Quantum Inf Process (2017) 16:212
DOI 10.1007/s11128-017-1640-9

Quantum watermarking scheme through Arnold scrambling and LSB steganography

Ri-Gui Zhou[1] · Wenwen Hu[2] · Ping Fan[2]

Received: 14 January 2017 / Accepted: 12 June 2017 / Published online: 20 July 2017

Abstract Based on the NEQR of quantum images, a new quantum gray-scale image watermarking scheme is proposed through Arnold scrambling and least significant bit (LSB) steganography. The sizes of the carrier image and the watermark image are assumed to be $2n \times 2n$ and $n \times n$, respectively. Firstly, a classical $n \times n$ sized watermark image with 8-bit gray scale is expanded to a $2n \times 2n$ sized image with 2-bit gray scale. Secondly, through the module of PA-MOD N, the expanded watermark image is scrambled to a meaningless image by the Arnold transform. Then, the expanded scrambled image is embedded into the carrier image by the steganography method of LSB. Finally, the time complexity analysis is given. The simulation experiment results show that our quantum circuit has lower time complexity, and the proposed watermarking scheme is superior to others.

Keywords Quantum watermarking · Arnold scramble · Least significant bit · Quantum circuit

1 Introduction

Images are an important medium in visual information transmission. Image processing becomes more popular because of the need to extract visual information from the natural world. Due to the rapid development of quantum computation and quantum information in the past several decades, quantum computer has demonstrated a bright

✉ Ping Fan
fp_ecjtu@126.com

[1] College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China

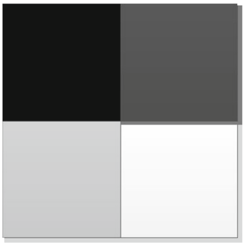
[2] School of Information Engineering, East China Jiaotong University, Nanchang 330013, Jiangxi, China

prospect over classic computer, particularly in Feynman's computation model [1], Deutsch's quantum parallelism assertion [2], Shor's integer factoring algorithm [3], and Grover's database searching algorithm [4].

Quantum image processing (QIMP), a new emerging sub-discipline of information and image processing, is devoted to utilizing the quantum computing technologies to capture, manipulate, and recover quantum image in different formats for different purposes. The investigation of QIMP is beginning with how to store and retrieve a quantum image in quantum computers. Venegas-Andraca and Bose proposed the quantum image representation of qubit lattice [5] in 2003 using one qubit to hold one pixel. Then, Latorre's Real Ket presented a way to store image information using quantum superposition state [6]. More recently, in 2010, Le et al. [7] proposed a flexible representation of quantum image (FRQI), which integrates the information of colors and the corresponding positions in an image into an entanglement state and captures the positions information into a normalized superposition quantum state. It encodes the color information of an image into angle θ using 1 qubit and uses the two-dimensional position information (Y-axis and X-axis). Further, in 2013, more quantum image representations were proposed. A novel enhanced quantum image representation (NEQR) of digital images [8] improves the color information representation of FRQI from 1 qubit to q qubits encoding the pixel value from 0 to $2^q - 1$, which makes the complex and elaborates color operations perform easier than FRQI does. QUALPI [9] stores images sampled in log-polar coordinates. Color image representation utilizes two sets of quantum states for M colors and N coordinates, respectively (QSMC and QSNC) [10]. Multi-dimensional image representation uses a normal arbitrary quantum superposition state (NAQSS) [11] and simple quantum representation of infrared images (SQR) [12]. A novel quantum representation of color digital images was proposed [13] in 2016.

In the literature [14,15], the QIMP is broadly classified into two groups: quantum-inspired image processing and classical-inspired image processing [16,17]. The quantum-inspired image processing aims to exploit some of the properties responsible for the potency of quantum computing to improve some well-known classical or digital (i.e., conventional or non-quantum) image processing. The classical-inspired image processing derives inspiration from the expectation that quantum computing hardware will soon be physically realized. Hence, such research focuses on extending classical image processing to the quantum computing framework. Some of the available literatures that fall under this direction include geometric transformations [18–20], color transformation [21], quantum image translation [22–24], quantum image scaling [25–27], image scrambling [28–32], image segmentation [33], feature extraction [34], edge detection [35], and image matching [36].

Quantum image protection devotes to protecting images from unauthorized use, copying, and manipulation when images are used for commercial purpose. It has been a very important theme for experts and researchers and mainly divided into two categories: quantum image cryptography and quantum image watermarking. The image cryptography is to transform a meaningful image into a meaningless (or disorder) form, while the image watermarking is to hide image information by embedding it into some other images. The quantum image scrambling realizes image cryptography in [29–32]. The quantum Arnold and Fibonacci image scrambling algorithms [28] and



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

Fig. 1 An example of 2 × 2 image and its NEQR

quantum Hilbert image scrambling algorithm [30] were proposed by Jiang et al; Several quantum watermarking schemes have been proposed in [37–41] using complex quantum circuits such as QFT [37], QWT [38], and Hadamard transform [39], and some other schemes were proposed, for example, a quantum watermarking scheme using simple and small-scale quantum circuits [40] and a novel LSB-based quantum watermarking [41].

This paper is organized as follows. Section 2 briefly introduces the quantum representation of NEQR, classical LSB steganography, Arnold transformation, the parallel adder, subtractor modulo N, and quantum equal. Section 3 presents the quantum watermarking scheme. Section 4 analyzes the time complexity of circuits and the experimental results. The conclusions are drawn in Sect. 5.

2 Preliminaries

2.1 Novel enhanced quantum image representation (NEQR) of digital image

Comparing to FRQI, the NEQR has improved the gray-scale value representation from 1 qubit to q qubits, which makes more image operations can be performed conveniently [8]. A gray-scale image $f(Y, X)$ with $2^n \times 2^n$ pixels is expressed in Eq. (1) based on NEQR. Figure 1 shows an example of an image of 2 × 2, and the corresponding NEQR is on the right of the image.

$$
|\mathrm{I}\rangle = \frac{1}{2^{\mathrm{n}}}\sum_{i=0}^{2^{2n}-1}|C_i\rangle\otimes|i\rangle = \frac{1}{2^{\mathrm{n}}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{k=0}^{q-1}\left|C_{YX}^{k}\right\rangle\otimes|Y\rangle\,|X\rangle \tag{1}
$$

where

$$
|C_i\rangle = \left|C_i^{q-1}\ldots C_i^1 C_i^0\right\rangle
$$

2.2 The classic LSB scheme

Steganography is a branch of information hiding which hides a message into a cover. It is a kind of subliminal channel that provides secret communication so that the intended hacker or attacker is unable to detect the presence of the message. The LSB

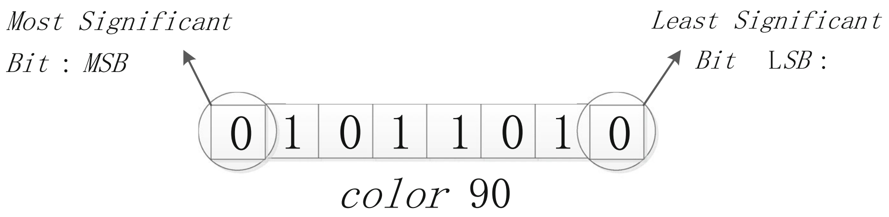


Fig. 2 Least significant bit

steganography, first proposed by Tirkel [42] in 1993, is a fundamental and simple data hiding method. The principle is using message bits to substitute the least significant bits of the cover. In general, the cover is a 24-bit or 8-bit image. Taking the latter, for example, it has $2^8 = 256$ colors (or gray scales). The least significant bit of one of the pixels is shown in Fig. 2. The message bit is "1"; then, we only need to change the least significant bit from "0" to"1," i.e., color 90 should be changed to color 91. The receiver can get the message by simply reading the least significant bit.

2.3 Arnold scramble method

The Arnold transform or Arnold's cat map was set up during the research of ergodic theory by Arnold [43]. Dyson et al. quoted the Arnold transform as an image scrambling method in 1992 [44]. Since then, it has been widely used in image processing.

