

A quantum watermarking scheme using simple and small-scale quantum circuits

S. Miyake¹ · K. Nakamae¹

Received: 20 October 2015 / Accepted: 28 January 2016 / Published online: 20 February 2016
© Springer Science+Business Media New York 2016

Abstract A new quantum gray-scale image watermarking scheme by using simple and small-scale quantum circuits is proposed. The NEQR representation for quantum images is used. The image sizes for carrier and watermark are assumed to be $2n \times 2n$ and $n \times n$, respectively. At first, a classical watermark with $n \times n$ image size and 8 bits gray scale is expanded to an image with $2n \times 2n$ image size and 2 bits gray scale. Then the expanded image is scrambled to be a meaningless image by the SWAP gates that controlled by the keys only known to the operator. The scrambled image is embedded into the carrier image by the CNOT gates (XOR operation). The watermark is extracted from the watermarked image by applying operations in the reverse order. Simulation-based experimental results show that our proposed scheme is excellent in terms of three items, visual quality, robustness performance under noises, and computational complexity.

Keywords Quantum watermarking · Quantum image processing · Quantum computation · Quantum circuit

1 Introduction

Digital image is one of the most important representation forms in the information society and widely used in many fields. There are many images which can be used in commercial purposes. Then to protect these images from unauthorized use, copying and manipulation is very important theme for experts and researchers. Image protection scheme is mainly divided in two categories. One is image cryptography, and the other

✉ K. Nakamae
nakamae@ist.osaka-u.ac.jp

¹ Information Science and Technology, Osaka University, Suita, Japan

is image watermarking [1–6], while the image cryptography is to transform an image to be protected to a meaningless form, the image watermarking is to hide image information by embedding it into some media (image).

In recent years, the technology of quantum information and quantum computers are rapidly developing. Especially Shor's prime factor decomposition algorithm is threatening cryptography used in conventional computers such as RSA cryptosystem. Similar to classical computers, data on quantum computer can be attacked in many ways, so the research interest of quantum data security is increasing. It means that the information protection technology that has been used on a classical computer is also necessary for the technology on a quantum computer.

Quantum computer implements parallel computation by using superposition of states that is a basic property of quantum mechanics and is expected to have greatly higher processing capabilities than that of a conventional (classical) computer. Quantum cryptography or watermarking provides a new foundation for an unconditionally secure global communications infrastructure. Its security rests upon quantum mechanical phenomena, such as the inevitability of changing a quantum state if it is measured in the "wrong" basis, and the impossibility of copying (or cloning) an unknown quantum state [7].

In quantum image processing, two image expression methods using quantum bits (qubits) have been reported: a flexible representation of quantum images (FRQI) [8] and a novel enhanced quantum representation of digital images (NEQR) [9]. FRQI is an expression method of quantum image that encodes a gray-scale value into one qubit. Several watermarking schemes using FRQI are proposed [10–12] where complex transforms such as quantum Fourier transform (QFT) and quantum wavelet transform (QWT) are utilized. Since such transforms requires many quantum gates, it is not easy to apply quantum error-correcting codes to such quantum circuits. So it is desirable to implement the quantum image watermarking scheme by using simple and small-scale quantum circuits.

In addition, these schemes [10–12] are pointed out that the procedures are not clearly described and several steps are ambiguous [13–15].

As an alternative to the FRQI, the NEQR have been proposed [9] where gray-level values of 8 bits are encoded into binary strings of 8 qubits. So it is easier to transform classical images into quantum images. Though a watermarking (steganography) scheme using NEQR has been proposed [16], the objective images for watermarking are binary images. Table 1 shows the summary of reported quantum image watermark-

Table 1 Summary of reported quantum image watermarking schemes

Scheme	Image representation	Quantum circuits	Watermark	Embedding size
Zhang et al. [10]	FRQI	QFT	Gray scale	$\times \frac{1}{2}$
Song et al. [11]	FRQI	QWT	Gray scale	$\times 1$
Song et al. [12]	FRQI	HT	Gray scale	$\times 1$
Jiang et al. [16]	NEQR	Moiré	Binary image	$\times 1$

QFT quantum Fourier transform, *QWT* quantum wavelet transform, *HT* Hadamard transform; Moiré, circuit generating Moiré pattern

ing schemes. As far as we know, a gray-scale watermarking scheme using the NEQR has not been reported.

