Quantum Information Processing (2020) 19:36
https://doi.org/10.1007/s11128-019-2523-z

Information hiding method based on quantum image by using Bell states

Cheng-Fu Su[1] · Chien-Yuan Chen[1]

Received: 18 November 2018 / Accepted: 22 November 2019 / Published online: 5 December 2019

Abstract
In this paper, we propose a novel information hiding method based on the NEQR quantum image and Bell states. We hide the secret information in the NEQR quantum image. The NEQR quantum image and the secret information are transferred to the recipient by using the quantum teleportation scheme. The recipient not only gets the secret information, but also holds the quantum image after one measurement. Our method can extract m secret bits after one measurement, while LSQb method can extract one secret bit.

Keywords Quantum information hiding · Quantum image processing · Quantum algorithm

1 Introduction

Due to the advantages of quantum mechanics overcoming the limitations of classical computation, quantum computation has attracted many researchers [1]. Many quantum algorithms have been proposed [1]. There are two famous quantum algorithms, Shor's factorization algorithm [2] and Grove's search algorithm [3]. The former provides a striking exponential speedup over the best known classical factorization algorithms. Therefore, the RSA system [4] will be successfully attacked by Shor's factorization algorithm. By Grove's search algorithm, we can obtain selected data from unsorted data in $O\left(\sqrt{N}\right)$ times, where N denotes the number of data. Grove's search algorithm provides a quadratic speedup over the best known classical algorithms.

✉ Chien-Yuan Chen
cychen07@nuk.edu.tw

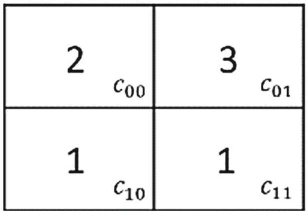
Cheng-Fu Su
devildream27@gmail.com

[1] Department of Computer Science and Information Engineering, National University of Kaohsiung, No. 700, Kaohsiung University Rd, Kaohsiung, Taiwan

In addition to computation speedup, quantum systems provide unconditional security based on no-cloning theorem and Hesienberg uncertainty theorem [5]. We can hide the secret information to avoid eavesdropping in the quantum system. The quantum data hiding methods are classified into three categories. First, quantum data hiding (QDH) [6, 7] embeds secret information by the physical of characteristic, local operations, and classical communications (LOCC). Second, narrow quantum steganography (QS) [8] hides secret information in quantum error-correcting code (QECC) or quantum image [9]. Last, quantum covert channels (QCC) [10] are utilized for key conveying in quantum cryptography.

In the second category, we pay attention to quantum images [11, 12]. Although many researchers have presented encryption algorithms [13–17] in quantum images, this paper only focuses on data hiding. In 2015, Wang et al. proposed least significant qubit (LSQb) information hiding algorithm for NEQR quantum image [18]. According to the color information and position information are entangled together in NEQR [19], they embedded the secret information into the least significant qubit of the color information by using the unitary operations. Therefore, like the traditional LSB method [20], LSQb method generates the quantum cover image hiding the secret information in the least significant qubit of the color information. Independently, Jiang et al. [21] proposed two LSB methods: standard LSB method and block LSB method. The standard LSB method hides one message bit in each pixel. In the block LSB method, each block only hides one message bit. In fact, the standard LSB method can be seen as a special case of the block LSB method. Obviously, the block LSB method provides more robustness.

In this paper, we hide the secret information in the $2^n \times 2^n$ NEQR quantum image with q-qubit color information. According to Yan et al.'s paper [11], the NEQR quantum image provides more accurate information retrieval. The NEQR quantum image and the secret information are transferred to the recipient by using the quantum teleportation scheme. The recipient not only gets the secret information, but also holds the quantum image after one measurement. At first, the third party constructs the $(4n + 2q + 2m)$-qubit general Bell state, including two quantum registers B_1 and B_2. The third party then distributes the registers B_1 and B_2 to the sender and the recipient, respectively. After getting the quantum register B_1, $(2n + q + m)$-qubit of half-Bell state, the sender attaches the q-qubit color register C, the $2n$-qubit position register P, and the m-qubit secret register M, to construct a $(4n + 2q + 2m)$-qubit quantum state. In the register C and the register P, the NEQR quantum image is produced by sub-operations gradually in quantum computation [19, 22, 23]. The sender then puts the secret information S into the register M by using the quantum operation CNOT. Because the sender and the recipient share $(4n + 2q + 2m)$-qubit general Bell state, the sender utilizes the quantum teleportation scheme [24] to transfer the NEQR quantum image and the secret information S to the recipient. In the quantum teleportation scheme, the sender must measure the register C, the register P, the register M, and the register B_1 and send measured values to the recipient by the classical channel. The recipient utilizes the measured values to recover the NEQR quantum image in the first $(2n + q)$ qubits of the register B_2 and the secret information S in the last m qubits of the register B_2. Last, the recipient gets information secret S after measuring the last m qubits of the register B_2 and retains a quantum image in the register B_2.



2 c_{00}	3 c_{01}
1 c_{10}	1 c_{11}

Fig. 1 An example of 2 × 2 classical image

The remainder of this paper is organized as follows. In the next section, Zhang et al.'s NEQR and Wang et al.'s method are reviewed. Section 3 describes our method. Section 4 gives an example of our method. The analysis and comparison of the proposed method are given in Sect. 5 and finally the last section, Sect. 6, concludes this paper.