2.3.1 The principle of Arnold scramble

Supposing that $I(x, y)$ is an original image with size $2^n \times 2^n$, (X, Y) and (X_A, Y_A) are the pixel coordinates of the original image and the scrambled image, respectively. Two-dimensional Arnold scrambling proceed is written by Eq. (2), and its inverse operation is shown in Eq. (3).

$$\begin{bmatrix} X_A \\ Y_A \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 2^n \tag{2}$$

where

$$X_A = (X + Y) \bmod 2^n \text{ , } Y_A = (X + 2Y) \bmod 2^n$$

The inverse Arnold transformation is

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} X_A \\ Y_A \end{bmatrix} \bmod 2^n = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} X_A \\ Y_A \end{bmatrix} \bmod 2^n, \tag{3}$$

i.e.,

$$X = (2X_A - Y_A) \bmod 2^n \text{ , } Y = (Y_A - X_A) \bmod 2^n$$

Table 1 Period of Arnold transform

Size of image	4	8	16	32	64	128	256	512
Arnold period	3	6	12	24	48	96	192	384

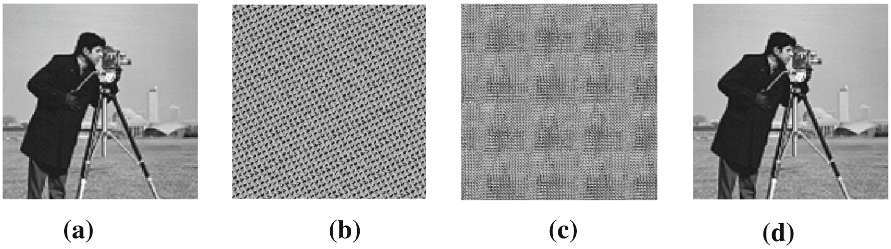


Fig. 3 Result of Arnold transformation after the specific iteration times. **a** Original image, **b** 12 times, **c** 48 times, **d** 192 times

2.3.2 The safety analysis of Arnold scrambling in quantum watermarking

Arnold transform is not a "pure" two-dimensional affine transformation because it has a "mod" operator. It can be seen as a process of cutting and splicing. Using Arnold scrambling, an original quantum image transforms into a disordered or meaningless quantum image. Besides, as an image preprocessing technology, it can reduce the distribution of scattered error bits of a quantum watermarked image to improve the robustness.

The Arnold scrambling algorithm is simple and cyclical, i.e., if repeating Arnold transform in certain iteration steps, it will surely resume the image. Based on Eq. (2), the iteration equation of Arnold transform is shown in Eq. (4). In [44], Dyson researched the period. Generally speaking, the explicit value of the period cannot be calculated. He gave the upper bound and the lower bound of the period and gave explicit values for particular cases as shown in Table 1. We can see that the period is connected with the image size N from Table 1.

$$\begin{cases} I^1 = \begin{bmatrix} X_A \\ Y_A \end{bmatrix}, \ A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, I^0 = \begin{bmatrix} X \\ Y \end{bmatrix} \\ I^1 = AI^0 \bmod 2^n \\ I^n = AI^{n-1} \bmod 2^n \ , n = 0, 1, 2, \ldots \end{cases} \tag{4}$$

Figure 3 shows the scrambling results and corresponding period of a real image. The size of the original image named "cameraman" is 256 × 256. (b)–(d) is the Arnold transformation, the sub-captions of which are the iteration times. For more comprehensive and state-of-the-art surveys of this topic, refer to paper [43,44].

2.4 Parallel adder and subtractor modulo N

Islam M S et al. proposed the reversible full adder based on Peres gate (PG) in [45]. Here, the introductions about the design of half adder, full adder, and parallel adder are

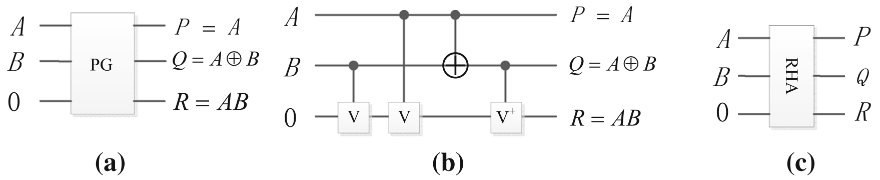


Fig. 4 Reversible half adder (RHA). **a** PG gate working as half adder, **b** quantum circuit implement of half adder, **c** simplified diagram of RHA

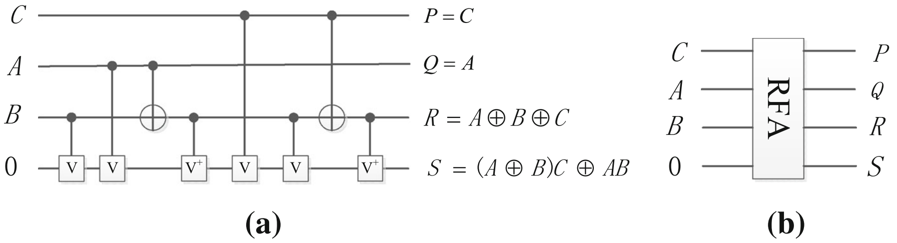


Fig. 5 Reversible full adder (RFA). **a** quantum implement of the reverse full adder, **b** simplified diagram of RFA

given. Then, the module of parallel adder modulo N (PA-MOD) and parallel subtractor modulo N (PS-MOD) are designed.

2.4.1 Reversible half adder (RHA)

Figure 4a shows the Peres Gate working as a half adder and its quantum circuit, where $Q = A \oplus B$ represents the sum of $A + B$ and $R = AB$ represents the carry of $A + B$. Figure 4b, c are the quantum circuit realization of RHA and corresponding diagram of RHA, respectively.

Where $V$is a square root of NOT gate defined by

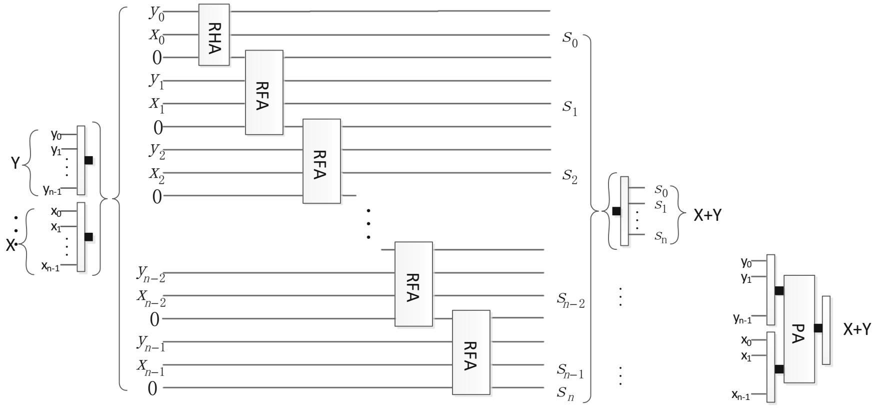
$$\mathrm{V} = \frac{i+1}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

V^{+} is the Hermitian matrix of V. V and V^{+} have the following properties:

$$V \times V = V^{+} \times V^{+} = NOT$$
$$V \times V^{+} = V^{+} \times V = I$$

2.4.2 Reversible full adder (RFA)

Based on the PG gates, we design the full adder as shown in Fig. 5, where $R = A \oplus B \oplus C$ represents the sum of $(A + \mathrm{B} + \mathrm{C})$ and $S = (A \oplus B)C \oplus AB$ represents the carry, respectively. The quantum circuit realization of RFA is shown in Fig. 5a, and its simplified graph is shown in Fig. 5b.



(a) (b)

Fig. 6 Reversible parallel adder. **a** Reverse parallel adder (PA), **b** block diagram of PA

2.4.3 Reversible parallel adder (PA)

The reversible parallel adder adds an n qubits Y from an n qubits X designed by one reversible half adder (RHA) and $(n-1)$ reversible full adders (RFA) as shown in Fig. 6a. Here, $S_nS_{n-1}\ldots S_1S_0$ represents the sum of $X+Y$. Other unremarked qubits are the garbage output, and the constant input qubit 0 is the ancillary qubit. For convenience, the block diagram of PA omits the ancillary inputs and the garbage outputs as shown in Fig. 6b.