In this paper, we propose a new quantum gray-scale image watermarking scheme by using simple and small-scale quantum circuits where the NEQR is utilized. The outline of this work is organized as follows. Section 2 gives background on reported watermarking and issues. Section 3 introduces the proposed scheme using simple and small-scale quantum circuits. Section 4 is devoted to the simulation-based experiments and analysis. Finally, the conclusion is drawn in Sect. 5.

2 Background on reported watermarking and issues

In this section, we introduce an overview of watermarking, the quantum image representation and the issues on reported quantum watermarking scheme.

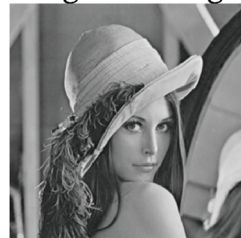
2.1 Reported quantum watermarking scheme using FRQI

Watermarking is becoming necessary components of commercial multimedia applications that are subject to illegal use. In the information protection technology, cryptography is well known (see Fig. 1). While cryptography transforms an image to a meaningless form, watermarking outputs some meaningful form, that is, the watermarked image (see Fig. 2). Watermarking for gray-scale images needs so enormous computation. Quantum-mechanical systems have an information-processing capability much greater than that of corresponding classical systems and could thus potentially be used to implement a new type of powerful computer, that is, quantum computer.

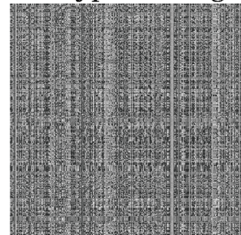
In image processing on quantum computers, the image is represented by using qubits. As one of representations, a FRQI has been proposed [8]. It provides a repre-

Fig. 1 Cryptography

Original Image



Encrypted Image



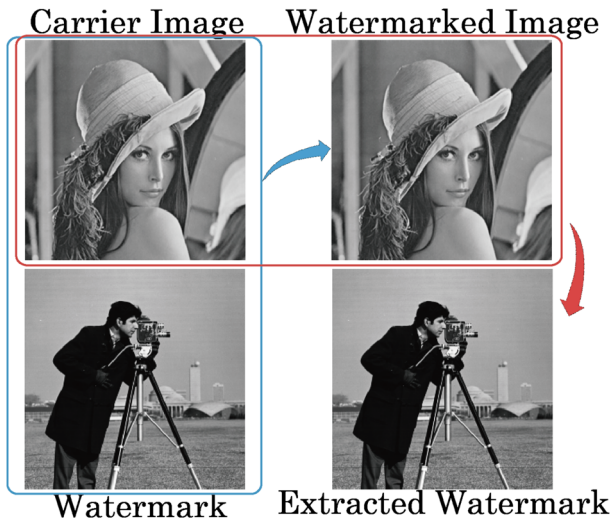


Fig. 2 Watermarking

sentation for images on quantum computers in the form of a normalized state which captures information about gray-scale values and their corresponding positions in the images [9].

Several quantum watermarking schemes using the FRQI has been proposed [10–12]. In these schemes, the complex quantum circuits such as QFT [10], QWT [11], and Hadamard transform [12] are utilized.

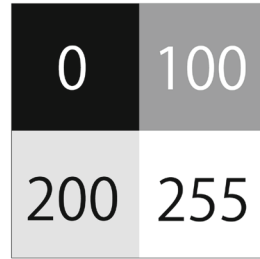
The quantum watermark strategy for quantum images based on quantum Fourier transform [10] is aimed to embed the watermark image into the Fourier coefficients of the quantum carrier image without affecting the carrier images visual effect. However, it is pointed out that the protocol is not clearly described, several steps are ambiguous, and the watermarking algorithm is incorrect [13].

The dynamic watermarking scheme for quantum images using quantum wavelet transform [11] is aimed to embed the watermark image into the wavelet coefficients of the quantum carrier image. However, it is pointed out that the key procedures of the protocol are wrong [14].

Dynamic watermarking scheme for quantum images based on Hadamard transform is also proposed [12]. It is pointed out that the watermarking scheme has the similar defects with another watermarking scheme based on QWT also proposed and that the key procedures during the watermark embedding and extracting are incorrect [15].