2 Related work

In this section, we review Zhang et al.'s NEQR representation [19] and Wang et al.'s method [18]. In 2013, Zhang et al. proposed a novel enhanced quantum representation of digital images [19]. Their model is more effective than Le et al.'s model [22] in quantum images. In NEQR representation, the color information qubit sequence and the position information qubit sequence are entangled, where the color information denotes color information of the classical image. We set the color information as the binary code $c_i = b^i_{q-1}b^i_q \dots b^i_0$, where i denotes the position of the image and q ($q = 1$ for binary image, $q = 8$ for grayscale, $q = 24$ for RGB image, etc.) is the length of the color information. In a $2^n \times 2^n$ NEQR representation, we construct two quantum registers: the q-qubit color register C and the $2n$-qubit position register P. Then, we apply $2n$ Hadamard gates on the position register P and get

$$|\varphi\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}(|0\rangle_C|i\rangle_P). \tag{2.1}$$

We perform the quantum operation $U_P = \prod_{i=0}^{2^{2n}-1} V_{iP}$ on $|\varphi\rangle$ satisfying $V_{iP}(|0\rangle_C |i\rangle_P) = |c_i\rangle_C|i\rangle_P$ and get

$$|\varphi_1\rangle = U_P(|\varphi\rangle) = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}(|c_i\rangle_C|i\rangle_P). \tag{2.2}$$

We give an example to understand the NEQR representation. Figure 1 gives a classical image. We know that $n = 1, q = 2$. The color information c_{01} is 3. To construct the corresponding NEQR representation, we perform the quantum circuit of Fig. 2.

According to Fig. 2, we prepare two quantum registers and set an initial state:

$$|\varphi\rangle_0 = |00\rangle_C|00\rangle_P. \tag{2.3}$$

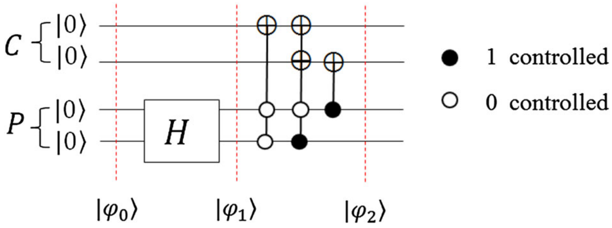


Fig. 2 Quantum circuit of the example

We execute two Hadamard gates on the position register P and get

$$\begin{aligned}|\varphi\rangle_1 &= |00\rangle_C\left(\frac{1}{2}(|00\rangle_P + |01\rangle_P + |10\rangle_P + |11\rangle_P)\right)\\ &= \frac{1}{2}(|00\rangle_C|00\rangle_P + |00\rangle_C|01\rangle_P + |00\rangle_C|10\rangle_P + |00\rangle_C|11\rangle_P). \qquad (2.4)\end{aligned}$$

Last, we utilize CNOT to control the image color information into the corresponding color register C. Then, we will get

$$\begin{aligned}|\varphi\rangle_2 &= \frac{1}{2}(|(0\oplus 1)0\rangle_C|00\rangle_P + |(0\oplus 1)(0\oplus 1)\rangle_C|01\rangle_P\\ &\quad + |0(0\oplus 1)\rangle_C|10\rangle_P + |0(0\oplus 1)\rangle_C|11\rangle_P)\\ &= \frac{1}{2}(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |01\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P) \qquad (2.5)\end{aligned}$$

Next, we review Wang et al.'s method [18]. Like the traditional LSB method [20], Wang et al.'s method embeds the secret information into the least significant qubit of the color information in the NEQR quantum image. First, the sender prepares an initial state $|\rho\rangle_0 = |0\rangle_C^{\otimes q}|0\rangle_P^{\otimes 2n}$. Then, according to the classical image, the sender constructs the corresponding a $2^n \times 2^n$ NEQR quantum image:

$$|\rho_1\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}(|c_i\rangle_C|i\rangle_P), \qquad (2.6)$$

where $c_i = \left(b_{q-1}^i b_{q-2}^i \ldots b_0^i\right), i = 0,\ 1\ldots, 2^{2n}-1$.

Now, the sender tries to embed the secret information $S = s_{2^{2n}-1}s_{2^{2n}-2}\ldots s_0$ into the least significant qubit of the color information c_i. To embed the secret bit s_m $(0 \le m \le 2^{2n}-1)$, the sender performs the quantum operation V_{jC} satisfying

$$\begin{aligned}V_{jC}(|\rho_1\rangle) &= V_{jC}\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|b_{q-1}^i b_{q-2}^i\ldots b_0^i\right\rangle_C|i\rangle_P\right)\right)\\ &= \frac{1}{2^n}\left(\left|b_{q-1}^j b_{q-2}^j\ldots b_1^j s_j\right\rangle_C|j\rangle\right) + \sum_{i=0,i\neq j}^{2^{2n}-1}|c_i\rangle_C|i\rangle_P). \qquad (2.7)\end{aligned}$$

After performing the quantum operation $U_C = \prod_{j=0}^{2^{2n}-1} V_{jC}$, the sender has

$$U_C(|\rho_1\rangle) = \prod_{j=0}^{2^{2n}-1} V_{jC}\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|b_{q-1}^i b_{q-2}^i \ldots b_0^i\right\rangle_C |i\rangle_P\right)\right)$$
$$= \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|b_{q-1}^i b_{q-2}^i \ldots b_1^i s_i\right\rangle_C |i\rangle_P\right). \tag{2.8}$$

Obviously, the secret information S has been embedded into the least significant qubit of the color information c_i in the NEQR quantum image.