2.4.4 Parallel adder modulo N (PA-MOD)

As shown in Fig. 7, X and Y are two n-bit binary numbers. Assuming that $N=2^n$, it is easy to find that $X+Y$ is a $(n+1)$-bit binary numbers $S_nS_{n-1}\ldots S_1S_0$ as shown in Fig. 6a. According to the mathematical proof of theorem 1 in [29], the result of $(X+Y)$ mod N is $S_{n-1}\ldots S_1S_0$, which just omits the highest-order bit of S_n. Figure 7a, b give the quantum circuit realization of PA-MOD and corresponding diagram of PA-MOD, respectively.

2.4.5 Parallel subtractor modulo N (PS-MOD)

The subtraction operation can be converted into complement addition to achieve addition and subtraction operations of the binary bit. Supposing that we need to calculate the difference between the two binary numbers X and Y, where $Y=y_{n-1}y_{n-2}\ldots y_0$ and $X=x_{n-1}x_{n-2}\ldots x_0$, then we can derive

$$\begin{aligned}&(Y-X) \mod 2^n\\&\quad=[Y+(-X)] \mod 2^n\\&\quad=[Y+(\bar{X}+1)] \mod 2^n\\&\quad=(y_{n-1}y_{n-2}\ldots y_0+\bar{x}_{n-1}\bar{x}_{n-2}\ldots\bar{x}_0+1) \mod 2^n\end{aligned} \tag{5}$$

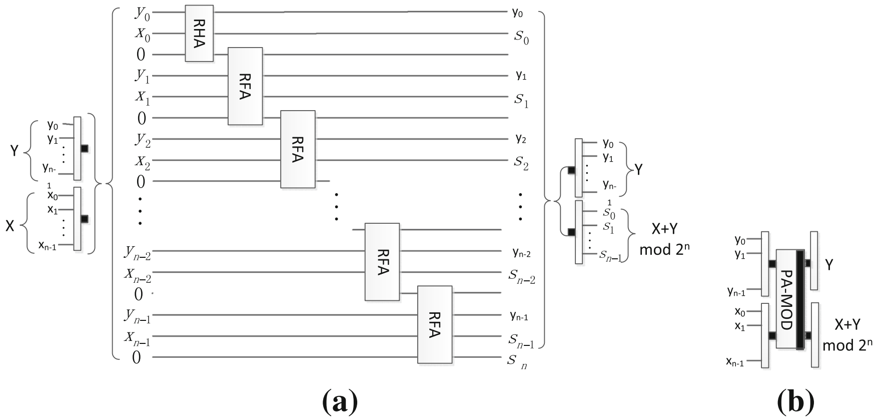


Fig. 7 Parallel adder modulo N. **a** Parallel adder modulo N (PA-MOD), **b** diagram of PA-MOD N

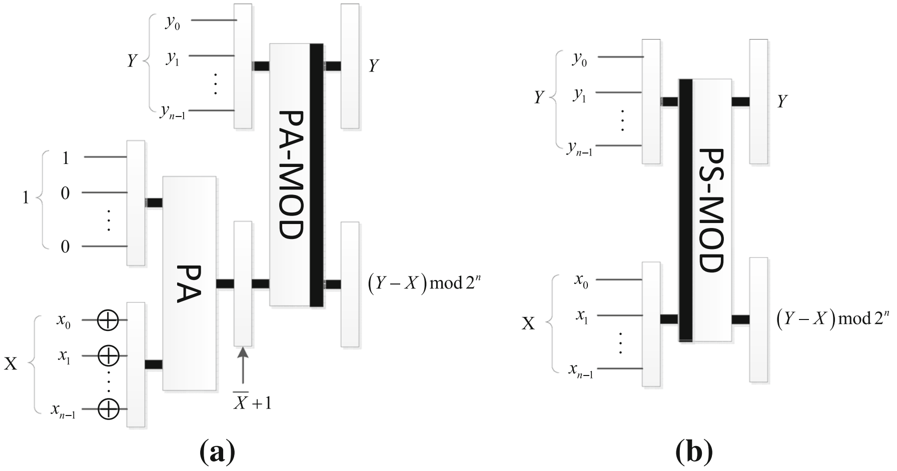
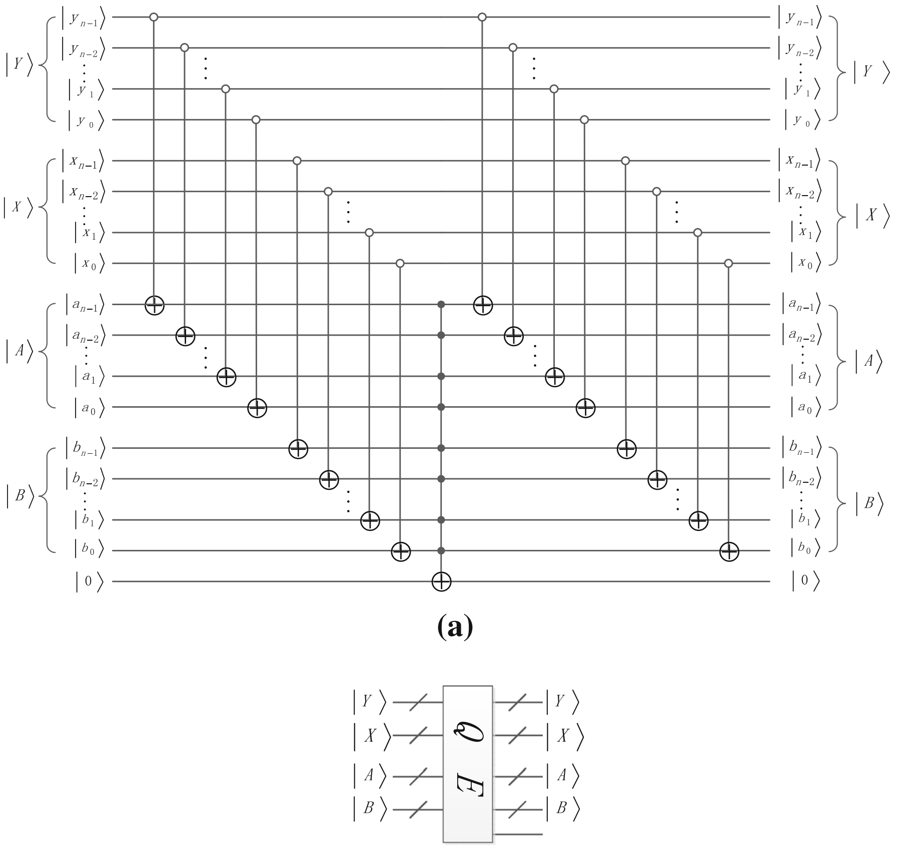


Fig. 8 Parallel subtractor modulo N. **a** Parallel subtract modulo N (PA-MOD), and **b** diagram of PS-MOD N

According to Eq. (5), the construction of PS-MOD is shown in Fig. 8a. The module diagram of PS-MOD is shown in Fig. 8b where the ancillary inputs and the garbage outputs are omitted.

2.5 Quantum equal (QE)

The quantum equal compares two numbers $|YX\rangle = |Y\rangle\,|X\rangle$ and $|AB\rangle = |A\rangle\,|B\rangle$ to find out whether they are equal or not, where $|Y\rangle = |y_{n-1}\ldots y_1 y_0\rangle\,, |X\rangle = |X_{n-1}\ldots X_1 X_0\rangle\,, |A\rangle = |a_{n-1}\ldots a_1 a_0\rangle\,, |B\rangle = |b_{n-1}\ldots b_1 b_0\rangle$ .Therein, $x_i, y_i, a_i, b_i \in \{0,\ 1\},\ i = n-1, \ldots 1$. The output qubit$|c\rangle$ represents the comparative result. If $|c\rangle = |1\rangle\,, |YX\rangle = |AB\rangle$; otherwise, $|YX\rangle \neq |AB\rangle$. The quantum circuit of QE and its diagram are shown in Fig. 9.