Any quantum computer requires a system with long-lived quantum states and a way to interact them. Typically, systems comprised of a number of two-state sub-systems, which are called qubits, are considered. The implementations of quantum computers share a much higher susceptibility to errors than modern classical computers. Entangled states are in general very delicate, and making a measurement on one will typically collapse it into a less entangled state. Small interactions with the environment provide a sort of continuous measurement of a system, and as the system

Fig. 3 2×2 , 256-level image and its NEQR representation



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

grows in size, these become harder and harder to ignore. The system will decohere and begin to look like a classical system. Reducing interactions with the environment can reduce the effects of decoherence, but not eliminate them entirely. Even if the basal error rate in a quantum computer can be reduced to some small value ϵ per unit time, after N time steps, the probability of surviving without an error is only $(1 - \epsilon)^N$, which decreases exponentially with N [17]. It is desirable to implement the watermarking by using simple and small-scale quantum circuits, though the error-correcting codes are considered.

2.2 Novel enhanced quantum representation (NEQR) of digital images

As an alternative to the FRQI, the NEQR have been proposed [9]. While the FRQI encodes a gray-scale value of 8 bits in 1 qubit, the NEQR represents it in a binary string of 8 qubits.

In the NEQR representation, the gray-scale image $f(Y, X)$ with $n \times n$ pixels is expressed by the following equation.

$$\begin{aligned}
 |I\rangle &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |f(Y, X)\rangle|YX\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \bigotimes_{i=0}^{q-1} |C_{YX}^i\rangle|YX\rangle \\
 f(Y, X) &= C_{YX}^0 C_{YX}^1 \dots C_{YX}^{q-2} C_{YX}^{q-1}, \quad C_{YX}^k \in [0, 1], \quad f(Y, X) \in [0, 2^q - 1] \quad (1)
 \end{aligned}$$

In order to explain our proposed scheme, we use a small image with 2×2 pixels as an example image. Figure 3 shows an example image and its NEQR representation. The range of gray scale is from 0 to 255.

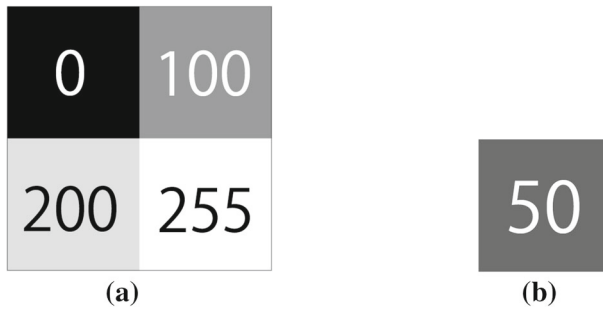


Fig. 4 **a** 2×2 Carrier image, **b** 1×1 watermark

2.3 Reported quantum watermarking (steganography) scheme using NEQR

Quantum image watermarking (image steganography technique) using NEQR has been reported [16]. The embedding algorithm begins with choosing an initial Moiré grating, i.e. a stochastic image, as the carrier image. Then deform the initial Moiré grating according to the secret binary image and the deformed Moiré grating is the Moiré pattern. Finally, alter the Moiré pattern to get the stego-image. The extraction algorithm is employed to regain the secret image by manipulating the initial Moiré grating and the watermarked image. Thus, the proposed steganography algorithm and the corresponding quantum circuits hide a binary image into a gray-scale image.

A watermarking scheme using the NEQR, which hides a secret gray-scale image to the carrier gray-scale image, is required.

3 Proposed scheme

We propose a quantum image watermarking scheme (a watermarking algorithm and corresponding quantum circuits) using the NEQR representation, which hides a gray-scale image (a secret gray-scale watermark image) into a gray-scale image (a carrier gray-scale image). We assume that the image sizes for carrier and watermark are $2n \times 2n$ and $n \times n$, respectively.

In order to explain the scheme, we use a small carrier image (2×2 pixels) and a small watermark (secret) image (1×1 pixel) as shown in Fig. 4.

3.1 Embedding procedure

Proposed embedding procedure is as follows (see Fig. 5a).