We give an example to understand Wang et al.'s method [18]. The sender wants to embed the secret information $S = (1010)_2$ into the NEQR quantum image $|\rho_1\rangle = \frac{1}{2}$ $(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |01\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P)$. After performing the quantum operation $U_C = \prod_{j=0}^{2^2-1} V_{jC}$, the sender has

$$|\rho_2\rangle = U_C(|\rho_1\rangle) = \prod_{j=0}^{2^2-1} V_{jC}\left(\frac{1}{2}\sum_{i=0}^{2^2-1}\left(\left|b_1^i b_0^i\right\rangle_C |i\rangle_P\right)\right) = \frac{1}{2}\sum_{i=0}^{2^2-1}\left(\left|b_1^i s_i\right\rangle_C |i\rangle_P\right)$$
$$= \frac{1}{2}(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |00\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P). \tag{2.9}$$

The sender transfers the quantum state $|\rho_2\rangle$ to the recipient. But, how to extract the secret information $S = (1010)_2$ from $|\rho_2\rangle$? In Wang et al.'s method [18], the recipient directly measures the quantum state $|\rho_2\rangle$. One bit of the secret information S will be discovered. Here we introduce another extracting algorithm in Sang et al.'s method [25]. The recipient attaches four qubits, say M_0, M_1, M_2, andM_3, to the quantum state $|\rho_2\rangle$ and gets

$$|\rho_3\rangle = \frac{1}{2}\big(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |00\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P\big)|0\rangle_{M_0}|0\rangle_{M_1}|0\rangle_{M_2}|0\rangle_{M_3}. \tag{2.10}$$

The recipient then uses the control-swap operation to swap M_i and the least significant qubit of the color information c_i. We have

$$|\rho_4\rangle = \frac{1}{2}\big(|1\mathbf{0}\rangle_C|00\rangle_P|\mathbf{0}\rangle_{M_0}|0\rangle_{M_1}|0\rangle_{M_2}|0\rangle_{M_3} + |1\mathbf{0}\rangle_C|01\rangle_P|0\rangle_{M_0}|\mathbf{1}\rangle_{M_1}|0\rangle_{M_2}|0\rangle_{M_3}$$
$$+ |0\mathbf{0}\rangle_C|10\rangle_P|0\rangle_{M_0}|0\rangle_{M_1}|\mathbf{0}\rangle_{M_2}|0\rangle_{M_3} + |0\mathbf{0}\rangle_C|11\rangle_P|0\rangle_{M_0}|0\rangle_{M_1}|0\rangle_{M_2}|\mathbf{1}\rangle_{M_3}\big). \tag{2.11}$$

In the quantum state $|\rho_4\rangle$, the secret information has been extracted in $M_0, M_1, M_2,$ and M_3. If the recipient wants to get the classical secret information, he/she will face the same measurement problem in Wang et al.'s method.

3 Our method

Assume that the sender wants to send m-bit secret information S and a $2^n \times 2^n$ NEQR quantum image I to the recipient, where I includes the q-qubit color register C and the $2n$-qubit position register P. At first, the third party constructs the $(4n + 2q + 2m)$-qubit general Bell state $\frac{1}{\sqrt{2^{2n+q+m}}} \sum_{j=0}^{2^{2n+q+m}-1} |j\rangle_{B_1} |j\rangle_{B_2}$, where B_1 and B_2 are two quantum registers with the same length. The third party distributes the quantum registers B_1 and B_2 to the sender and the recipient, respectively. After getting the quantum register B_1, $(2n + q + m)$-qubit of half-Bell state, the sender constructs the quantum state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{2n+q+m}}} |0\rangle_C^{\otimes q} |0\rangle_P^{\otimes 2n} |0\rangle_M^{\otimes m} \left(\sum_{j=0}^{2^{2n+q+m}-1} |j\rangle_{B_1} \right), \tag{3.1}$$

by attaching the q-qubit color register C, the $2n$-qubit position register P and the m-qubit secret register M. The sender then applies $2n$ Hadamard gates on the position register P and the quantum operation U_P to generate a $2^n \times 2^n$ NEQR quantum image in the color register C and the position register P according to the classical image. Using Zhang et al.'s NEQR representation, the sender gets the following quantum state

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{4n+q+m}}} \left(\sum_{i=0}^{2^{2n}-1} |c_i\rangle_C |i\rangle_P \right) |0\rangle_M \left(\sum_{j=0}^{2^{2n+q+m}-1} |j\rangle_{B_1} \right), \tag{3.2}$$

where $\frac{1}{2^n} \left(\sum_{i=0}^{2^{2n}-1} |c_i\rangle_C |i\rangle_P \right)$ denotes the NEQR quantum image I. Next, the sender performs the operation U_s to put the secret information $S = s_{m-1} s_{q-2} \ldots s_0$ into the secret register M and gets

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{4n+q+m}}} \left(\sum_{i=0}^{2^{2n}-1} |c_i\rangle_C |i\rangle_P \right) |S\rangle_M \left(\sum_{j=0}^{2^{2n+q+m}-1} |j\rangle_{B_1} \right). \tag{3.3}$$

In $|\psi_3\rangle$, we let $|c_i\rangle_C |i\rangle_P |S\rangle_M$ be $|h_i\rangle_{CPM}$ and get

$$|\psi_3'\rangle = \frac{1}{\sqrt{2^{4n+q+m}}} \left(\sum_{i=0}^{2^{2n}-1} |h_i\rangle_{CPM} \right) \left(\sum_{j=0}^{2^{2n+q+m}-1} |j\rangle_{B_1} \right). \tag{3.4}$$

The sender next transfers h_i to the recipient by using the quantum teleportation scheme. The sender utilizes quantum operation U_B $(2n + q + m$ qubit of CNOT) to flip the register B_1 (the target qubit) according to quantum registers C, P, and M. Then, the sender gets

$$
\begin{aligned}
|\psi_4\rangle &= \frac{1}{\sqrt{2^{4n+q+m}}} U_B\left(\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}\right)\right)\\
&= \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}\right).
\end{aligned}
\tag{3.5}
$$

Actually, the registers B_1 and B_2 are entangled. Therefore, the quantum system is

$$
|\psi_4'\rangle = \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}|j\rangle_{B_2}\right).
\tag{3.6}
$$

Now, the sender performs $2n+q+m$ Hadamard gates on registers C, P, and M and has

$$
\begin{aligned}
|\psi_5\rangle &= \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}H^{\otimes(2n+q+m)}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}|j\rangle_{B_2}\right)\\
&= \frac{1}{2^{3n+q+m}}\left(\left(\sum_{i=0}^{2^{2n}-1}\sum_{k=0}^{2^{2n+q+m}-1}(-1)^{h_i\cdot k}|k\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}|j\rangle_{B_2}\right)\right).
\end{aligned}
\tag{3.7}
$$