(a)

(b)

Fig. 9 Quantum equal (QE) circuit realization and its diagram. **a** Circuit of quantum equal (QE), **b** diagram of QE

3 The proposed quantum watermarking scheme

In this section, a quantum watermarking scheme was proposed based on NEQR, which hides a secret gray-scale image (watermark) into a gray-scale image (carrier). Assume that the size of the carrier image and the watermark image is $2^n \times 2^n$ and $2^{n-1} \times 2^{n-1}$, respectively.

In order to explain the scheme, we take a small watermark (secret) image with 1×1 pixels and a small carrier image with 2×2 pixel as the example shown in Fig. 10.

3.1 Embedding procedure

Proposed embedding procedure of quantum watermarking shown in Fig. 11(a) is as follows.

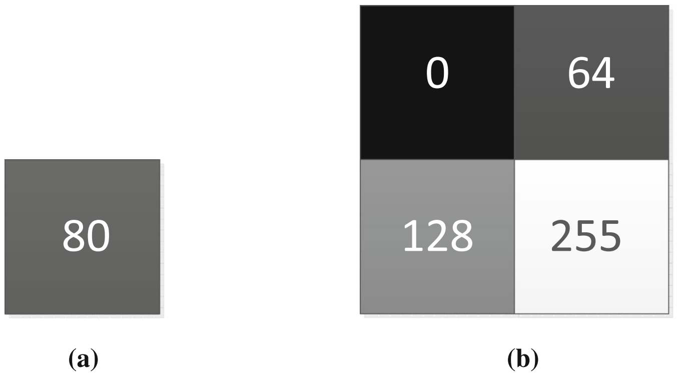


Fig. 10 Watermark image and carrier image. **a** 1 × 1 watermark image, **b** 2 × 2 carrier image

1. Transform a classical carrier image with $2^n \times 2^n$ size and 8-bit gray scale into a quantum image by the NEQR $|C\rangle$.
2. Expand a classical watermark image with $2^{n-1} \times 2^{n-1}$ size and 8-bit gray scale to an image with $2^n \times 2^n$size and 2-bit gray scale. An example is shown in Fig. 12 (where n = 1), as we can see, the 8-bit string is divided into four 2-bit strings.
3. Transform the expanded watermark image into a quantum image by the NEQR $|W\rangle$.
4. Scramble the expanded watermark image to a meaningless image $\left|W'\right\rangle$ through Arnold scrambling.
5. Embed the watermark image into the carrier image according to the embedding procedure shown in Fig. 11a to obtain watermarked image $\left|CW'\right\rangle$ and generate the extracting key image K_1, K_0.
6. Transform$\left|CW'\right\rangle$into a classical digital watermarked image through quantum measurement.

3.1.1 Quantum image preparing works

The watermark image with $2^{n-1} \times 2^{n-1}$ size and 8-bit gray scale is firstly expanded to an image with $2^n \times 2^n$ size and 2-bit gray scale; thus, a 8-bit string is divided into four 2-bit strings. Then, the expanded image is transformed into the quantum image $|W\rangle$ by the NEQR as shown in Eq. (6).

$$|W\rangle = \frac{1}{2^n} \sum_{YX=0}^{2^{2n}-1} |W_{YX}\rangle \otimes |YX\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \bigotimes_{k=0}^{1} \left|W_{YX}^k\right\rangle \otimes |YX\rangle \tag{6}$$

For example, the watermark image with 1 × 1 image size and 8-bit gray scale is expanded to the image with 2 × 2 image size as shown in Fig. 12. Since the value of gray scale 183 is expressed as $(10110111)_2$ by 8 bits, the expanded image consists of four pixels: $(10)_2$, $(11)_2$, $(01)_2$ and $(11)_2$, respectively. Then, we can obtain the NEQR as follows.

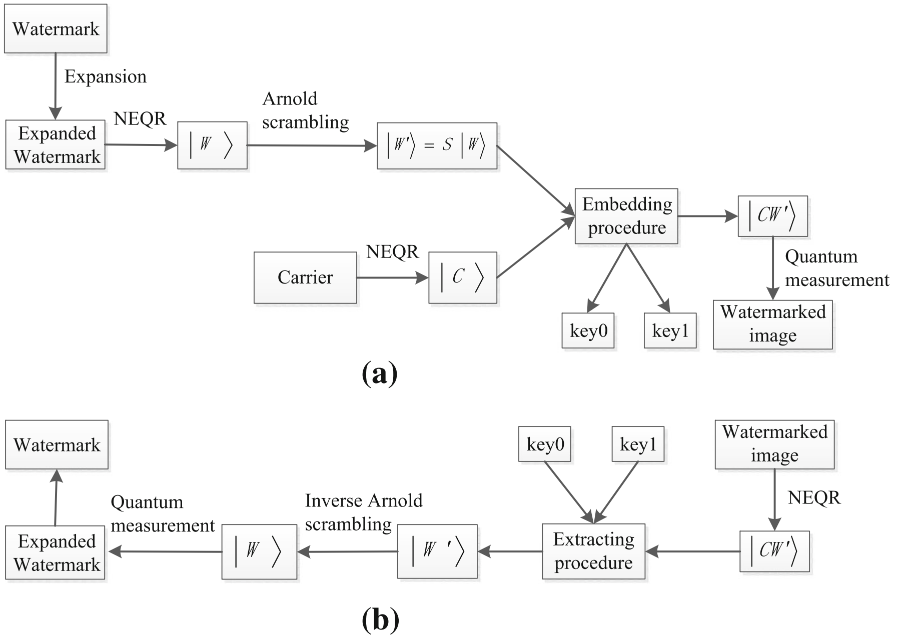


Fig. 11 Procedures of proposed quantum watermarking scheme. **a** Embedding procedure of quantum watermarking and **b** extracting procedure of quantum watermarking

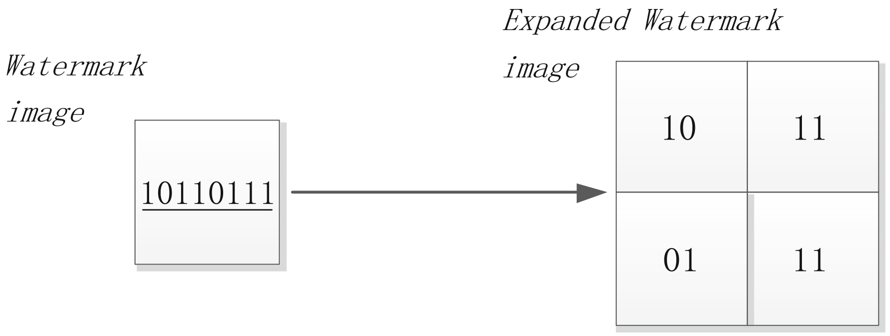


Fig. 12 An example of expanding a watermark image from 1 × 1 size into 2 × 2 size

$$|W\rangle = \frac{1}{2}\left(|10\rangle\,|00\rangle + |11\rangle\,|01\rangle + |01\rangle\,|10\rangle + |11\rangle\,|11\rangle\right)$$

Transform the carrier image into the NEQR as shown in Eq. (7).

$$|\mathrm{C}\rangle = \frac{1}{2^{\mathrm{n}}}\sum_{i=0}^{2^{2n}-1}|C_i\rangle \otimes |i\rangle = \frac{1}{2^{\mathrm{n}}}\sum_{YX=0}^{2^{2n}-1}\bigotimes_{k=0}^{q-1}\left|C_{YX}^{k}\right\rangle \otimes |YX\rangle \tag{7}$$

where

$$C_{YX} = C_{YX}^{q-1} C_{YX}^{q-2} \ldots C_{YX}^{0}.$$

The prepared quantum key image K_0 and K_1 are expressed by Eq. (8)

$$|K_1\rangle = I \otimes H^{\otimes n} \, |0\rangle^{\otimes(n+1)} = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} \left|C_i^{k1}\right\rangle \otimes |i\rangle \,, \left|C_i^{k1}\right\rangle = |0\rangle$$

$$|K_0\rangle = I \otimes H^{\otimes n} \, |0\rangle^{\otimes(n+1)} = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} \left|C_i^{k0}\right\rangle \otimes |i\rangle \,, \ \left|C_i^{k0}\right\rangle = |0\rangle \qquad (8)$$

3.1.2 Arnold scrambling

In order to enhance the confidentiality, we adopt two-step process. In the first step, a watermark with $2^{n-1} \times 2^{n-1}$ image size and 8-bit gray scale is expanded to an image with $2^n \times 2^n$ image size and 2-bit gray scale as shown in Fig. 12. In the second step, the watermark image $|W\rangle$ is scrambled into a disorder image $|W'\rangle$ through Arnold scrambling as shown in Fig. 13.

