

A Quantum Image Watermarking Scheme Based on Two-Bit Superposition

Yang Zhou¹ \bigcirc • Ri-Gui Zhou¹ • XingAo Liu¹ • GaoFeng Luo¹

 \circled{c} Springer Science+Business Media, LLC, part of Springer Nature 2019 Received: 6 August 2018 /Accepted: 11 December 2018 /Published online: 3 January 2019

Abstract

Quantum watermarking technology protects copyright by embedding an invisible quantum signal in quantum multimedia data. This paper proposes a two-bit superposition method which embeds a watermark image (or secret information) into a carrier image. Firstly, the bit-plane is used to encrypt the watermark image. At the same time, the quantum expansion method is used to extend the watermark image to the same size with the carrier image, and then the image is encrypted through the Fibonacci scramble method again. Secondly, the first proposed method is the two bits of the watermark image which is embedded into the carrier image in accordance with the order of the high and lowest qubit, and the second proposed method which is the high bit of the watermark image is embedded to the lowest bit. Then the lowest bit of the watermark image is embedded in carrier image. Third, the watermark image is extracted through 1-CNOT and swap gates, and the watermark image is restored by inverse Fibonacci scramble, inverse expansion method and inverse bit-plane scramble method. Finally, for the validation of the proposed scheme, the signal-to-noise ratio (PSNR), the image histogram and the robustness of the two watermarking methods are analyzed.

Keywords Superposition \cdot Swap gates \cdot Fibonacci scramble \cdot Robustness \cdot Bit-plane scramble

Yang Zhou and Ri-Gui Zhou are co-first authors.

 \boxtimes Ri-Gui Zhou rgzhou@shmtu.edu.cn

> Yang Zhou zhouyang65@stu.shmtu.edu.cn

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

1 Introduction

In recent years, the development of quantum information processing shows that the development of quantum computer systems has a tremendous impact on the field of computer science. The fundamental reason is that quantum computers are beyond the reach of traditional computers $[1-3]$ $[1-3]$ $[1-3]$. One of the goals of quantum computers is to solve complex problems that cannot be solved even in supercomputers. Therefore, because of the remarkable nature of quantum computers, many innovative ideas have emerged in all related fields such as quantum image processing. However, the use of quantum computers to accelerate certain deterministic signal processing tasks still not be achieved. Similarly, quantum computers also have some potential roles in some areas. For example, running a new type of quantum Fourier transform [[4](#page-17-0)], wavelet transform and discrete cosine transform [\[5](#page-17-0)] and so on. However, quantum image processing in quantum computing still faces a large number of fundamental issues, such as the storage and presentation of quantum images.

Although there are many fundamental problems in quantum image processing, many methods that presentation of a quantum image was proposed in recent years. For example, the quantum logarithmic polar representation (QUALPI) proposed in Ref. [[6](#page-17-0)], a novel quantum color digital image representation (NCQI [[7\]](#page-17-0)), and so on. Under these quantum representations, quantum watermarking has appeared many research results, such as watermarking scheme based on the Quantum Fourier Transform [\[8\]](#page-17-0), watermarking scheme based on wavelet transform [\[9\]](#page-17-0) and the Hadamard gate transform [\[10](#page-17-0)] proposed by Song et al. Jiang propose the quantum watermarking scheme based on LSB and the encryption algorithm based on quantum LSB [[11](#page-17-0)]. A simple small-scale quantum circuit watermarking scheme was proposed [[12](#page-17-0)]. In 2016, the quantum least significant bit algorithm based on the NCQI representation [[13\]](#page-17-0) was proposed. In 2018, the least significant bit algorithm based on the INEQR was proposed [[14\]](#page-17-0). Similarly, there are some achievements in the sub-directions in image processing. In 2017, quantum space value domain filtering was proposed [[15\]](#page-17-0). In 2018, Li proposed an improved frequency domain filtering method based on quantum color images [[16\]](#page-18-0). For 2015 years, Mario proposed a quantum logic image denoising method [[17\]](#page-18-0). Hua proposed a quantum image encryption algorithm based on image correlation decomposition [\[18](#page-18-0)]. Song proposed a method based on constrained geometry and color transformed quantum image encryption algorithm [[19\]](#page-18-0). Zhou proposed an encryption scheme based on quantum iterative Arnold transform and quantum image shift operation [[20](#page-18-0)]. In summary, although there are some problems in the current stage of quantum image processing, these not stop the rapid development trend.