1. Transform a classical carrier image with $2n \times 2n$ image size and 8 bits gray scale into a quantum image in the NEQR representation $|C\rangle$,
2. Expand a classical watermark with $n \times n$ image size and 8 bits gray scale to an image with $2n \times 2n$ image size and 2 bits gray scale (see Fig. 6). An 8 bits string is divided into four 2 bits strings,

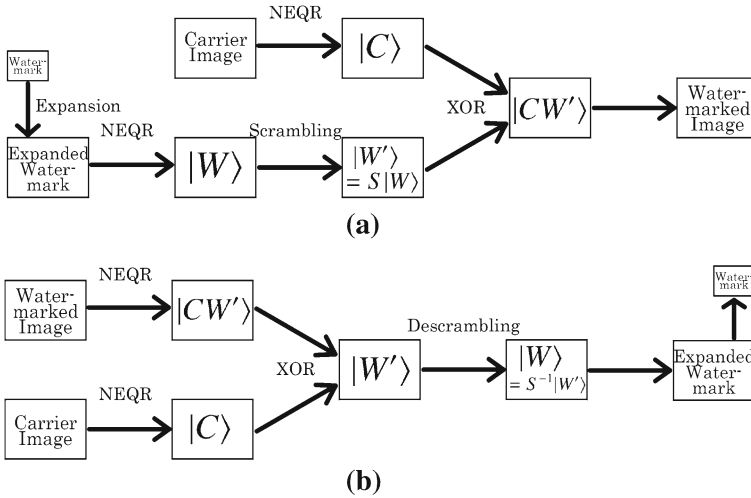
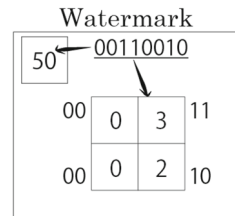


Fig. 5 Procedure of proposed scheme: **a** embedding and **b** extraction procedures

Fig. 6 Expanding $n \times n$ watermark to $2n \times 2n$ image ($n = 1$ in the figure)



3. Transform the expanded watermark image into a quantum image in the NEQR representation $|W\rangle$,
4. Scramble the image $|W\rangle$ to be a meaningless image $|W'\rangle$ by using the keys only known to the operator,
5. Execute XOR between $|C\rangle$ and $|W'\rangle$ in order to obtain $|CW'\rangle$,
6. Transform the $|CW'\rangle$ into a classical digital watermarked image.

3.1.1 Transformation of a carrier image and a watermark to quantum images

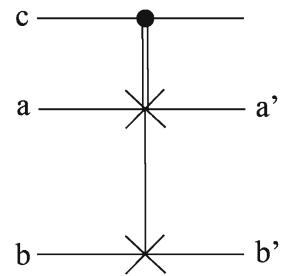
The carrier image is transformed into the quantum image in the NEQR representation as shown in Eq. 1.

The watermark image with $n \times n$ image size and 8 bits gray scale is firstly expanded to an image with $2n \times 2n$ image size and 2 bits gray scale (an 8 bits string is divided into four 2 bits strings). Then the expanded image is transformed into the quantum image in the NEQR representation.

For example, the watermark image with 1×1 image size and 8 bits gray scale is expanded to the image with 2×2 image size as shown in Fig. 6. Since the value of gray scale 50 is expressed as $(00110010)_2$ in 8 bits, the expanded image consists of four

Table 2 Truth table for SWAP

c	a	b	a'	b'
0	0	0	0	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	1

Fig. 7 Icon for SWAP

pixels with $(00)_2$, $(11)_2$, $(00)_2$, $(10)_2$, respectively (see Fig. 6). Then the following NEQR representation is obtained.

$$\begin{aligned}
 |W\rangle &= \frac{1}{2} (|00\rangle|00\rangle + |11\rangle|01\rangle + |00\rangle|10\rangle + |10\rangle|11\rangle) \\
 &= \frac{1}{2} (|(0)_{10}\rangle|00\rangle + |(3)_{10}\rangle|01\rangle + |(0)_{10}\rangle|10\rangle + |(2)_{10}\rangle|11\rangle) \quad (2)
 \end{aligned}$$

3.1.2 Scrambling for watermarking

In order to enhance the confidentiality, we adapt two-step process. In the first step, a watermark with $n \times n$ image size and 8 bits gray scale is expanded to an image with $2n \times 2n$ image size and 2 bits gray scale as shown in Fig. 6. In the second step, the expanded watermark is scrambled by using the controlled SWAP gates. The controlled 2-input/2-output SWAP gate simply exchanges the bit values controlled by the value of the first bit. Its truth table is shown in Table 2. The circuit icon for the SWAP gate is shown in Fig. 7

Figure 8 shows a quantum circuit for scrambling which consists of the controlled SWAP gate. The two position states $|Y_i\rangle$ and $|X_{n-1-i}\rangle$ are connected to two inputs of the SWAP gate, respectively. When the control input to the SWAP gate is set at 1, the gate exchanges the position states.