Set $l = h_i \oplus j$. The above quantum state will be

$$
\begin{aligned}
|\psi_5'\rangle &= \frac{1}{2^{3n+q+m}}\left(\left(\sum_{i=0}^{2^{2n}-1}\sum_{k=0}^{2^{2n+q+m}-1}(-1)^{h_i\cdot k}|k\rangle_{CPM}\right)\left(\sum_{l=0}^{2^{2n+q+m}-1}|l\rangle_{B_1}|h_i\oplus l\rangle_{B_2}\right)\right)\\
&= \frac{1}{2^{3n+q+m}}\left(\sum_{i=0}^{2^{2n}-1}\sum_{k=0}^{2^{2n+q+m}-1}\sum_{l=0}^{2^{2n+q+m}-1}|k\rangle_{CPM}|l\rangle_{B_1}(-1)^{h_i\cdot k}|h_i\oplus l\rangle_{B_2}\right).
\end{aligned}
\tag{3.8}
$$

Now, the sender performs the measurement operation on registers $C, P, M,$ and B_1. The resulting quantum state is $\frac{1}{2^n}\left(|k\rangle_{CPM}|l\rangle_{B_1}\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\oplus l\rangle_{B_2}\right)$. The sender gets k and l after measurement and sends k and l to the recipient by the classical channel. After receiving k and l from the sender, the recipient has

$$|\psi_6\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i \oplus l\rangle_{B_2}. \tag{3.9}$$

The recipient performs the operation CNOT on $|\psi_6\rangle$ according to l and gets

$$|\psi_7\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i \oplus l \oplus l\rangle_{B_2}\right) = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\rangle_{B_2}\right). \tag{3.10}$$

Given $k = \left(k_{2n+q+m-1}k_{2n+q+m-2}\ldots k_0\right)$, the recipient generates the operation $U_z^{k_t} = \begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{\pi i\cdot k_t}\end{bmatrix}$ satisfying $\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{\pi i\cdot k_t}\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{\pi i\cdot k_t}\end{bmatrix} = I$, where $k_t \in \{0, 1\}, 0 \le t \le 2n+q+m-1$. These $2n+q+m$ operations form $U_z = \prod_{t=0}^{2n+q+m-1} U_z^{k_t}$. The recipient performs the operation U_z on $|\psi_7\rangle$ and gets

$$\begin{aligned}|\psi_8\rangle &= \frac{1}{2^n}U_z\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\rangle_{B_2}\right) = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}\left(\mathrm{e}^{\pi i\cdot h_i\cdot k}\right)|h_i\rangle_{B_2}\right)\\ &= \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}(-1)^{h_i\cdot k}|h_i\rangle_{B_2}\right) = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{B_2}\right).\\ &= \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle|i\rangle|S\rangle\right)_{B_2}\end{aligned} \tag{3.11}$$

After measuring the last m qubits of the register B_2, the recipient gets information secret S and a quantum image

$$|\psi_9\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle|i\rangle\right)_{B_2}. \tag{3.12}$$

In the following, Figs. 3 and 4 show, respectively, the quantum circuits of the sender and recipient. According to these quantum circuits, we design two quantum algorithms: quantum information hiding algorithm and quantum information extracting algorithm. Furthermore, we give the schematic for our method in Fig. 5.

Algorithm 1. **Quantum information hiding algorithm**

Input: the $2^n \times 2^n$ classical image (including the q-bit color information c_i), the m-bit secret information $S = s_{m-1}s_{q-2}\dots s_0$ and the quantum register B_1 ($(2n+q+m)$-qubit of half-Bell state from the third party).

Output: classical integers k, l, and quantum state $|\psi_6\rangle$.

Step 1. Construct an initial quantum state

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{2n+q+m}}}|0\rangle_C^{\otimes q}|0\rangle_P^{\otimes 2n}|0\rangle_M^{\otimes m}\left(\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}\right),$$

where C, P, M and, B_1 denote the q-qubit color register, the $2n$-qubit position register, the m-qubit secret register, and the $(2n+q+m)$-qubit of half-Bell state, respectively.

Step 2. Perform $2n$ Hadamard gates and the operation U_P to generate an NEQR quantum image in quantum registers C and P according to the classical image. Then, we get

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle_C|i\rangle_P\right)|0\rangle_M\left(\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}\right).$$

Step 3. Perform the operation U_s to put the secret information $S = s_{m-1}s_{q-2}\dots s_0$ into the secret register M and get

$$|\psi_3\rangle = \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle_C|i\rangle_P\right)|S\rangle_M\left(\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}\right).$$

Step 4. Perform quantum operation U_B to produce $|\psi_4\rangle$ by setting register C, P, and M as control bits and register B_1 as target bits. We then get

$$|\psi_4\rangle = \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}\right),$$

where $|h_i\rangle_{CPM} = |c_i\rangle_C|i\rangle_P|S\rangle_M$. Because the sender and the recipient hold the Bell state, this quantum system will be

$$|\psi_4'\rangle = \frac{1}{\sqrt{2^{4n+q+m}}}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}|j\rangle_{B_2}\right).$$

Step 5. Perform $(2n+q+m)$ Hadamard gates on registers C, P, and M. We get

$$|\psi_5\rangle = \frac{1}{2^{3n+q+m}}\left(\left(\sum_{i=0}^{2^{2n}-1}\sum_{k=0}^{2^{2n+q+m}-1}(-1)^{h_i\cdot k}|k\rangle_{CPM}\right)\left(\sum_{j=0}^{2^{2n+q+m}-1}|h_i\oplus j\rangle_{B_1}|j\rangle_{B_2}\right)\right).$$

Set $l = h_i \oplus j$, we have

$$|\psi_5'\rangle = \frac{1}{2^{3n+q+m}}\left(\sum_{i=0}^{2^{2n}-1}\sum_{k=0}^{2^{2n+q+m}-1}\sum_{l=0}^{2^{2n+q+m}-1}|k\rangle_{CPM}|l\rangle_{B_1}(-1)^{h_i\cdot k}|h_i\oplus l\rangle_{B_2}\right).$$

Step 6. Perform the measurement operation on registers C, P, M, and B_1. We get classical integers k and l after measurement. It is worthy of noting that the recipient has

$$|\psi_6\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\oplus l\rangle_{B_2}\right).$$

At last, the sender transfers the classical integers k and l to the recipient by the classical channel.