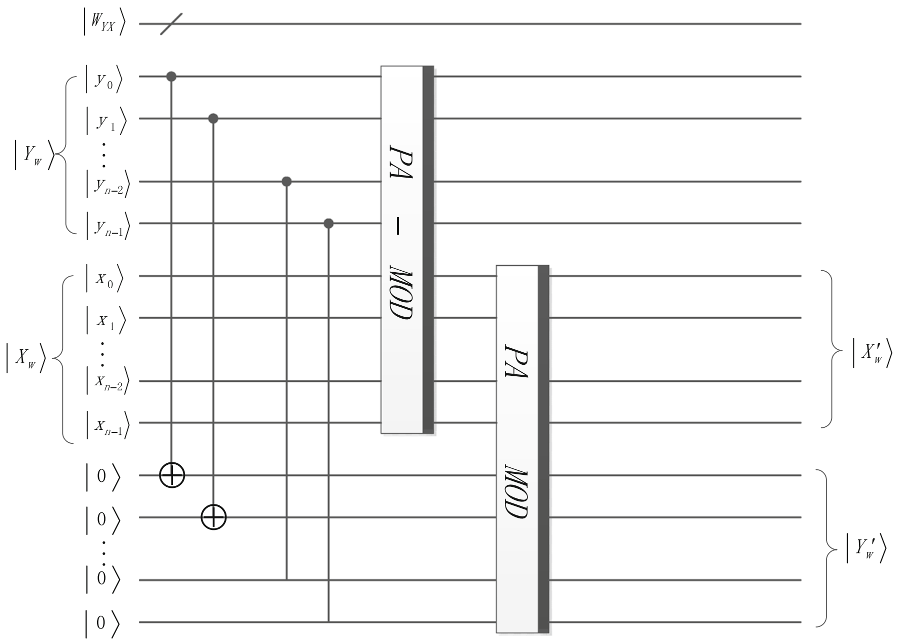


Fig. 13 Arnold scrambling of watermark image

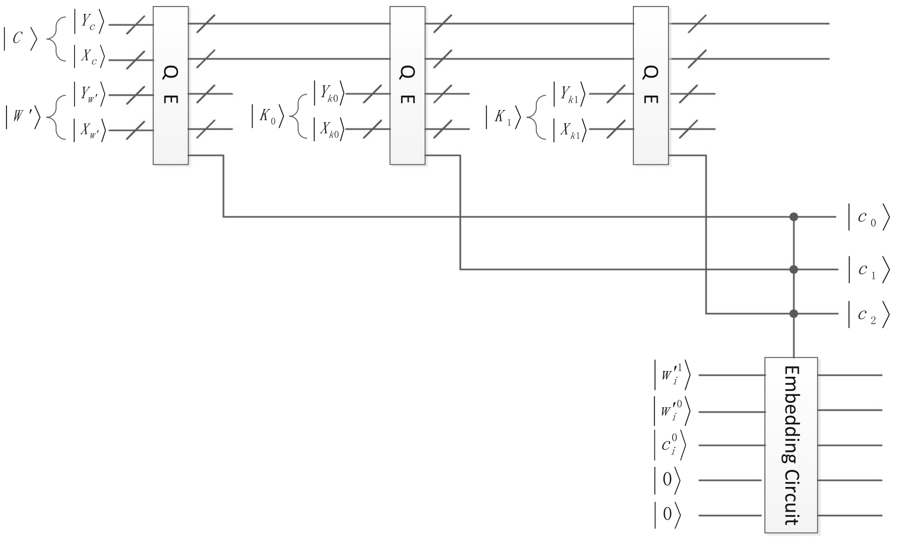
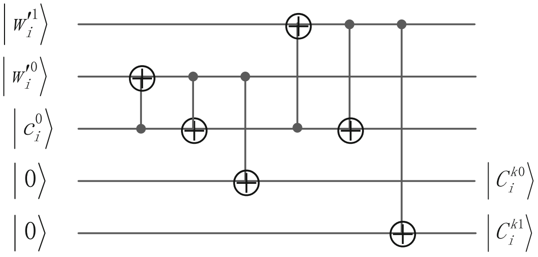


Fig. 14 Quantum watermarking embedding procedure

Fig. 15 Embedding circuit



3.1.3 Implement embedding

A scrambled watermark image $\left|W'\right\rangle$ is embedded into a carrier image $|C\rangle$ through the LSB method as shown in Fig. 14. Therein, the output qubits $|c_0\rangle$, $|c_1\rangle$ and $|c_2\rangle$ are acted as the control qubits of Embedding Circuit. As shown in Fig. 15, under the control qubits, $|W_{YX}^{'0}\rangle$ and $|W_{YX}^{'1}\rangle$ of $|W_{YX}^{'}\rangle$ are used to substitute the least significant qubit $|C_{YX}^{0}\rangle$ of $|C_{YX}\rangle$ twice. The QE module is a quantum circuit as shown in Fig. 9a. Firstly, the three QE modules are used to compare the coordinates of the carrier image $|C\rangle$, the scrambled expanded watermark image $\left|W'\right\rangle$, the two prepared key images $|K_1\rangle$, and $|K_0\rangle$.

The pixel embedding steps are as follows:

If the coordinates of all the input images are equal, the outputs $|c_0\rangle$, $|c_1\rangle$, and $|c_2\rangle$ of each QE module would be state $|1\rangle$. The qubits$|c_0\rangle$, $|c_1\rangle$, and $|c_2\rangle$ are acted as the control qubits in Fig. 15, which is implemented by the following steps:

If $\left|w_i^{'0}\right\rangle = |c_i^0\rangle \oplus \left|w_i^{'0}\right\rangle$, then $|c_i^0\rangle = \left|w_i^{'0}\right\rangle \oplus |c_i^0\rangle$, $|C_i^{k0}\rangle = \left|w_i^{'0}\right\rangle \oplus |0\rangle$. Otherwise, no change will be made.

If $\left|w_i'^1\right\rangle = |c_i^0\rangle \oplus \left|w_i'^1\right\rangle$, then $|c_i^0\rangle = \left|w_i'^1\right\rangle \oplus |c_i^0\rangle$, $|C_i^{k1}\rangle = \left|w_i'^1\right\rangle \oplus |0\rangle$. Otherwise, no changes will be made.

By doing these, the watermark image is embedded into the carrier image, and it will generate two key images $|K_1\rangle$ and $|K_0\rangle$ at the same time.

3.2 Extracting procedure

Extracting procedure shown in Fig. 11b is as follows.

1. Extract the scrambled expanded watermark image $\left|W'\right\rangle$ according to the extracting circuit, and the two extracting key images K_1, K_0 and the watermarked image$\left|CW'\right\rangle$ are needed.
2. Implement the inverse Arnold scrambling $\left|W'\right\rangle$ to get the expanded watermark image $|W\rangle$.
3. Measure the expanded watermark quantum image$|W\rangle$to get the corresponding classic image, and further implement the inverse expanded transformation to get the watermark image.