In this paper, a double embedded watermarking scheme is proposed. Firstly, the watermark image is scrambled by the bit-plane scrambling method. Secondly, the watermark image is expanded by the quantum expansion circuit. Thirdly, utilizes the Fibonacci scrambling method to scramble the expanded image. Finally, the watermark image is embedded in the carrier image.

The rest of the paper is organized as follows. A brief basic theoretic knowledge is given in Section 2. In Section 3 a new quantum embedded watermarking scheme is proposed. Section 4 is devoted to the simulation-based experiments and analysis. Finally, the conclusion is drawn in Section 5.

2 Basic Knowledge

2.1 The Novel Enhanced Quantum Representation (NEQR)

The NEQR was first proposed in 2013 [\[21\]](#page-18-0). It uses q quantum bits to store the color values of each pixel [[22](#page-18-0)], which is more convenient for the operation of image colors. According to NEQR this Eq. (1) is shown.

$$
|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |f(Y,X)\rangle |YX\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \sum_{i=0}^{q-1} |C_{YX}^i\rangle |YX\rangle
$$
(1)

$$
f(Y,X) = C_{YX}^{0} C_{YX}^{1} \dots C_{YX}^{q-2} C_{YX}^{q-1}, C_{YX}^{k} \in \{0,1\}, f\langle Y,X\rangle \in \{0,2^q-1\}
$$
 (2)

Where the binary sequence $|C_{YX}^{0}\rangle |C_{YX}^{1}\rangle...|C_{YX}^{q-2}\rangle |C_{YX}^{q-1}\rangle$ encodes the color value, and the gray range is2ⁿ, $|YX\rangle = |y_{n-1}y_{n-2}...y_1y_0\rangle |x_{n-1}x_{n-2}...x_1x_0\rangle, |y_1y_0\rangle \in \{0, 1\}$ encodes the vertical and horizontal coordinates information. Therefore, NEQR needs $q + 2n$ qubits to represent an $2^n \times 2^n$ image with gray range 2^n .

An example of 2×2 pixels image is shown in Fig. [1](#page-3-0). In this example, the gray value ranges from 0 to 255, so the 8 qubits are needed to store this color information.

2.2 Fibonacci Image Scrambling

When the Fibonacci scrambling [\[23](#page-18-0)] acts on a digital classical image sized $2^n \times 2^n$, this transformation can be defined as follows Eq. (3):

$$
\begin{pmatrix} x_F \\ y_F \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{(mod } 2^n)
$$
 (3)

i.e.,

$$
x_F = (x \pm y) \mod 2^n
$$

$$
y_F = x
$$

 (x_F, y_F) is the coordinates of the scrambled image.

The inverse Fibonacci transformation is defined as follows:

$$
\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} x_F \\ y_F \end{pmatrix} (mod 2^n) = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x_F \\ y_F \end{pmatrix} (mod 2^n)
$$
(4)

i.e.,

$$
x = y_F
$$

$$
y = (x_F - y_F) \text{mod} 2^n
$$

As shown in Eq. (4), the adder modulo plays an important role in the Fibonacci Scrambling, and its quantum circuit proposed in Ref. [\[23](#page-18-0)] is given as follows Fig. [3.](#page-4-0)

Plain adder network shown in Fig. [2](#page-3-0) consists of basic sum circuit and carries circuit. Based on Plain adder, Ref. [[23](#page-18-0)] designed a ADDER-MOD module as shown in Fig. [3](#page-4-0).

The reversible sum and reversible carries circuit proposed in Ref. [\[23\]](#page-18-0) is shown in Fig. [4](#page-4-0).

$$
\begin{array}{c|c|c} \hline 80 & 100 & |I\rangle = \frac{1}{2} \langle 01010000 \rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle \\ \hline 150 & 200 & + |10010110\rangle \otimes |10\rangle + |11001000\rangle |11\rangle \end{array}
$$

Fig. 1 2×2 image

3 Watermarking Scheme

At present, the implemented watermarking scheme usually uses the least significant bit algorithm. However, the embedded capacity is only a qubit. This paper proposes two kinds of watermarking scheme. One method is to embed the two bits of the watermark image into the image of the carrier image through the overlay method. Another method is to embed the two-qubit of the watermark image by itself, and then the operated watermark image is embedded into the carrier image. Next, the two kinds of watermarking methods are introduced.