The control inputs are connected to KEY sequence. When $k_i = 1$ and the others are 0 in $[\text{KEY}] = [k_0 k_1 \dots k_{n-2} k_{n-1}]$, the SWAP gate exchanges $|Y_i\rangle$ and $|X_{n-1-i}\rangle$.

Fig. 8 Scrambling of a watermark using SWAP gates

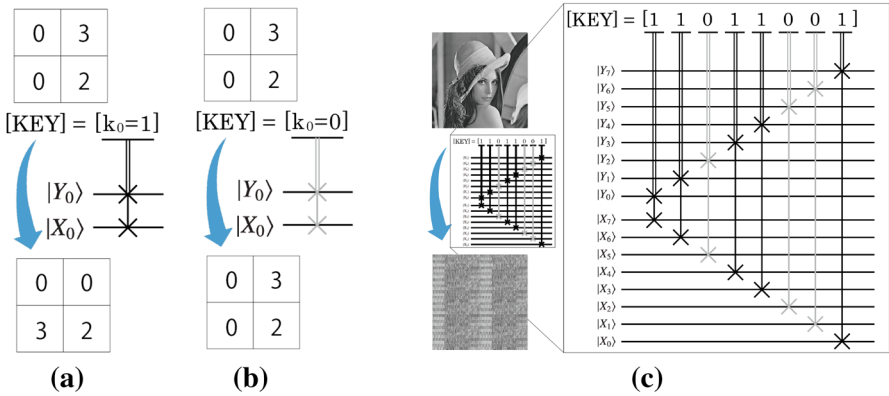
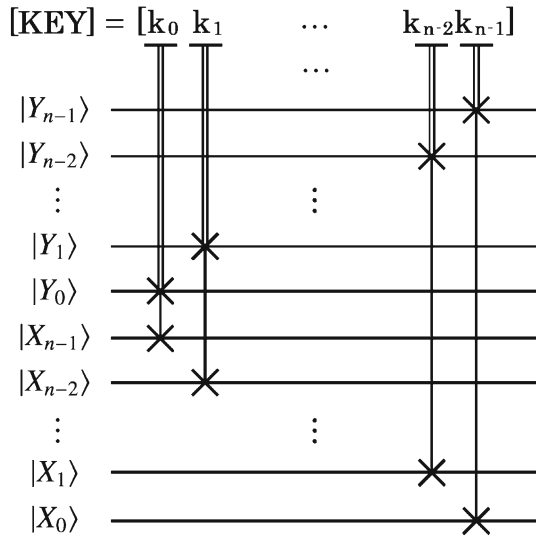


Fig. 9 Examples of scrambling **a** 2×2 image with $k_0 = 1$, **b** 2×2 image with $k_0 = 0$, and **c** 256×256 Lena with $[KEY] = [11011001]$

Fig. 9 shows examples of scrambling. (a) and (b) are for a small image with 2×2 size, and (c) is for an image with 256×256 where the KEY sequence is $[11011001]$.

If we define an operator S which carries out scrambling, scrambling a watermark $|W\rangle$ can be represented as follows.