3.2.1 Implement extracting

A scrambled watermark image $\left|W'\right\rangle$ is extracted from the carrier image $|C\rangle$ through the LSB method as shown in Fig. 16. Therein, the output qubits $|c_0\rangle$ and $|c_1\rangle$ are acted

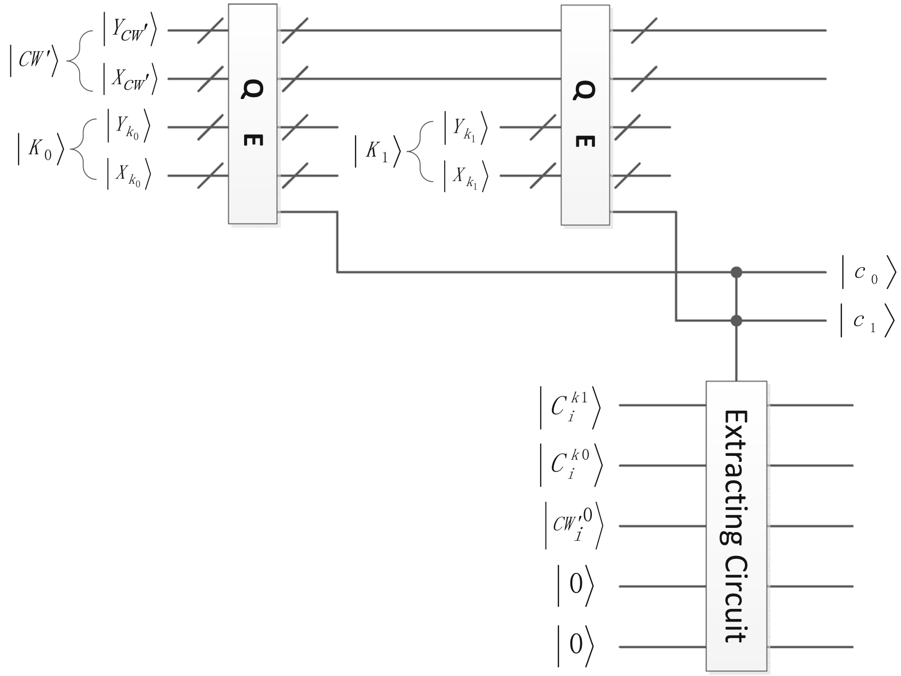
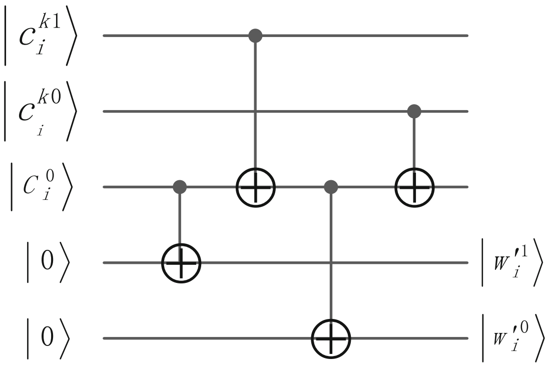


Fig. 16 Quantum watermarking extracting procedure

Fig. 17 Extracting circuit


$\left|C_i^{k1}\right\rangle$
$\left|C_i^{k0}\right\rangle$
$\left|C_i^{0}\right\rangle$
$\left|0\right\rangle$
$\left|0\right\rangle$
$\left|W_i'^{1}\right\rangle$
$\left|W_i'^{0}\right\rangle$

as the control qubits of Extracting Circuit. As shown in Fig. 17, under the control qubits, $\left|C_i^{k0}\right\rangle$ and $\left|C_i^{k1}\right\rangle$ of $\left|c_i^{0}\right\rangle$ are used to retrieve the pixel qubits $\left|W_{YX}'^{1}\right\rangle$ and $\left|W_{YX}'^{0}\right\rangle$. The two QE modules are used to compare the coordinates of the watermarked image $\left|CW'\right\rangle$, and the two key images $|K_1\rangle$, $|K_0\rangle$.

The pixel extracting steps are as follows:

If the coordinates of all the input images are equal, the outputs $|c_0\rangle$ and $|c_1\rangle$ of each QE module would be state $|1\rangle$. Then qubits $|c_0\rangle$ and $|c_1\rangle$ are acted as the control qubits in Fig. 17, which is implemented by the following steps:

$$\left|w_i'^{1}\right\rangle = \left|c_i^{0}\right\rangle \oplus |0\rangle\,,\ \left|c_i^{0}\right\rangle = \left|C_i^{k1}\right\rangle \oplus \left|c_i^{0}\right\rangle,\ \left|w_i'^{0}\right\rangle = \left|c_i^{0}\right\rangle \oplus |0\rangle\ and\ \left|c_i^{0}\right\rangle = \left|C_i^{k0}\right\rangle \oplus \left|c_i^{0}\right\rangle.$$

By doing these, the scrambled expanded watermark image $\left|W'\right\rangle$ is extracted from the carrier image, and the carrier image $|C\rangle$ is retrieved at the same time.

3.2.2 Inverse Arnold scrambling

As shown in Fig. 11b, the extracting watermark image is a scrambled image; thus, we need do the inverse Arnold image scrambling to obtain the expanded watermark image $|W\rangle$. According to Eq. (3), the concrete circuit realizes inverse Arnold scrambling as shown in Fig. 18 where the constant input qubits $|0\rangle$ act as the ancillary qubit.

After we obtain the expanded watermark image, we need do the inverse expand operation and quantum measurement to obtain the classic watermark image.

3.3 Measurement

Obviously, the quantum watermark image is quantum superposition state as a composite quantum system composed by $2n + q$ qubits. In order to obtain the classical watermark image, we need do measurements on these states. For a $2^n \times 2^n$ NEQR watermark image with gray range $[0,\ 2^{q-1}]$, the measurement results are some collection of basis states$\left\{S_1, S_2, \ldots, S_{2(n+m)}\right\}$dimension Hilbert space. In [36], based on Grover's algorithm, the probability of pixels could be modified to measure the target

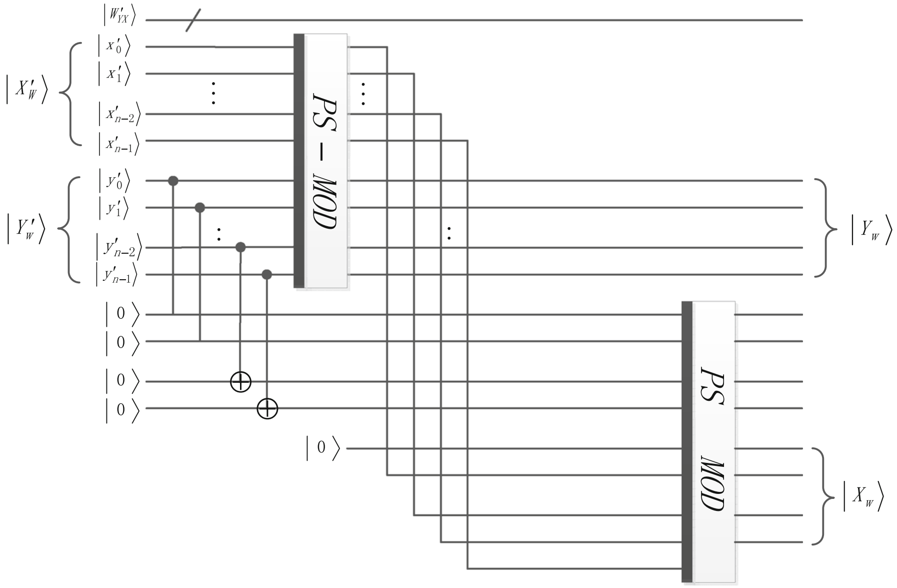


Fig. 18 Inverse Arnold scrambling

pixel with higher probability. It points that we can measure with probability $t^2_{\hat{i}}$ to get the result after certain iterations $\hat{i}$, where

$$\hat{i} \approx 0.7962a - 0.6057, t^2_{\hat{i}} \geq (0.9194 + 0.0567a^{-1} + 0.2302a^{-2} - 0.0336a^{-3})^2,$$
$$a = 2^{n+\frac{q}{2}}.$$

In practice, however, the quantum state cannot be practically observed in quantum system because a measurement will destroy the superposition. And what is worse, 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 quantum watermarked image state n times ($n > 1$) and measure each one to summarize the measurement results, from which we can estimate the watermark image. For more details, refer to the literature [36].