3.1 Image Preprocessing

3.1.1 Image Bit-Plane Scramble

In 2015, the quantum image gray-code and bit-plane scrambling [\[24](#page-18-0)] was proposed by Zhou et al. Inspired by this article, this paper utilizes a similar pixel bit-plane algorithm. The bitplane scramble circuit is shown in Fig. [5.](#page-5-0)

Generally, an image has 8-pixel bit-plane. When the digital watermark image is transformed into a quantum watermark image through the NEQR, the digital bit-plane of the image becomes a qubit-plane. Next, watermark image is scrambled by a bitplane scramble. Firstly, in accordance with the order of " $0-4$ ", " $1-5$ ", " $2-6$ ", and " $3-$ 7", these bit planes are exchanged through quantum swap gates. After the exchange is completed, if the quantum state of the pixel bit-plane in the original order "4567" is

Fig. 2 Plain adder network

Fig. 3 Adder modulo N

∣1〉, 1-CNOT is used to change the other bit-plane pixel bit stream. Go through this operation, watermark image's bit-plane order is changed and some bit-plane pixel's bit stream is changed. Finally, the watermark image scramble is completed by means of the simple bit-plane scramble algorithm. Utilizes the scrambling circuit, the watermark image can be scrambled so as to achieve the scrambling effect in Fig. [6.](#page-5-0)

In Fig. [6,](#page-5-0) (a) is original watermark image, (b) scrambled watermark image. The grey-value image becomes chaotic after bit-plane scramble is executed. And then the scrambled image can't be recognized.

3.1.2 Image Expand Method

The first step of the watermark image preprocessing has been completed. Next, utilizes the quantum expansion circuit to expand the scrambled watermark image, in order to gain the same size as carrier image. This expansion circuit is shown in Fig. [7](#page-6-0).

Via the quantum expansion circuit, watermark image is expanded in accord with the order the clock-wise direction. Suppose there are a watermark image with the size of $1 \times$ 1, and a carrier image with the size of 4×4 . Because of the original watermark image coordinate is $[0, 0]$, expanded watermark image coordinate is $[0, 0][0, 1][1, 0][1, 1]$. Thus, utilizes the auxiliary qubits ∣0〉 record the expanded watermark image coordinate information and pixel bit-plane distribution information in Fig. [7](#page-6-0). On account of the expand watermark image dependence the clock-wise direction, that's the corresponding coordinates after the bit-plane expansion is " $(0, 1) - [0, 0]$ ", " $(2, 3) - [0, 1]$ ", " $(4, 5) - [1, 1]$ 1]", "(6, 7) − [1, 0]". Finally, the eight bit-plane is distributed and new watermark image is obtained. In the Fig. [7,](#page-6-0) $|C_{xy}^0 \cdots C_{xy}^7\rangle$ represent the original watermark image bit-plane pixel value, auxiliary qubits ∣0〉 represent the coordinates and temporary memory pixel *a b*
 b
 b
 b
 c + *b*) model
 c + *b*) model in the image can be seramble as co

(a) the sum operation

(b) the carry operation

Fig. 5 Bit-plane scramble circuit

3.1.3 Image Fibonacci Scramble

Referring to the Fibonacci scramble formula [\(3\)](#page-2-0) in Section 2.2, the expanded image can be encrypted through the scramble circuit in the Fig. [8.](#page-7-0)

In Fig. [8](#page-7-0), X and Y represent the expanded image's coordinate information, X_F and Y_F represent the scramble expanded image's coordinate information. Through the scramble circuit, expanded watermark image is scrambled. However, expanded watermark image is sightless, so that the watermark image has an additional layer of protection and attacker cannot recognize the scrambled image.

3.2 Watermark Embedded Scheme

Through image preprocessing, the watermark image and the carrier image have the same size. All preparations have been completed. Next, the watermark image is need to be embedded in the carrier image. The entire embedded procedure is shown in Fig. [9.](#page-7-0)

Fig. 6 Bit-plane scramble effect

Fig. 7 quantum expansion circuit

Observe the Fig. [9](#page-7-0), the watermark image is embedded in the carrier image after multiple operations. The first operation of the watermark image has been introduced in section 3.1. Next, the operation which the watermarking image is embedded, is shown in the following steps.