$$|W'\rangle = S|W\rangle \tag{3}$$

For example, the operation for Fig. 9a can be expressed as

$$S = I^{\otimes 2} \otimes \text{SWAP},$$

$$|W'\rangle = S|W\rangle$$

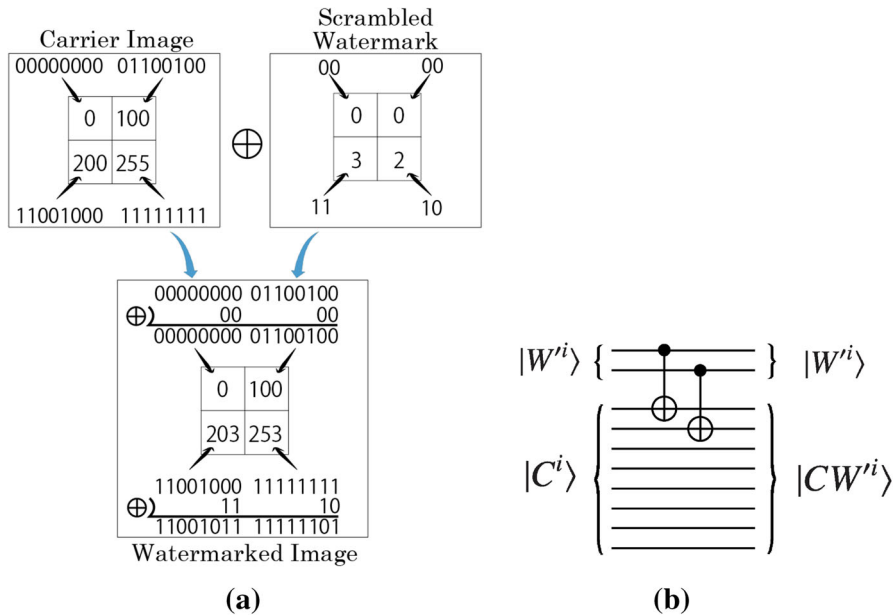


Fig. 10 Embedding of a watermark by XOR. **a** XOR between a carrier image and a watermark, **b** XOR substituted by CNOT

Table 3 Truth table for CNOT

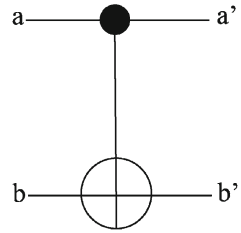
a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\begin{aligned}
 &= (I^{\otimes 2} \otimes \text{SWAP}) \cdot \frac{1}{2} \left(|00\rangle|00\rangle + |11\rangle|01\rangle + |00\rangle|10\rangle + |10\rangle|11\rangle \right) \\
 &= \frac{1}{2} \left(|00\rangle|00\rangle + |11\rangle|10\rangle + |00\rangle|01\rangle + |10\rangle|11\rangle \right). \tag{4}
 \end{aligned}$$

3.1.3 Embedding using XOR

A scrambled watermark $|W'\rangle$ is embedded into a carrier image $|C\rangle$. This operation is carried out by the XOR operation between the lowest 2 qubits of $|C\rangle$ and $|W'\rangle$ as shown in Fig. 10a. The XOR operation on a classical computer is equivalent to the CNOT operation on a quantum computer. The truth table for CNOT is shown in Table 3. The circuit icon for CNOT gate is shown in Fig. 11. Figure 10b shows the quantum circuit for embedding.

Fig. 11 Icon for CNOT



3.2 Extraction procedure

Extraction procedure is as follows (see Fig. 5b).

1. Transform a classical watermarked image and a carrier image into the NEQR representation, $|CW'\rangle$, $|C\rangle$, respectively,
2. Execute the XOR operation between $|CW'\rangle$ and $|C\rangle$ in order to obtain $|W'\rangle$,
3. Descramble $|W'\rangle$ by using private key [KEY] in order to obtain $|W\rangle (= S^{-1}|W'\rangle)$,
4. Transform the $|W\rangle$ into a classical watermark image.

4 Simulation-based experiments and analysis

This section gives some simulation-based experiments and analysis of the results and performance of the proposed watermarking scheme. All experiments are simulated on the MATLAB R2013a.

Three images “Lena”, “mandrill”, and “cameraman” are used in the experiments as carrier images and watermark images. The image sizes for carrier and watermark are 256×256 and 128×128 , respectively.

4.1 Visual quality

We evaluate the watermarked image quality by using PSNR (Peak signal-to-noise ratio) as defined in the following equation.

$$\text{PSNR} = 10 \log_{10} \frac{\text{MAX}_I^2}{\text{MSE}} \tag{5}$$

$$= 20 \log_{10} \frac{\text{MAX}_I}{\sqrt{\text{MSE}}}, \tag{6}$$

where MAX_I is the maximum possible gray-level value of the image. MSE is the mean squared error for two $n \times n$ gray-scale images, a carrier image (or watermark) I and its watermarked version (or extracted watermark) O , as defined in the following equation.

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



Fig. 12 Example of proposed scheme (carrier image: Lena watermark: mandrill), **a** watermark, **b** carrier image, **c** watermarked image, PSNR = 43.85 **d** extracted watermark PSNR = Inf

Table 4 Evaluation of similarity of watermarked images in proposed scheme (PSNR [dB])

Carrier image	Watermark		
	Lena	Mandrill	Cameraman
Lena	–	43.85	43.88
Mandrill	44.16	–	44.05
Cameraman	44.17	44.05	–

The more the watermarked image resembles its carrier image, the more the value of PSNR increases.