4 Circuit complexity and simulation experiments

4.1 Circuit complexity

The time complexity of the circuit depends on the number of the basic quantum gate. Literatures [46,47] pointed out that any reversible gate can be realized using 1 × 1 NOT gate and 2 × 2 reversible gates such as Controlled-V, Controlled-V^{+}, and Controlled-

NOT gate (CNOT). Thus, we take any one-qubit or two-qubit gate as the basic quantum gate, the time complexity of which is 1.

4.1.1 The time complexity of embedding procedure

The watermarking embedding procedure is shown in Fig. 11a. The quantum Arnold scrambling circuit (shown in Fig.13) needs 2 PA-MOD modules and n constant qubits $|0\rangle$. The PA-MOD module contains 1 RHA and $(n-1)$ RFA. The circuit realization of RHA is shown in Fig. 4b, the complexity of which is 4. The circuit realization of RFA is shown in Fig. 5a and the complexity is 8. Thus, the complexity of the single PA-MOD is $8n-4$. Therefore, the circuit complexity of Arnold scrambling is $\mathrm{O}(n)$ and n constant qubits are needed. In realizing embedding procedure steps as shown in Fig. 14, it includes three QE modules and the embedding circuit is shown in Fig. 15. The literatures [48] pointed out that only $(4\,k-8)$ 2-Control-Not gates were needed to construct a k-Control-Not gate, as well as some assistant qubits. The QE module (see Fig. 9a) contains $4n$ Controlled-Not gates and one $2n$-Controlled-Not gate (it means $2n$ qubits act as the controlled qubits). Thus, the complexity of single QE is $\mathrm{O}(n)$. Besides, the embedding circuit as shown in Fig. 15 can be regarded as containing six 4-Controlled-Not gates, and the complexity of which is $\mathrm{O}(1)$. Therefore, the circuit complexity of embedding the scrambling expanded watermark image into the carrier image is $\mathrm{O}(n)$.

4.1.2 The time complexity of extracting procedure

The watermarking extracting procedure is shown in Fig. 11b. In realizing extracting procedure steps as shown in Fig. 16, it includes two QE modules and the extracting circuit is shown in Fig. 17, which can be regarded as containing four 3-Controlled-Not gates, the time complexity of which is around $\mathrm{O}(1)$. The quantum inverse Arnold scrambling operation circuit shown in Fig. 17 includes two PS-MOD modules and $n+1$ constant input qubits $|0\rangle$. The single PS-MOD contains a PA module and a PA-MOD module, the time complexity of which is around $\mathrm{O}(n)$. Thus, the circuit complexity of realizing extracting the scrambling expanded watermark image from the watermarked image is $\mathrm{O}(n)$.

Therefore, according to the above analysis, the time complexity of watermarking embedding and extracting procedures of the proposed scheme is around $\mathrm{O}(n)$. Compared to classical image processing, the complexity of the Arnold scrambling and Arnold reverse scrambling is $\mathrm{O}(2^{2n})$ for a $2^n \times 2^n$ sized image. The complexity of the watermark embedding and extracting algorithm based on the least significant bit is also $\mathrm{O}(2^{2n})$ for a $2^n \times 2^n$sized image. Thus, the complexity of the scheme in classic image processing is $\mathrm{O}(2^{2n})$ for a $2^n \times 2^n$ sized image. However, in quantum image processing, if we omit the quantum image processing and measurement procedure, the quantum circuit cost is around $\mathrm{O}(n)$, which is very low for quantum image processing compared to classical image processing.

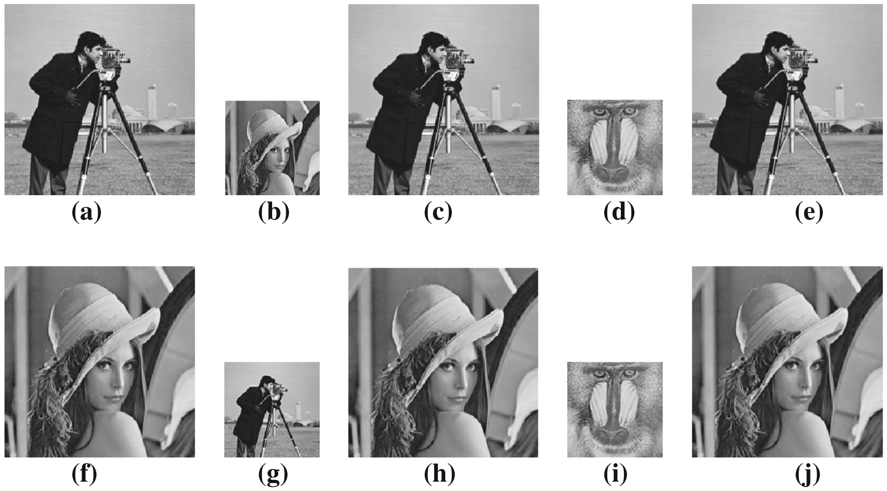


Fig. 19 Result of quantum watermarking experiments. **a** Carrier image, **b** watermark image, **c** watermarked image, **d** watermark image, **e** watermarked image, **f** carrier image, **g** watermark image, **h** watermarked image, **i** watermark image, **j** watermarked image

4.2 Simulation experiments analysis

This section gives the simulation experiment results of the proposed watermarking scheme. All experiments are simulated on the MATLAB R2014b. Three images named "baboon," "cameraman," and "Lena" are used. The sizes of carrier image and watermark image are 256 × 256 and 128 × 128, respectively.

The peak signal-to-noise ratio (PSNR) is one of the most used quantities to compare the fidelity of a stego image with its original version. PSNR is defined as follows:

$$PSNR = 10 \ \log_{10} \frac{MAX_I^2}{MSE} = 20 \ \log \ \frac{MAX_I}{\sqrt{MSE}} \tag{9}$$

Therein, MAX_I is the maximum gray-level value of the image. MSE is the mean squared error for two $m \times n$ gray-scale images: a carrier image I and its watermarked image version O, as defined in Eq. (10).

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - O(i, j)]^2 \tag{10}$$

The experimental results are shown in Fig. 19. The size of the watermark image is 128 × 128, and the size of the carrier image is 256 × 256.

Comparing to the carrier image of the experimental shown in Fig. 19, Table 2 shows the visual quality of the watermarked images. The visual quality PSNR is all around 54 dB. Therefore, we can conclude that the PSNR by our scheme is obviously higher than previous studies in [39] (around 30 dB) and [40] (around 44 dB).

Table 2 Similarity of watermarked images of our proposed scheme (PSNR [dB])

Watermark Carrier image	Lena	Cameraman	Mandrill
Cameraman	53.5916	–	54.1324
Lena	–	54.3408	54.1218

In a noiseless environment, our proposed scheme can extract an error-free watermark image. However, considering the complexity and difficulty to describe the noise environment in the quantum system, it is unreasonable to take it for granted that the noise types in classical image (macroscopic world) exist in quantum image (microscopic world). Thus, the robustness analysis of the watermark scheme in the noise environment is not discussed in this paper.

5 Conclusions

In this paper, a quantum gray-scale watermarking scheme using Arnold scrambling and LSB method based on NEQR is proposed. We assume that the size of carrier image and watermark image is $2n \times 2n$ and $n \times n$, respectively.

Watermark embedding and extracting procedures consist of two processes: comparing coordinates and replacing pixel bit. Before realizing the watermarking scheme, a series of quantum modules are designed to realize special functions, which mainly include QE, PA-MOD, and PS-MOD. The QE is used to compare the coordinates of all input images whether they are equal or not. The PA-MOD and PS-MOD are used to scramble and recover the watermark image, respectively. Besides, comparing with the other watermarking schemes, the experiment results show that our proposed scheme is superior to other schemes whether or not in noisy environment.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant No. 61463016, Program for New Century Excellent Talents in University under Grant No. NCET-13-0795, Training program of Academic and technical leaders of Jiangxi Province under Grant No. 20153BCB22002, and the advantages of scientific and technological innovation team of Nanchang City under Grant No. 2015CXTD003. Project of Science and Technology of Jiangxi province Grant No. 20161BAB202065. Project of International Cooperation and Exchanges of Jiangxi Province under Grant No. 20161BBH80034. Project of Humanities and Social Sciences in colleges and universities of Jiangxi Province under Grant No. JC161023.