Algorithm 2. **Quantum information extracting algorithm**

Input: classical integers k, l, and the quantum state $|\psi_6\rangle$.

Output: secret information S and the quantum image $|\psi_9\rangle$.

Step 1. Perform the operation CNOT on $|\psi_6\rangle$ according to l and get

$$|\psi_7\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\oplus l\oplus l\rangle_{B_2}\right) = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}(-1)^{h_i\cdot k}|h_i\rangle_{B_2}\right).$$

Step 2. Perform the operation $U_z = \prod_{t=0}^{2n+q+m-1} U_z^{k_t}$ on $|\psi_7\rangle$ according to k and get

$$|\psi_8\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|h_i\rangle_{B_2}\right) = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle|i\rangle|S\rangle\right)_{B_2}.$$

Step 3. Measure the last m qubits of the register B_2 to extract secret information S and get a quantum image

$$|\psi_9\rangle = \frac{1}{2^n}\left(\sum_{i=0}^{2^{2n}-1}|c_i\rangle|i\rangle\right)_{B_2}.$$

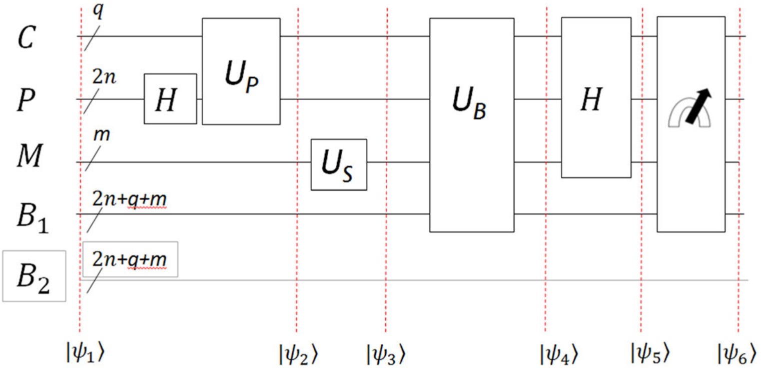


Fig. 3 Quantum circuit of the sender

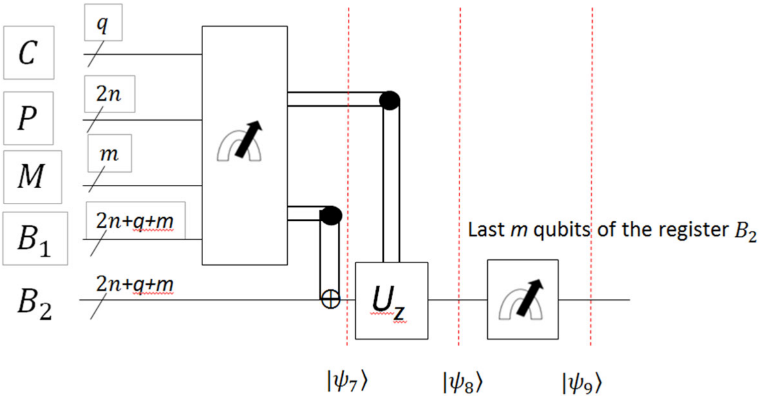


Fig. 4 Quantum circuit of the recipient

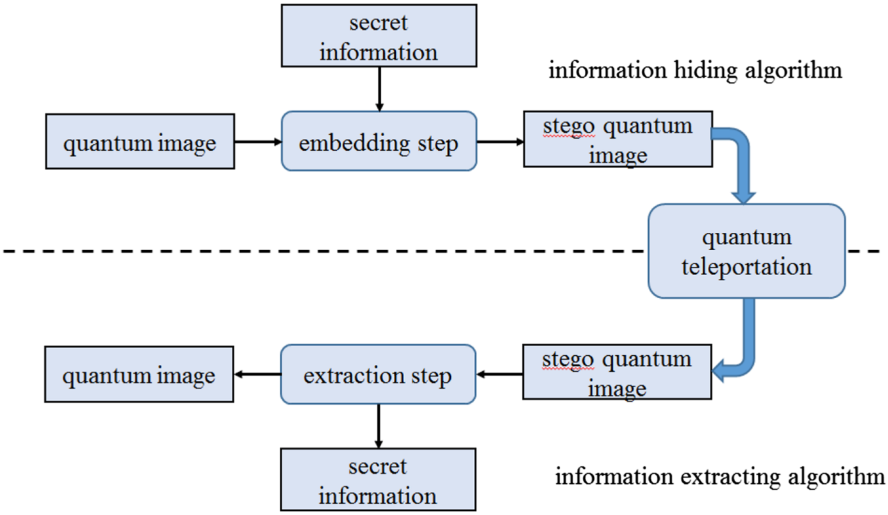


Fig. 5 Schematic for our method

4 An example of our method

To understand our method easily, we give an example in this section. First, we construct the quantum image $|\psi\rangle = \frac{1}{2}(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |01\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P)$ according to Fig. 1. Assume that the sender wants to transfer the secret information $S = (10)_2$ and the quantum image $|\psi\rangle$ to the recipient. Figure 6 shows the sender's quantum circuit which stems from Fig. 3. Similarly, Fig. 7 shows the recipient's quantum circuit which stems from Fig. 4. The simulation of our example has been implemented in Julia language, as shown in Fig. 8, and has been tested on a Core i7 4790 with 8 GB of RAM. The simulation shows that the recipient extracts the secret information $S = (10)_2$ and the quantum image $|\psi\rangle = \frac{1}{2}(|10\rangle_C|00\rangle_P + |11\rangle_C|01\rangle_P + |01\rangle_C|10\rangle_P + |01\rangle_C|11\rangle_P)$ if measured values $k = (010101)_2$ and $l = (110011)_2$.