- Step 1: Watermark and carrier images are transformed into the quantum image $|W\rangle$ and $|C\rangle$ through the NEQR.
- Step 2: Quantum watermark image is scrambled through the bit-plane scramble algorithm. The scrambled watermark image is disordered and chaotized, and then detail operation procedure is described in section 3.1.1. In the end, the scrambled watermark image $|PW\rangle$ is obtained.
- Step 3: The scrambled quantum watermark image is unable to embedded in the carrier, because of watermark image size is not the same as carrier image. Next, scrambled watermark image need to be expanded, so that watermark has the same size as carrier image. However, there is a problem that how to expand watermark image. In order to solve this problem, quantum expansion circuit is proposed in Fig. 7. Through quantum expansion circuit, watermark image ∣EPW have the same size

Fig. 8 Fibonacci scramble circuit

as carrier image and a detailed description of the expand procedure is shown in section 3.1.2.

According to the image preprocessing procedure, the extended watermark image needs to be re-encrypted by means of a Fibonacci scramble, so that the watermark image is less easily cracked by the attacker. This procedure is described in section 3.1.3.

Fig. 9 Embedded procedure

 \mathcal{D} Springer

Step 4: In this step, the extended watermark image is embedded into the carrier image by two kinds of embedding methods. The descriptions of the two kinds of embedding methods are given in section 3.2.1 and 3.2.2.

3.2.1 Self-Embedded Watermark Scheme

In the previous section, the watermark was embedded into the carrier image, but it is not described that how to embed in carrier image. This section will introduce the first watermark embedding method in detail. a detailed embedded circuit is shown in Fig. 10.

In the Fig. 10, $|K_1\rangle$ represent the least bit that the carrier image. Specific NEQR presentment is given in Eq. (5) .

$$
|K_1\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n - 1} \sum_{X=0}^{2^n - 1} \sum_{i=0}^{q-1} |K_{YX}^i\rangle |YX\rangle
$$
 (5)

Firstly, if the $|C_{xy}^0\rangle$ and $|FEPW_{xy}^1\rangle$ are equal, control swap gate is not performed. If the $|C_{xy}^0\rangle$ and $|FEPW^1_{xy}\rangle$ are not equal, this information is recorded through auxiliary qubit ∣0), and then $\ket{FEPW_N^1}$ is embedded in $\ket{C_N^0}$ through the control swap gates. Secondly, utilizes the $\ket{K_1}$ record the recent carrier image $|C_{xy}^{(0)}\rangle$. Thirdly, if the $|C_{xy}^{(0)}\rangle$ and $|FEPW_{xy}^{(0)}\rangle$ are not equal, utilizes the auxiliary qubit∣0〉record this inequality information, and then auxiliary qubit state is ∣1〉 when the $|C_{xy}^0\rangle$ and $|FEPW_{xy}^0\rangle$ are not equal, the carrier information is exchanged by the 1-
CONT In the and synopter images $|GW|K\rangle$ and $|K\rangle$ are alternational CONT. In the end, quantum image $|CW\rangle, |K_1\rangle$ and $|K_2\rangle$ are obtained.

3.2.2 Superimposed Embedded Watermark Scheme

The first method of watermark image embedded scheme is introduced in section 3.2.1. Thus, the other method is introduced in this section and the detailed embedded circuit is shown in Fig. [11.](#page-9-0)

Among them, $|K_1\rangle$ represents an image with only one bit-plane, which is shown in Eq. (5), $|K_2\rangle$ represents the key image that stores the original carrier image $|C_{xy}^0\rangle$ information. In this

Fig. 11 Detailed superimposed embedded circuit

embedded circuit, firstly, utilizes the 1-CNOT record and store the $|FEPW_{xy}^0\rangle$ information. Secondly, if the state of the two bit-plane contained in the quantum image∣FEPW) is not the same, the upper bit bit-plane is embedded in the low order through 1-CNOT. Finally, if the state of changed $|FEPW_{xy}^{0}\rangle$ and $|C_{xy}^{0}\rangle$ are not equal, this qubit is exchanged through the control swap gates. In the end, three quantum images $|CW\rangle, |K_1\rangle$ and $|K_2\rangle$ are obtained, and the quantum image ∣CW is the most important of the copyright businessman.

