image and the stego-image, respectively.

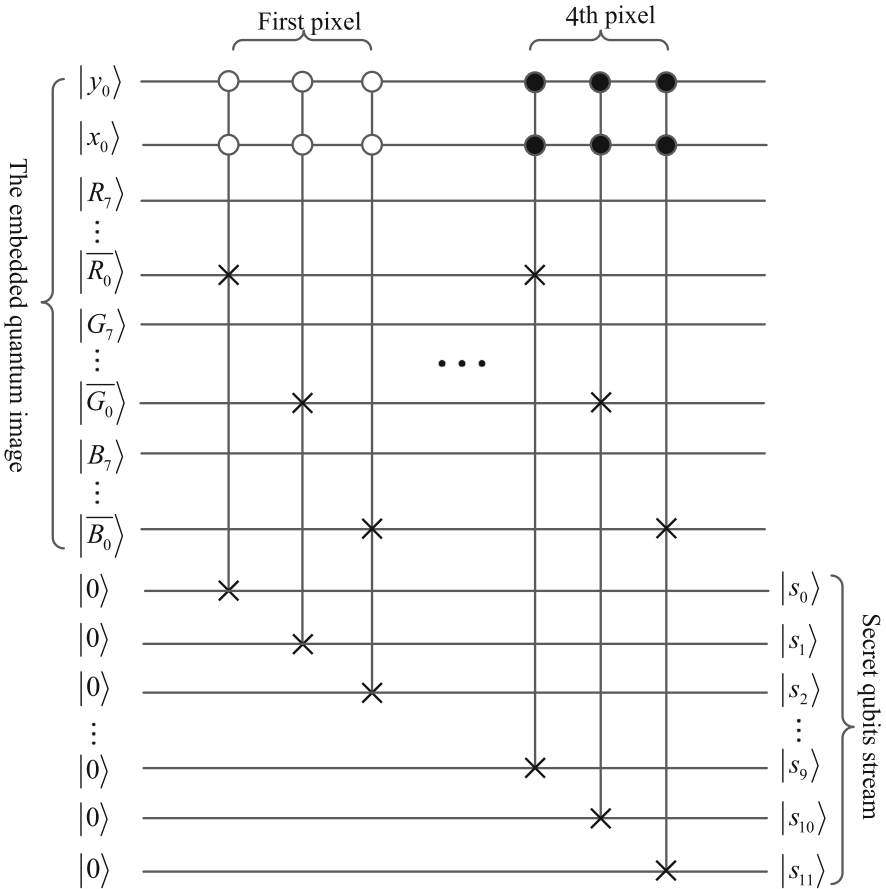


Fig. 9 Quantum circuit of extracting secret qubits for the example

PSNR is inversely proportional to MSE. Actually, MSE can be deemed as a ratio of the number of pixels that has been changed during the embedding process. It is independent with the size of cover image.

Since our algorithm is a LSB-based algorithm, if a pixel’s LSB qubit is the same as the message bit it accommodates, $[I(i, j) - J(i, j)]^2 = 0$. Suppose $MAX_I = 255$ for 8-bit natural image and $MSE = 0.5$, that means half of the pixels is changed, then

$$PSNR = 20 \log_{10} \left(\frac{255}{\sqrt{0.5}} \right) = 51.1411$$

Even if every pixel is changed, i.e. $MSE=1$, PSNR still can reach 48.1308 dB.

Some simulation examples are shown in Fig. 10, where (a)–(d) with 256×256 and (e) “message” with 256×256 are used as the carrier and the secret image, respectively. The visual quality of the embedded images is obtained in Table 1. It can be seen that the PSNR is around 51 dB, which indicates that the invisibility of our scheme is good.

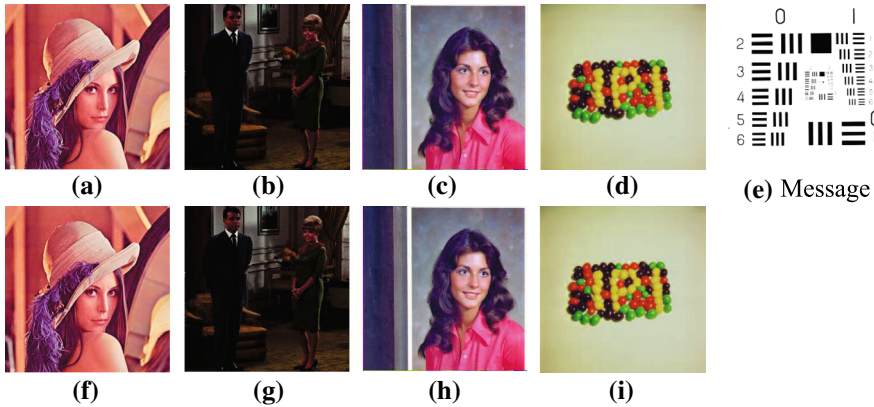


Fig. 10 Simulation examples by LSQb algorithm of color digital images. **a–d** are four cover images and **e** is message. **f–i** are four embedded images