5 Analysis and comparison

In our method, if the third party is trusted and the classical channel is secure, anyone cannot copy an unknown quantum state according to no-cloning theorem. Therefore, the information cannot be leaked in our method. But if the third party is untrusted, this party may be an eavesdropper who is in possession of a third sub-system that may be entangled with those given to the sender and the recipient [26]. For example, the third party uses the general Bell state $\frac{1}{\sqrt{2^{2n+q+m}}}\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}|j\rangle_{B_2}|j\rangle_{B_3}$ instead of $\frac{1}{\sqrt{2^{2n+q+m}}}\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}|j\rangle_{B_2}$, where the quantum register B_3 is the third subsystem. We further suppose that the third party can obtain the measured values k and l from the classical channel. After the recipient measuring the last m qubits of the register B_2 to extract secret information, the third party can use the sub-system $|j\rangle_{B_3}$

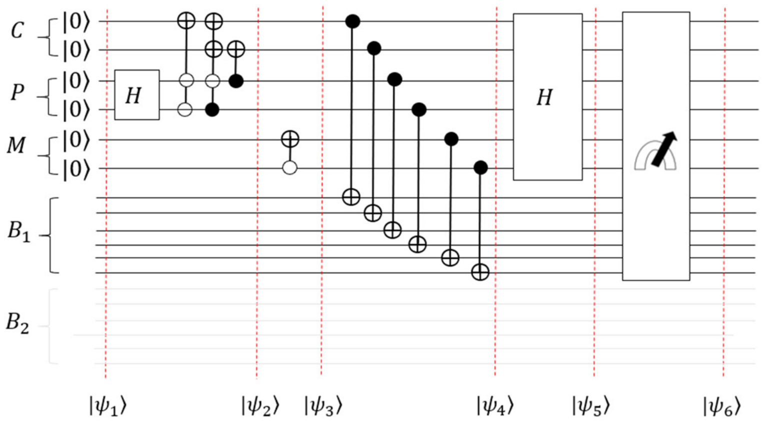


Fig. 6 An example of the sender's quantum circuit

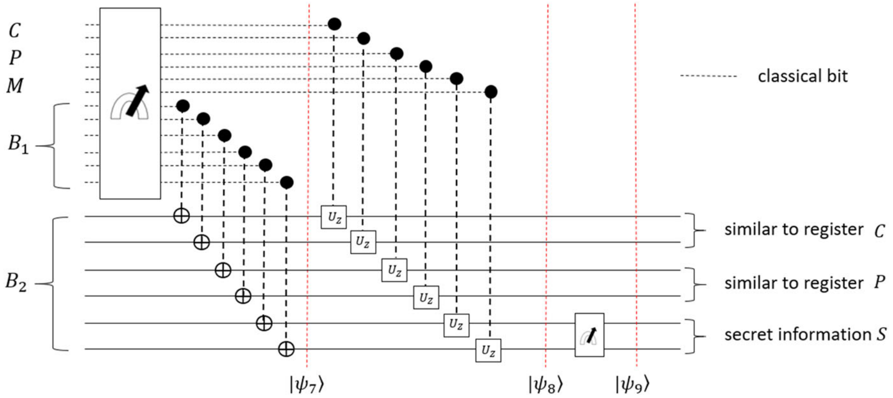


Fig. 7 An example of the recipient's quantum circuit

to obtain secret information. To be sure that the third party is completely decoupled from data of the sender and the recipient, the sender and the recipient must share a maximally entangled state, which can be proven by local measurements and public discussion alone [27]. To prove the presence of entanglement in a quantum state that is effectively distributed between the sender and the recipient, the class of entanglement witness operators is used [26, 28]. However, not all entanglement witness operators are useful for the purpose of teleportation. Teleportation witness operators are presented [29, 30]. Therefore, the sender and the recipient must verify the general Bell state $\frac{1}{\sqrt{2^{2n+q+m}}}\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}|j\rangle_{B_2}$ before using it. In our method, the third party must construct r general Bell states $\frac{1}{\sqrt{2^{2n+q+m}}}\sum_{j=0}^{2^{2n+q+m}-1}|j\rangle_{B_1}|j\rangle_{B_2}$ and distribute them to the sender and the recipient. The sender and the recipient then randomly select $r-1$ general Bell states to see if these general Bell states are verified with the use of teleportation witness operators [29, 30]. Once $r-1$ general Bell states are verified,

```
# Quantum information hiding algorithm for example#
  using LinearAlgebra
# Input: the 2^n*2^n classical image, the q-bit color information, the m-bit secret information #
  n=1; q=2;m=2; t=2*n+q+m
#Construct Bell state #
  B=zeros(2^(2*t),1)
  for i=0:(2^t-1)
     B[i*2^t+i+1,1]=1
  end
  MF=zeros(2^t,1);MF[1,1]=1;MI=kron(MF,B)  #initial state#
  H=[1 1;1 -1];X=[0 1;1 0];Z=[1 0;0 -1];One=[0 0;0 1];Zero=[1 0;0 0]
#Construct a quantum image #
  H2= kron(H,H)/2
  D1=kron(Matrix(I, 2^q,2^q),H2)
  D1=(kron(X,Matrix(I,2,2),Zero,Zero)-kron(Matrix(I,2,2),Matrix(I,2,2),Zero,Zero)+Matrix(I,2^4,2^4))*D1
  D1 = (kron(X,X,Zero,One)-kron(Matrix(I,2,2),Matrix(I,2,2),Zero,One)+Matrix(I,2^4,2^4))*D1
  D1 = (kron(Matrix(I,2,2),X,One,Matrix(I,2,2))-kron(Matrix(I,4,4),One,Matrix(I,2,2))+Matrix(I,2^4,2^4))*D1
  I1=1.0*Matrix(I,2^(2*t-4),2^(2*t-4));D2=kron(D1,I1)
#Hide the secret information “10” #
  C1=kron(X,Zero)+kron(Matrix(I,2,2),One)
  D2=kron(Matrix(I,2^4,2^4),C1,Matrix(I, 2^(2*t-6),2^(2*t-6)))*D2
#Use the quantum teleportation scheme #
  C2=Matrix(I,2^(t+1),2^(t+1))- kron(One,Matrix(I,2^(t-1),2^(t-1)), Matrix(I,2,2))+ kron(One,Matrix(I,2^(t-1),2^(t-1)),X)
  D3=kron(C2,Matrix(I,2^(t-1),2^(t-1)))*D2
  for i=1:(t-2) D3=kron(Matrix(I, 2^i,2^i),C2,Matrix(I, 2^(t-1-i),2^(t-1-i)))*D3 end