3.3 Watermark Extraction Scheme

The watermark image has been embedded in the carrier image through. However, if copyright businessman wants to get the embedded information that contained in the cover image, the extracting circuit is needed. Thus, the entire extracting circuit is introduced. The extract framework is shown in Fig. 12.

In this figure, the quantum images $|CW\rangle$, $|K_1\rangle$ and $|K_2\rangle$ are needed.

In Fig. 12, quantum images $|CW\rangle$, $|K_1\rangle$ and $|K_2\rangle$ are obtained through NEOR, and then scrambled expanded watermark image is gained by quantum extract circuit. In the end, the original watermark image is restored through a set of reversible quantum circuits. The concrete operation can be divided into the following several steps.

Fig. 12 Watermark extract framework

- Step 1: A classical image that contained hidden information is loaded, next those relative key images are processed by NEQR quantum presentation.
- Step 2: After those relative images has been prepared, the carrier image that hidden secret information, and the key image is operated through the quantum extract circuit. Finally, the scrambled watermark image is gained. But due to the quantum extract circuit contain two kinds of watermark method, the watermark extract method is described in section 3.3.1and 3.3.2.
- Step 3: Quantum extract operation has been completed, but there gets a chaotic and unrecognized image that rooted in the carrier image. Next, reversible Fibonacci scramble is used to get the expanded watermark image. According to the Eq. ([4\)](#page-2-0), the chaotic and unrecognized image is restored, so that expanded watermark image is gotten. However, this image is not recognized, next the quantum restored circuit that shown in Fig. 13 is utilized to restore the watermark image.

In the Fig. 13, $|y_0 \cdots y_n\rangle$ and $|x_0 \cdots x_n\rangle$ represents the expanded watermark's coordinates information, $|y_0 \cdots y_{n-1}\rangle$ and $|x_0 \cdots x_{n-1}\rangle$ represents the restored watermark's coordinates

Fig. 14 Reversible bit-plane scramble circuit

information, $|C_{xy}^0 \cdots C_{xy}^7\rangle$ represent the restored watermark's bit-plane pixel information. Firstly, utilizes the quantum state $|x_0\rangle$ and $|y_0\rangle$ are used to express the expanded coordinates. Secondly, according to the relative coordinates, the original watermark image bitplane pixels is assigned in new quantum coordinates. Finally, this image is restored through N-CNOT. However, this image is chaotic, so that watermark image is not recognized. On the basis of image preprocessing, reversible bit-plane is used to restore the original watermark image. According to the Fig. [5](#page-5-0) bit-plane scramble circuit, reversible scramble circuit is shown in Fig. 14.

In Fig. 14, the scrambled image bit-plane is exchanged in accord with order "0–4", "1–5", " $2-6$ ", " $3-7$ ". And then 1-CNOT is utilized when the "0123" bit-plane quantum state is | 1).

Step 4: the original watermark image is retrieved through quantum measurement.

Fig. 15 Detailed extract circuit

Fig. 16 Detailed extract circuit

3.3.1 Self-Embedded Extract Method

According to the step2, we will introduce the first method. This circuit is shown in Fig. [15.](#page-11-0)

Firstly, the watermarked carrier image $|CW_{xy}^{0} \rangle$ is recorded through auxiliary qubit $|0\rangle$, which represented the watermark least qubit $|W_{xy}^0\rangle$. Secondly, utilizes swap gates to restore exprise increase that the courier increase is restored. Finally, the least increase $|K\rangle$ is recorded carrier image, then the carrier image is restored. Finally, the key image $|K_1\rangle$ is recorded through auxiliary qubit $|0\rangle$, which represented the watermark image qubit $|W_{xy}^1\rangle$. In the end, the watermark image is extracted.

3.3.2 Superimposed Embedded Extract Method

Compared with the first one self-embedded extract method, the other superimposed embedded extract method is simple and easy to implement. The detailed circuit is shown in Fig. 16.