References

1. Feynman, R.: Simulating physics with computers. Int. J. Theor. Phys. **21**(6–7), 467–488 (1982)
2. Deutsch, D.: Quantum theory, the church-turing principle and the universal quantum computer. Proc. R. Soc. Lond. A **400**, 97–117 (1985)
3. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124–134 (1994)
4. Grover, L.A.: fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219 (1996)

5. Venegas-Andraca, S., Bose, S.: Storing, processing, and retrieving an image using quantum mechanics.In: Proceedings of SPIE Conference of Quantum Information and Computation, **5105**, 134–147 (2003)
6. Latorre, J.: Image Compression and Entanglement. arXiv:quant-ph/0510031 (2005)
7. Le, P., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quant. Inf. Process. **10**(1), 63–84 (2011)
8. Zhang, Y., Lu, K., Gao, Y., et al.: NEQR: a novel enhanced quantum representation of digital images. Quant. Inf. Process. **12**(8), 2833–2860 (2013)
9. Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log-polar images. Quant. Inf. Process. **12**(9), 3103–3126 (2013)
10. Li, H., Zhu, Q., Lan, S., Shen, C., Zhou, R., Mo, J.: Image storage, retrieval, compression and segmentation in a quantum system. Quant. Inf. Process. **12**(6), 2269–2290 (2013)
11. Li, H., Zhu, Q., Zhou, R., Song, L., Yang, X.: Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. Quant. Inf. Process. **13**(4), 991–1011 (2014)
12. Yuan, S., Mao, X., Xue, Y., Chen, L., Xiong, Q., Compare, A.: SQR: a simple quantum representation of infrared images. Quant. Inf. Process. **13**(6), 1353–1379 (2014)
13. Sang, J., Wang, S., Li, Q.: A novel quantum representation of color digital images. Quant. Inf. Process **16**(2), 42 (2017)
14. Iliyasu, A.: Towards realising secure and efficient image and video processing applications on quantum computers. Entropy **15**, 2874–2974 (2013)
15. Yan, F., Iliyasu, A.M., Venegas-Andraca, S.E.: A survey of quantum image representations. Quant. Inf. Process **15**, 1–35 (2016)
16. Yan, F.: Quantum Computation Based Image Data Searching, Image Watermarking, and representation of Emotion Space. Ph.D. Thesis, Tokyo Institute of Technology, Japan (2014)
17. Yan, F., Iliyasu, A., Jiang, Z.: Quantum computation-based image representation, processing operations and their applications. Entropy **16**(10), 5290–5338 (2014)
18. Le, P.Q., Iliyasu, A.M., Dong, F., et al.: Strategies for designing geometric transformations on quantum images. Theor. Comput. Sci. **412**(15), 1406–1418 (2011)
19. Fan, P., Zhou, R.G., Jing, N., et al.: Geometric transformations of multidimensional color images based on NASS. Inf. Sci. S **340–341**, 191–208 (2016)
20. Le, P.Q., Iliyasu, A.M., Dong, F., et al.: Fast geometric transformations on quantum images. Iaeng Int. J. Appl. Math. **40**(3), 113–123 (2010)
21. Le, P.Q., Iliyasu, A.M., Dong, F., et al.: Efficient color transformations on quantum images. J. Adv. Comput. Intell. Intell. Inf. **15**(6), 698–706 (2011)
22. Fan, P., Zhou, Rigui: Quantum gray-scale image translation transform. J. Comput. Inf. Syst. **11**(23), 8763–8770 (2015)
23. Wang, J., Jiang, N., Wang, L.: Quantum image translation. Quant. Inf. Process. **14**(5), 1589–1604 (2015)
24. Zhou, R.G., Tan, C., Hou, I.: Global and local translation designs of quantum image based on FRQI. Int. J. Theor. Phys. **56**(4), 1382–1398 (2017)
25. Sang, J., Wang, S., Niu, X.: Quantum realization of the nearest-neighbor interpolation method for FRQI and NEQR. Quant. Inf. Process. **15**(1), 37–64 (2016)
26. Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. Quant. Inf. Process. **14**(5), 1559–1571 (2015)
27. Jiang, N., Wang, J., Mu, Y.: Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. Quant. Inf. Process. **14**(11), 4001–4026 (2015)
28. Jiang, N., Wu, W.Y., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling. Quant. Inf. Process. **13**(5), 1223–1236 (2014)
29. Jiang, N., Wang, L.: Analysis and improvement of the quantum Arnold image scrambling. Quant. Inf. Process. **13**(7), 1545–1551 (2014)
30. Jiang, N., Wang, L., Wu, W.Y.: Quantum Hilbert image scrambling. Int. J. Theor. Phys. **53**(7), 2463–2484 (2014)
31. Zhou, RiGui, Sun, YaJuan, Fan, Ping: Quantum image Gray-code and bit-plane scrambling. Quant. Inf. Process. **14**, 1717–1734 (2015)
32. Sang, J., Wang, S., Shi, X., Li, Qiong: Quantum realization of Arnold scrambling for IFRQI. Int. J. Theor. Phys. **55**(8), 3706–3721 (2016)

33. Caraiman, S., Manta, V.I.: Image segmentation on a quantum computer. Quant. Inf. Process. **14**(5), 1693–1715 (2015)
34. Zhang, Y., Lu, K., Xu, K., et al.: Local feature point extraction for quantum images. Quant. Inf. Process. **14**(5), 1573–1588 (2015)
35. Zhang, Y., Lu, K., Gao, Y.H.: QSobel: a novel quantum image edge extraction algorithm. Sci. China Inf. Sci. **58**(1), 1–13 (2015)
36. Jiang, N., Dang, Y., Wang, J.: Quantum image matching. Quant. Inf. Process. **15**(9), 3543–3572 (2016)
37. Zhang, W.W., Gao, F., Liu, B., Wen, Q.Y., Chen, H.: A watermark strategy for quantum images based on quantum Fourier transform. Quant. Inf. Process. **12**(2), 793–803 (2013)
38. Song, X.H., Wang, S., Liu, S., et al.: A dynamic watermarking scheme for quantum images using quantum wavelet transform. Quant. Inf. Process. **12**(12), 3689–3706 (2013)
39. Song, X., Wang, S., El-Latif, A.A.A., Niu, X.: Dynamic watermarking scheme for quantum images based on Hadamard transform. Multimed. Syst. **20**(4), 379–388 (2014)
40. Miyake, S., Nakamael, K.: A quantum watermarking scheme using simple and small-scale quantum circuits. Quant. Inf. Process. **15**, 1849–1864 (2016)
41. Heidari, S., Naseri, M.: A novel LSB based quantum watermarking. Int. J. Theor. Phys. **55**(10), 1–14 (2016)
42. Tirkel, A.Z., Rankin, G.A., VanSchyndel, R.M et al.: Electronic watermark. In: Proceedings of Digital Image Computing: Techniques and Applications, Macquarie University. 666–672 (1993)
43. Arnold, V.I., Avez, A.: Ergodic Problems of Classical Mechanics. Benjamin, New York (1968)
44. Dyson, F.J., Falk, H.: Period of a discrete cat mapping. Am. Math. Mon. **99**(7), 603–614 (1992)
45. Islam, M.S., Rahman, M.M., Begum, Z., et al.: Low cost quantum realization of reversible multiplier circuit. Inf. Technol. J. **8**(2), 208–213 (2009)
46. Thapliyal, H., Ranganathan, N.A .: New design of the reversible subtractor circuit. In: 11th IEEE Conference on Nanotechnology (IEEE-NANO), 2011. IEEE. pp. 1430–1435 (2011)
47. Kotiyal, S., Thapliyal, H., Ranganathan, N.: Circuit for reversible quantum multiplier based on binary tree optimizing ancilla and garbage bits. In: 2014 27th International Conference on VLSI Design and 2014 13th International Conference on Embedded Systems. IEEE. 545–550 (2014)
48. Weinfurter, H., Smolin, J.A.: Elementary gates for quantum computation. Phys. Rev. A **52**, 3457 (1995)