  D3=kron(Matrix(I, 2^(t-1),2^(t-1)),C2)*D3
  H6= kron(H,H,H,H,H,H)/8;C3=kron(H6,Matrix(I, 2^6,2^6))
  D3=C3*D3
#the meansurement stage : assume the measured value  k="010101” and  l=”110011"#
  MS=kron(Zero,One,Zero,One,Zero,One,One,One,Zero,Zero,One,One)
  D3=MS*D3
# the following steps are requires due to lack of memory #
  NN = zeros(2^(3*t),1)
  I2=1.0*Matrix(I,2^t,2^t)
            for i=1: 2^(2*t)
                 for j=1: 2^t
                         temp=MI[(i-1)*(2^t)+j,1]
                         if temp !=0
                               NN = kron(D3[:,i],I2[:,j])*temp + NN
                         end
                 end
            end
  MI=NN
#the meansurement stage for k="010101” and  l=”110011"#
temp=0
  for i=1:2^(3*t)
      if (MI[i,1]!=0) temp+=MI[i,1]^2 end
  end
  temp= temp^0.5
  for i=1:2^(3*t)
      if (MI[i,1]!=0) MI[i,1]=MI[i,1]/temp end
  end

# Quantum information extracting algorithm for example#
  MO=zeros(2^t,1);temp=0
  for i=1:2^(3*t)
      if (MI[i,1]!=0) temp+=1; MO[parse(Int,bitstring(Int32(i-1))[27:end],base=2)+1,1]=MI[i,1] end
  end
# Contruct matrix accoding to measured values k="010101” and  l=”110011"#
  E1=kron(X,X,Matrix(I,2,2),Matrix(I,2,2),X,X)
  E1=kron(Matrix(I,2,2),Z,Matrix(I,2,2),Z,Matrix(I,2,2),Z)*E1
  MO=E1*MO
#Extract quantum image and secret information #
  println("quantum image:");S=""
  for i=1:2^t
        if (MO[i,1]!=0) print("+",MO[i,1]," |",bitstring(Int8(i-1))[3:end-m],"> ");S=bitstring(Int8(i-1))[end-m+1:end] end
  end
  println("");println("secret information:");println(S)
```

Fig. 8 Simulation of our example in Julia language

Table 1 Comparison of LSQb method, the block LSB method, and our method

Aspects	Methods		
	LSQb method	The block LSB method	Our method
Computational complexity	$O(2^{2n}qn)$	$O(2^{2n}qn)$	$O(2^{2n}qn)$
Capacity	2^{2n}	$2^{2n-p_1-p_2}$ [21]	m
Key size	0	0	$4n+2q+2m$
The third party	No	No	Yes
The number of extracted bits after measurement	*1*	*1*	m

the sender and the recipient will perform our method by using the remaining general Bell state.

Table 1 gives a comparison of LSQb method, the block LSB method and our method in computational complexity, capacity, key size, the third party, and the number of extracted bits.

To analyze the computational complexity of our method, we assume that all one qubit gates and all controlled-V gates are elementary operations [1, 31]. At first, we consider the cost of constructing the $2^n \times 2^n$ NEQR image. In Step 2 of Algorithm 1, we need $2n$ Hadamard gates and a quantum operation $U_P = \prod_{i=0}^{2^{2n}-1} V_i$. Because $V_i($ $|0\rangle_C \otimes |i\rangle_P) = |c_i\rangle_C \otimes |i\rangle_P$, one V_i operation requires q $(2n+1)$-qubit Toffoli gates. We know that one $(2n+1)$-qubit Toffoli gate is implemented by 32 $\times(2n)$- 120 elementary operations and one garbage bit which is passed unchanged [32]. Therefore, we need $(2n+2^{2n}q(64n - 120))$ elementary operations to construct the $2^n \times 2^n$ NEQR image. In Step 3 of Algorithm 1, we only need m *CNOT* gates to perform the operation U_s. Step 4 requires $(2n + q + m)$ *CNOT* gates to perform the operation U_B. In Step 5 of Algorithm 1, we need $(2n + q + m)$ Hadamard gates. Assuming that $m < (2n + q)$, Algorithm 1 requires $O\left(2^{2n}qn\right)$ elementary operations. Similarly, in Algorithm 2, Step 1 needs $(2n + q + m)$ *CNOT* gates and Step 2 needs $(2n + q + m)$ $U_z^{k_t}$ gates. Thus, Algorithm 2 requires $O(n + q + m)$ elementary operations. Thus, our method requires $O\left(2^{2n}qn\right)$ elementary operations. In LSQb method and the block LSB method, the NEQR image must be constructed. These two methods also require $O\left(2^{2n}qn\right)$ elementary operations.