In the Fig. 16, firstly, the original carrier image (CW_{xy}^0) is recorded through auxiliary qubit∣0), which represented the watermark qubit $|W_{xy}^1\rangle$. Secondly, the carrier image is restored by swap gates. Finally, the watermark image least qubit $|W_{xy}^0\rangle$ is restored through 1-CNOT recorded the key image $|K_1\rangle$, so that encrypted watermark image is obtained. In the end, the original carrier image is restored while the encrypted watermark image is also acquired.

4 Experiments and Analysis

At present, quantum computers are in the theoretical stage and there is no available quantum computer to analyze this method. Thus, this article utilizes MATLAB2014b to simulate this experiment on a classical computer. So, this section gives the simulation experiment results of

Original Watermark Image	Extracted Watermark Image					
	Barbara	Cameraman	Bank	Peppers	Couple	
Barbara		37.2690	37.1229	37.1918	37.1243	
Cameraman	39.2024		39.2511	39.2630	39.2504	
Bank	37.7192	37.6618		37.7244	37.7437	
Peppers	38.2067	38.1160	38.2307		38.0308	

Table 1 The robustness of the self-embedded method

Original Watermark Image	Extracted Watermark Image					
	Barbara	Cameraman	Bank	Peppers	Couple	
Barbara		37.2296	37.0956	37.0752	37.0566	
Cameraman	36.3280		36.2414	36.1932	36.2763	
Bank	37.0513	37.0920		37.0462	37.0693	
Peppers	37.1624	37.2952	37.3478		37.2148	

Table 2 The robustness of the superimposed embedded method

the proposed watermarking scheme [[25\]](#page-18-0). The simulations are built on linear algebraic constructions. The quantum states and the quantum operations are simulated by complex vectors and unitary matrices [\[25](#page-18-0)]. In this experiment, we use bridge image [[26](#page-18-0)], cameraman image,

Fig. 17 Experiment result

2 Springer

Carrier Image	Watermark Image					
	Barbara	Couple	Bank	Cameraman	Peppers	
Barbara		53.9953	53.7851	53.3425	53.7396	
Couple	54.1840		53.9034	53.4445	53.7998	
Bank	54.1009	54.0199		53.3581	53.7310	
Cameraman	54.0889	54.0002	53.8110		53.7209	
Peppers	54.0701	53.9836	53.7951	53.3530		

Table 3 The PSNR values of the self-embedded method (PSNR [dB])

Barbara image and baboon image and so on to verify this idea. The watermark image size $is256 \times 256$ and carrier image size is 512×512 .

4.1 Robust Analysis

The robustness of the watermark, is the watermark information must be difficult to remove, or any attempt to destroy the watermark will result in a serious degradation of the image quality. Therefore, salt and pepper noise are added to the watermarked carrier image in this paper, and the robustness of the proposed scheme is obtained. as a rule, the PSNR is utilized to observe the watermark-image's visually effect. If the visually effect is higher, the robustness of watermark is stronger. The PSNR as defined in the following Eq. ([6](#page-16-0)). The robustness of the self-embedded method is shown in Table [1](#page-12-0). The robustness of the superimposed embedded method is shown in Table [2.](#page-13-0)

In Table [1](#page-12-0), it is seen that the comparison result between the extracted watermarked image and the original watermarked image. But the watermark image under this self-embedded method has a few missing, the robustness of self-embedded method is about 38db. Meanwhile, the robustness of superimposed embedded method is as same as the self-embedded method. In Table [2](#page-13-0), the robustness of superimposed method is about 37db.

4.2 Visual Analysis

The peak-signal-to-noise ratio(PSNR), being one of the most used quantity in classical for comparing the fidelity of a watermarked image with its original version, will be used as our embedded carrier image evaluation quantity by transforming the quantum images into classical

Carrier Image	Watermark Image					
	Barbara	Couple	Bank	Cameraman	Peppers	
Barbara		54.1064	53.8552	54.4640	53.8425	
Couple	53.9815		53.9593	54.5482	53.9431	
Bank	53.9075	54.1181		54.4669	53.8435	
Cameraman	53.8954	54.1293	53.8676		53.8498	
Peppers	53.8852	54.0950	53.8457	54.4566		

Table 4 The PSNR values of the superimposed embedded method (PSNR [dB])

Fig. 18 The histogram graphs of carrier images and watermarked images

 $\underline{\textcircled{2}}$ Springer

forms [\[26](#page-18-0)]. PSNR as defined in the following eq. (6). The more the watermarked image resembles its carrier image, the more the value of PSNR increases.

$$
PSNR = 10 \log_{10} \frac{MAX_I^2}{MSE} = 20 \log \frac{MAX_I}{\sqrt{MSE}}
$$
(6)

Therein, *MAX_I* is the maximum possible gray-level value of the image. MSE is the mean squared error for two gray-scale images, a carrier image (or watermark) I and its watermarked version (or extracted watermark) O, as defined in the following Eq. (7).

$$
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - O(i,j)]^2
$$
 (7)

The experiment result is shown in Fig. [17](#page-13-0).