Table 1 PSNR value of the simulation results

Cover image	Embedded image	PSNR (dB)
(a)	(f)	50.7120
(b)	(g)	50.5868
(c)	(h)	51.0501
(d)	(i)	50.9208

5.2 Capacity

Steganography capacity is defined as the ratio between the number of message bits and the number of cover pixels. Therefore, the capacity of the proposed algorithm is

$$C = \frac{\text{The number of message qubits}}{\text{The number of cover image's pixels}} = \frac{3t}{2^{2n}} \text{ (bit/pixel)} \tag{4}$$

From Eq. (4), it can be seen that the capacity is proportional to the length of secret binary qubits stream. The maximum of capacity can be reached at 3 bit/pixel when $t = 2^{2n}$.

5.3 Comparison analysis

In this section, our work and the Ref. [31] are compared, especially pointing out the differences between them.

The feasibility of LSQb information hiding algorithm based on NEQR was presented in [31]. However, the discussion and focus of this paper is on the reasonability and feasibility of LSQb hiding algorithm rooted in NCQI, and the major contribution of our work lies in the designment of unitary operators.

To show the novelty and advantage of our idea, the proposed scheme is compared with the related scheme, especially [31]. Analysis of the differences is given mainly from the following aspects.

The first important distinguish is that these two schemes focus on two entirely different research targets, i.e., NEQR and NCQI. NEQR can only represent gray image, while NCQI can represent color image. So these two schemes will be applied into different fields.

In classical digital image processing, some gray image processing algorithms can be directly applied into the color digital image. However, in quantum image processing, gray image processing algorithms cannot be directly applied into the color digital image. We have to design different methods for the realization of LSQb for NEQR and NCQI.

In [31], the specific LSQb information hiding algorithm based on NEQR is given through constructing the unitary operators u_i , $i = 0, 1, \dots, 2^{2n} - 1$, which can realize the aim of embedding secret qubits into the least significant qubit of gray information.

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

The paper offers a novel method for the realization of LSQb information hiding of NCQI. In our work, to achieve the aim of embedding secret qubits into the least significant qubits of three channels *RGB*, the different unitary operators, which can be seen in Sect. 3, are constructed based on analyzing the color encoding form of NCQI. In addition, the novel three qubits comparator is designed instead of using one qubit comparator in [31].

In a word, the entirely different unitary operators, which are of significance in the aspect of directing the construction of the information embedding algorithm, are the second difference and determine our work is not similar to the work [31]. Since the most important work in quantum image processing lies in designing the unitary operators, then the corresponding quantum circuits can be given.

Except the differences in the secrets embedding process between our work and [31], that is, the entirely different unitary operators described in Sect. 3. There is another obvious distinction between these two works. In the process of extracting the secret qubits, in [31], we need to decompose the quantum embedded image state into the basis states, which is a complex work. However, in our proposed work, it only needs to use the control-swap gates to exchange the secret qubits with the ancillary qubits $|0\rangle$. Compared with [31], this is our obvious advantage.

Finally, we should point out that our work is not the extension of the work in [31]. From the above descriptions, there are clear differences between the two works. The two works research two different objects and show two distinct ultimate information embedding algorithm and extraction algorithm, then finally can be applied into different fields.

5.4 Analysis of quantum measurement on the outcome

The impact of quantum measurement on the outcome is analyzed in this section.

Fig. 11 Quantum circuit symbol for measurement

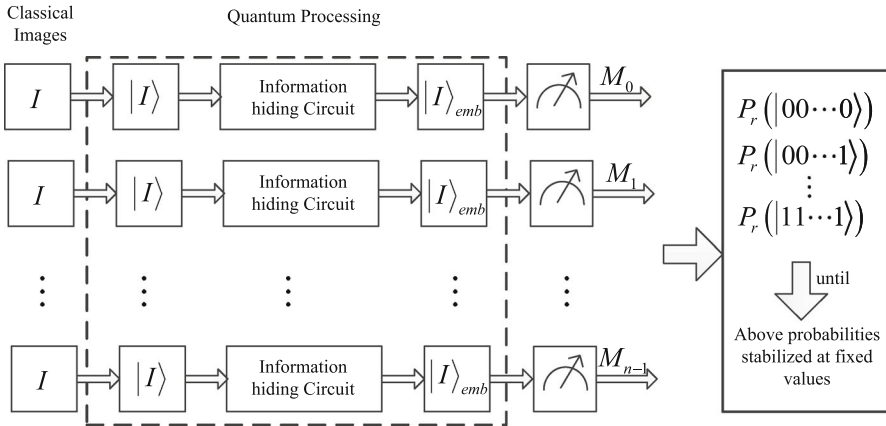
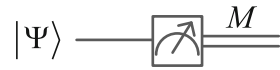