Next, we compare the hiding capacity of our method with that of LSQb method. Our method hides m secret bits which is independent of the size of the quantum image. LSQb method can hide 2^n secret bits which depend on the size of the quantum image. According to our assumption $m < (2n + q)$, LSQb method has higher hiding capacity. However, LSQb method only gets one secret bit with just one measurement. If one wants to get another secret bit, he/she must execute LSQb method again. After measurement, he/she can get another secret bit with the probability $\left(1 - 2^{-n}\right)$. Therefore, one can get m secret bits with the probability $\prod_{i=1}^{m-1}\left(1 - \frac{i}{2^n}\right)$ if he/she executes LSQb method m times. It is worthy of noting that the quantum image collapses after measurement. In our method, we will extract m secret bits and a quantum image after measurement with certainty. However, our method must transfer $(4n + 2q + 2m)$ bits by the classical channel.

6 Conclusion

This paper has proposed a novel information hiding method based on the NEQR quantum image by using the quantum teleportation scheme. In the proposed method, the recipient not only gets the secret information, but also holds the quantum image after measurement. As compared with Wang et al.'s method which hides secret information in the least significant qubit (LSQb), our method will not collapse the quantum image and decrease the computed cost of extracting one secret bit by $O(m)$ times.

References

1. Nielson, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, 10th Anniversary edition published, Cambridge (2010)
2. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on Foundations Computer Science, pp. 124–134 (1994)
3. Grove, L.K.: Quantum computers can search arbitrarily large databases by a single query. Phys. Rev. Lett. **79**(23), 4709–4712 (1997)
4. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120–126 (1978)
5. Liu, L., Tang, G.M., Sun, Y.F., Yan, S.F.: Quantum steganography for multi-party covert communication. Int. J. Theory Phys. **55**, 191–201 (2016)
6. DiVincenzo, D.P., Leung, D.W., Terhal, B.M.: Quantum data hiding. IEEE Trans. Inf. Theory **48**(3), 1–19 (2001)
7. Terhal, B.M., DiVincenzo, D.P., Leung, D.W.: Hiding bits in Bell states. Phys. Rev. Lett. **86**(25), 5807–5810 (2001)
8. Banacloche, J.G.: Hiding messages in quantum data. J. Math. Phys. **43**(9), 4531–4536 (2002)
9. Mogos, G.: A quantum way to data hiding. Int. J. Multimed. Ubiquitous Eng. **4**(2), 13–20 (2009)
10. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**(P1), 7–11 (2014)
11. Yan, F., Iliyasu, A.M., Venegas-Andraca, S.E.: A survey of quantum image representations. Quantum Inf. Process. **15**(1), 1–35 (2016)
12. Yan, F., Iliyasu, A.M., Le, P.Q.: Quantum image processing: a review of advances in its security technologies. Int. J. Quantum Inf. **15**(3), 1730001 (2017)
13. Hua, T., Chen, J., Pei, D., Zhang, W., Zhou, N.: Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theor. Phys. **54**(2), 526–537 (2015)
14. Zhou, N.R., Hua, T.X., Gong, L.H., Pei, D.J., Liao, Q.H.: Quantum image encryption based on generalized Arnold transform and double random phase encoding. Quantum Inf. Process. **14**(4), 1193–1213 (2015)
15. Zhou, N., Hu, Y., Gong, L., Li, G.: Quantum image encryption scheme with iterative generalized Arnold transform and quantum image cycle shift operations. Quantum Inf. Process. **16**(6), 164 (2017)
16. Zhou, N., Chen, W., Yan, X., Wang, Y.: Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf. Process. **17**(6), 137 (2018)
17. Zhou, N., Yan, X., Liang, H., Tao, X., Li, G.: Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. Quantum Inf. Process. **17**(12), 338 (2018)
18. 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)
19. 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)

20. van Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A digital watermark. Int. Conf. Image Proc. **2**, 86–90 (1994)
21. Jiang, N., Zhao, N., Wang, L.: LSB based quantum image steganography algorithm. Int. J. Theory Phys. **55**(1), 107–123 (2016)
22. Le, P., Dong, F., Hitora, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**(1), 63–84 (2011)
23. 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)
24. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895–1899 (1993)
25. Sang, J.Z., Wang, S., Li, Q.: Least significant qubit algorithm for quantum images. Quantum Inf. Process. **15**(11), 4441–4460 (2016)
26. Curty, M., Lewenstein, M., Lütkenhaus, N.: Entanglement as a precondition for secure quantum key distribution. Phys. Rev. Lett. **92**(21), 217903 (2004)
27. Curty, M., Guehne, O., Lewenstein, M., Luetkenhaus, N.: Detecting quantum correlations for quantum key distribution. In: Proceedings of Conference on Quantum Optics and Applications in Computing and Communications II, International Society for Optics and Photonics, vol. 5631, pp. 9–20 (2005)
28. Curty, M., Gühne, O., Lewenstein, M., Lütkenhaus, N.: Detecting two-party quantum correlations in quantum-key-distribution protocols. Phys. Rev. A **71**(2), 022306 (2005)
29. Ganguly, N., Adhikari, S., Majumdar, A.S., Chatterjee, J.: Entanglement witness operator for quantum teleportation. Phys. Rev. Lett. **107**(27), 270501 (2011)
30. Zhao, M.-J., Chen, B., Fei, S.-M.: Detection of the ideal resource for multiqubit teleportation. Chin. Phys. B **24**(7), 070302 (2015)
31. Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J., Weinfurter, H.: Elementary gates for quantum computation. Phys. Rev. A **52**(5), 3457–3487 (1995)
32. Maslov, D., Dueck, G.W.: Improved quantum cost for n-bit Toffoli gates. Electron. Lett. **39**(25), 1790–1791 (2003)