In the Fig. [17](#page-13-0), (a) represent the carrier image, (b) represent the original watermark image, (c) represent the watermarked carrier image, (d) represent the extracted watermark image. In order to detect watermarked carrier image visual quality, the peak-signal-to-noise ratio is given in Tables [3](#page-14-0) and [4.](#page-14-0)

Observe the peak signal-to-noise ratios of carrier image in the two watermarking embedded methods in Tables [3](#page-14-0) and [4.](#page-14-0) The two watermark methods proposed in this paper have similar peak-to-noise ratios as same as others watermarking scheme. However, the two watermarking embedded methods in this paper have some other advantages. First, the embedding capacity is embedded 2-qubit information bit in the carrier image least significant qubit. Second, the circuit are simpler and more convenient in this paper.

4.3 Image Grey-Value Analysis

Now, there is another tool to evaluate the fidelity of the watermarking image, which is the histogram of the image. The images' histogram is the frequency used to display the pixel intensity values. In the images' histogram, the x-axis shows the grayscale intensity, and the yaxis shows the frequencies of these intensities. The histogram of the image has many applications in image processing. One of the applications is image analysis [\[27](#page-18-0)]. By looking at the histogram of the image, we can compare the grayscale and intensity of the image after the watermarked of the image. In order to further test the results of the experiment, a histogram of the three original carrier images and the embedded watermarked carrier image in Fig. [18](#page-15-0). According to Fig. [18](#page-15-0), the histogram of the watermarked image is very consistent with the histogram of the carrier image.

5 Conclusion

In this article, two superimposed watermarking methods have been proposed. The watermark and carrier image sizes are used in this paper are 256×256 and 512×512 , respectively.

In the paper, the two of the watermarking methods is proposed. Firstly, the watermark image and the carrier image are transformed into the quantum images by NEQR. Secondly, the watermark image is encrypted for the first time utilizes a new bit-plane scramble algorithm. Thirdly, the watermark image is extended to the same image as the carrier through the quantum expansion circuit. Fourthly, utilizes the Fibonacci scramble to encrypt the watermark image

again. After the fourth operation has been completed, the watermark image will be embedded in the carrier image. The first self-embedded method is to separate all of the watermark image qubit planes, and then the qubit planes are respectively embedded in the least significant bits of the carrier image. Control swap gates and 1-CNOT gates is employed to complete this operation. The other superposition embedding method is to embed the high qubits of the watermark image in the least qubits of the watermark image, and then the operated lowest bits is embedded in the carrier image. Finally, a watermarked carrier image is obtained.

Next, the extraction of the watermark image is introduced. Firstly, the classical image is converted into a quantum image by NEQR. Secondly, the watermark image is extracted through detailed extract circuit, which is divided into two kinds of cases. The extracting method is similar, which is utilizes 1-CNOT and swap gate to accomplish this operation. Thirdly, the extracted watermark image is converted into the original watermark image by inverse Fibonacci, inverse extension and inverse qubit-plane scramble. Finally, the watermark image is restored.

Acknowledgements This work is supported by the National Natural Science Foundation of China under Grant No. 61463016, "Science and technology innovation action plan" of Shanghai in 2017 under Grant No. 17510740300, and the advantages of scientific and technological innovation team of Nanchang City under Grant No. 2015CXTD003;