Fig. 12 Block diagram of measurement procedure on quantum computers

When designing a quantum image processing algorithm, the authors generally consider the measurement in the final step, i.e., quantum simulation, which converts the quantum information into the classical information in form of probability distributions.

In the design of the whole LSQb information hiding and extracting algorithm, there is no quantum measurement operation. However, the projective measurement is used in the final step of quantum simulation. The final step in quantum simulation is the measurement which converts the quantum information into the classical information in form of probability distributions, i.e., it converts a single qubit state $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a probability classical bit M (distinguished from a qubit by drawing it as a double-line wire), which is 0 with probability $|\alpha|^2$, or 1 with probability $|\beta|^2$ as shown in Fig. 11.

In practice, the quantum state cannot be practically observed in quantum system because the measurement will destroy the superposition. And what's worse is that, it is not allowed to make copies of the state and measure each one due to the Non-Cloning theorem. Hence, it is necessary to repeat the construction of the embedded image state n times ($n > 1$), and measure each one to summarize the measurement results from which we can estimate the embedded image.

Measurement results on the embedded image sized $2^n \times 2^n$ find a value in the set $\{s_1, s_2, \dots, s_{2^{2n+3q}}\}$, which $s_i, i = 1, 2, \dots, 2^{2n+3q}$ are basis states in 2^{2n+3q} dimension Hilbert space. After multiple measurements, these basis states follow a probability distribution. The measurement will be continued until the probability of every basis state stabilized at a fixed value. According to law of large numbers, there is a limit for these basis states. The block diagram of measurement procedure on quantum computer is shown in Fig. 12.

6 Conclusion

In this paper, a LSQb information hiding algorithm is proposed for quantum image model NCQI. The proposed method constructs a LSQb-embedded image and mainly contains two steps: (1) qubits comparison and (2) qubits embedding. In the qubits comparison step, the designed three qubits comparator is utilized to compare the secret qubits with three least significant qubits of *RGB* channels of one pixel in the cover image. In the qubits embedding step, eight types of unitary operators are constructed, but it should be noted that which kind of unitary operators should be acted on the cover image. These unitary operators are decided by the output qubits of the comparator. When extracting the secret qubits, control-swap gates are used instead of introducing quantum measurement. So our algorithm has at least two advantages: (1) the algorithm is absolutely blind since the extracting procedure does not need the original cover image. (2) The whole procedure of information extraction does not need any quantum measurement operation or any other help from classical computer. Complexity analysis, simulation results and comparison analysis with other work show that the proposed LSQb information hiding algorithm has good performance. Designing other quantum image steganography algorithms, especially LSQb-based algorithms, is our future work.

Acknowledgments This work is supported by the National Science Foundation of China (Grant Numbers: 61471141, 61301099, 61361166006), and Basic Research Project of Shenzhen, China (Grant Numbers: JCYJ20150513151706561). We deeply thanks the previous researchers' work about NEQR. Thanks are due to many anonymous reviewers for their assistance with the discussion about the designed three qubits comparator and the quantum measurement.

References

1. Benioff, P.: The computer as a physical system: a microscopic quantum mechanical Hamiltonian models of computers as represented by Turing machines. *J. Stat. Phys.* **22**(5), 563–591 (1980)
2. Feynman, R.P.: Simulating physics with computers. *Int. J. Theor. Phys.* **21**(6/7), 467–488 (1982)
3. Mastriani, M.: Quantum image processing? [arXiv: 1512.02942](https://arxiv.org/abs/1512.02942) [quan-ph] (2016)
4. Venegas-Andraca, S.E., Bose, S.: Storing, processing and retrieving an image using quantum mechanics. *Proc. SPIE Conf. Quantum Inf. Comput.* **5105**, 137–147 (2003)
5. Venegas-Andraca, S.E., Ball, J.L., Burnett, K., Bose, S.: Processing images in entangled quantum systems. *Quantum Inf. Process.* **9**, 1–11 (2010)
6. Latorre, J.I.: Image compression and entanglement. [arXiv: quant-ph/0510031](https://arxiv.org/abs/quant-ph/0510031) (2005)
7. 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 (2010)
8. Zhang, Y., Lu, K., Gao, Y.H., Xu, K.: A novel quantum representation for log-polar images. *Quantum Inf. Process.* **12**(9), 3103–3126 (2013)
9. Zhang, Y., Lu, K., Gao, Y.H., Wang, M.: NEQR: a novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **12**(8), 2833–2860 (2013)
10. Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. *Quantum Inf. Process* **14**(5), 1559–1571 (2015)
11. Sun, B., Le, P.Q., Iliyasu, A.M.: A multi-channel representation for images on quantum computers using the *RGB α* color space. In: *Intelligent Signal Processing, 2011 IEEE 7th International Symposium on*. Floriana, Malta: IEEE. pp. 1–6 (2011)
12. Sang, J.Z., Wang, S., Li, Q.: A novel quantum representation for color digital images. *Quantum Inf. Process*, submitted (2016)

13. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
14. Fijany, A., Williams, C.: Quantum wavelet transform: fast algorithm and complete circuits. [arXiv:quant-ph/9809004](https://arxiv.org/abs/quant-ph/9809004) (1998)
15. Klappenecker, A., Roetteler, M.: Discrete cosine transforms on quantum computers. In: IEEEER8-EURASIP Symposium on Image and Signal Processing and Analysis (ISPA01), Pula, Croatia. pp. 464–468 (2001)
16. Le, P.Q., Iliyasu, A.M., Dong, F.Y., Hirota, K.: Fast geometric transformation on quantum images. *IAENG Int. J. Appl. Math.* **40**(3), 113–123 (2010)
17. Jiang, N., Wu, W.Y., Wang, L.: the quantum realization of Arnold and Fibonacci image scrambling. *Quantum Inf. Process.* **13**(5), 1223–1236 (2014)
18. Jiang, N., Wang, L., Wu, W.Y.: Quantum Hilbert image scrambling. *Int. J. Theor. Phys.* **53**(7), 2463–2484 (2014)
19. Wang, J., Jiang, N., Wang, L.: Quantum image translation. *Quantum Inf. Process.* **14**(5), 1589–1604 (2014)
20. Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. *Quantum Inf. Process.* **14**(5), 1559–1571 (2014)
21. Sang, J.Z., Wang, S., Niu, X.M.: Quantum realization of the nearest-neighbor interpolation method for FRQI and NEQR. *Quantum Inf. Process.* **15**, 37–64 (2016)
22. Jiang, N., Wu, W.Y., Wang, L., Zhao, N.: Quantum image pseudocolor coding based on the density-stratified method. *Quantum Inf. Process.* **13**(5), 1735–1755 (2015)
23. Mastriani, M.: Quantum Boolean Image Denoising. *Quantum Inf. Process.* **14**(5), 1647–1673 (2015)
24. Iliyasu, A.M., Phuc, Q.L., Dong, F., Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformation. *Inform. Sci.* **186**, 126–149 (2011)
25. Zhang, W.W., Gao, F., Liu, B., Jia, H.Y., Wen, Q., Chen, H.: A quantum watermark protocol. *Int. J. Theor. Phys.* **52**(2), 504–513 (2013)
26. Zhang, W.W., Gao, F., Liu, B., Wen, Q., Chen, H.: A watermark strategy for quantum images based on quantum Fourier transform. *Quantum Inf. Process.* **12**(2), 792–803 (2012)
27. Song, X.H., Wang, S., Liu, S., El-Latif, A.A., Niu, X.M.: A dynamic watermarking scheme for quantum images using quantum wavelet transform. *Quantum Inf. Process.* **12**(12), 3689–3706 (2013)
28. Song, X.H., Wang, S., Liu, S., El-Latif, A.A., Niu, X.M.: Dynamic watermarking scheme for quantum images based on Hadamard transform. *Multimedia Syst.* **20**(4), 379–388 (2014)
29. Miyake, S., Nakamae, K.: A quantum watermarking scheme using simple and small-scale quantum circuits. *Quantum Inf. Process.* (2016). doi:[10.1007/s11128-016-1260-9](https://doi.org/10.1007/s11128-016-1260-9)
30. Jiang, N., Wang, L.: A novel strategy for quantum image steganography based on Moiré Pattern. *Int. J. Theor. Phys.* **54**(3), 1021–1032 (2015)
31. Wang, S., Sang, J.Z., Song, X.H., Niu, X.M.: Least significant qubit (LSQB) information hiding algorithm for quantum image. *Measurement* **73**, 352–359 (2015)
32. Jiang, N., Zhao, N., Wang, L.: LSB based quantum image steganography algorithm. *Quantum Inf. Process.* **55**, 107–123 (2016)
33. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)