References

- 1. N, X., Zhu, J., D, L., et al.: Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. Phys. Rev. Lett. 108(13), 130501 (2012)
- 2. Van d, S.T., Wang, Z.H., Blok, M.S., et al.: Decoherence-protected quantum gates for a hybrid solid-state spin register. Nature. 484(7392), 82–86 (2012)
- 3. Pla, J.J., Tan, K.Y., Dehollain, J.P., Lim, W.H., Morton, J.J.L., Jamieson, D.N., Dzurak, A.S., Morello, A.: A single-atom electron spin qubit in silicon. Nature. 489(7417), 541–545 (2012)
- 4. Fijany, A., Williams, C.P.: Quantum wavelet transforms: fast algorithms and complete circuits. Lect. Notes Comput. Sci. 1509, 10–33 (1998)
- 5. Tseng C C., Hwang T M.: Quantum circuit design of 8×8 discrete cosine transform using its fast computation flow graph// IEEE International Symposium on Circuits and Systems. IEEE. 1, 828-831(2005)
- 6. Zhang, Y., Lu, K., Gao, Y., Xu, K.: A novel quantum representation for log-polar images. Quantum Inf. Process. 12(9), 3103–3126 (2013)
- 7. Sang, J., Wang, S., Li, Q.: A novel quantum representation of color digital images. Quantum Inf. Process. 16(2), 16–42 (2017)
- 8. Yang, Y.G., Jia, X., Xu, P., et al.: Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform. Quantum Inf. Process. 12(2), 793–803 (2013)
- 9. Song, X.H., Wang, S., Liu, S., Abd 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)
- 10. Song, X., Wang, S., El-Latif, A.A.A., et al.: Dynamic watermarking scheme for quantum images based on Hadamard transform. Multimedia Systems. 22(2), 273–274 (2016)
- 11. Jiang, N., Zhao, N., Wang, L.: LSB based quantum image steganography algorithm. Int. J. Theor. Phys. 55(1), 107–123 (2016)
- 12. Miyake, S., Nakamae, K.: A quantum watermarking scheme using simple and small-scale quantum circuits. Quantum Inf Process. 15(5), 1849–1864 (2016)
- 13. Sang, J., Wang, S., Li, Q.: Least significant qubit algorithm for quantum images. Quantum Inf. Process. 15(11), 4441–4460 (2016)
- 14. Zhou, R.G., Zhou, Y., Zhu, C., Wei, L., Zhang, X., Ian, H.: Quantum watermarking scheme based on INEQR. Int. J. Theor. Phys. 57(4), 1120–1131 (2018)
- 15. Yuan, S., Mao, X., Zhou, J., Wang, X.: Quantum image filtering in the spatial domain. Int. J. Theor. Phys. 56(8), 2495–2511 (2017)
- 16. Li, P., Xiao, H.: An improved filtering method for quantum color image in frequency domain. Int. J. Theor. Phys. 57(1), 258–278 (2018)
- 17. Mastriani, M.: Quantum Boolean image denoising. Quantum Inf. Process. 14(5), 1647–1673 (2015)
- 18. 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)
- 19. Song, X.H., Wang, S., El-Latif, A.A.A., et al.: Quantum image encryption based on restricted geometric and color transformations. Quantum Inf. Process. 13(8), 1765–1787 (2014)
- 20. Zhou, N., Hu, Y., Gong, L., et al.: Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations. Quantum Inf. Process. 16(6), 1–23 (2017)
- 21. Zhang, Y., Lu, K., Gao, Y., Wang, M.: A novel enhanced quantum representation of digital images. Quantum Inf. Process. 12(8), 2833–2860 (2013)
- 22. Ping, F., Zhou, R.-G., Jing, N., Li, H.-S.: Geometric transformations of multidimensional color images based on NASS. Inf Sci. 340–341 (2016)
- 23. Jiang, N., Wang, L.: Analysis and improvement of the quantum Arnold image scrambling. Quantum Inf. Process. 13(7), 1545–1551 (2014)
- 24. Ri-gui, Z., Ya Juan, S., Fan, P.: Quantum image gray-code and bit-plane scrambling. Quantum Inf Process. 14(5), 1717–1734 (2015)
- 25. Ri-Gui, Z., Wenwen, H., Ping, F.: Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Inf. Process. 16(9), 212–233 (2017)
- 26. Jianzhi, S., Shen, W., Qiong, L.: Least significant qubit algorithm for quantum images. Quantum Inf. Process. 15(11), 4441–4460 (2016)
- 27. Caraiman, S., Vasile, M.: Histogram-based segmentationof quantum image. Theor. Comput. Sci. 529, 46–60 (2014)