One of experimental results is shown in Fig. 12 where “Lena” with 256×256 and “mandrill” with 128×128 are used as the carrier and the watermark images, respectively. The visual quality of the watermarked image was obtained as 43.85 dB. Table 4 shows the visual quality of the watermarked images for all combinations of three images. It is seen from Table 4 that the visual quality is around 44 dB. Therefore, we can conclude that the PSNR in our scheme is obviously higher than that (around 30 dB) in [16].

4.2 Robustness performance under noises

In a noiseless environment, our proposed scheme can extract an error-free watermark image. However, the extraction procedure of a watermark is not always carried out in a noiseless environment. The robustness of the proposed quantum steganography method under the salt and pepper noise is analyzed in [16]. Here we compare the robustness of our proposed scheme under noises to the steganography approach using the same NEQR representation [16].

In the experiment, Fig. 13a, b were used as the carrier image (monotonic) and the watermark [white (gray level 255) and black (0)] image for our proposed scheme, respectively. For the steganography approach, Fig. 13a was used as the watermark (white and black) image, since the approach needs the secret image with the same size.

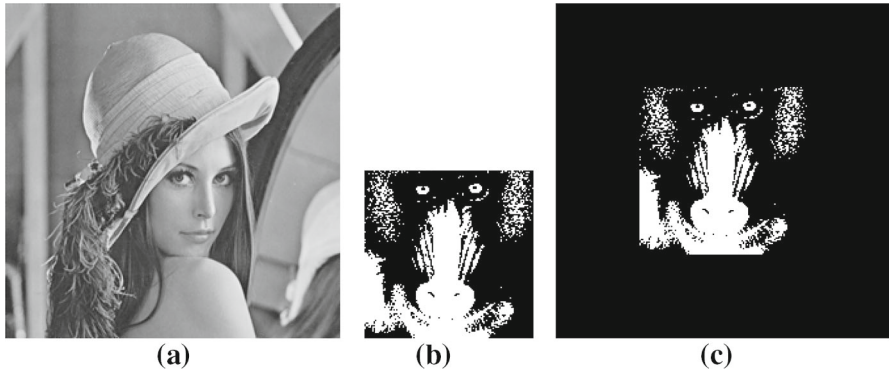


Fig. 13 Images for robustness performance under noises: **a** carrier image, **b** watermark (white and black) for proposed scheme, and **c** watermark for steganography [16]

Table 5 Salt and pepper noise tolerance of extracted watermark (PSNR [dB])

Scheme	Noise density			
	0	0.05	0.10	0.15
Jiang et al. [16]	Inf	15.03	12.15	10.20
Proposed scheme	Inf	19.30	16.34	14.37

Salt and pepper noises are applied with different density of from 0 to 0.15 into 256×256 “Lena” watermarked images as shown in Fig. 14. The corresponding extracted results from the watermarked images with noises are shown in Fig. 14 and in Table 5. It is seen from these figures and Table 5 that the value of PSNR in our scheme is obviously higher than that even under noises.

The reason is considered as follows. In the steganography approach [16], when the gray level of pixel in the watermarked image is coincident with that in the same position of carrier image, the pixel is extracted to be a “black” pixel in the watermark image. Then the watermark image is affected by noises. On the other hand, in our proposed scheme, one pixel with 8 bits gray level in the watermark is expanded into four pixels with 2 bits gray scale and then these gray levels are embedded into the watermarked image. Then the noise effect is suppressed.

Furthermore, in our proposed scheme, many errors included in the extracted watermark image can be corrected easily on a classical computer. The salt and pepper noise affects the gray level (8 bits) of each pixel in the watermarked image. However, in the embedded watermark image, it gives the effect on only 2 bits in 8 bits that represents the gray level of a pixel. Thus, the errors (8 bit scale) in the extracted watermark image is corrected by majority vote based on the digit 0 and 1 that represent the 8 bits gray level when the noise density is low. For example, $(11000000)_2$ is corrected as $(00000000)_2$. We applied the error correction method to the extracted watermark images in Fig. 14. Results are shown in Fig. 15. The values of PSNR for noise densities 0.05, 0.1, and 0.15 were 26.96, 22.14, and 18.34, respectively. It is seen that the error correction method is effective.

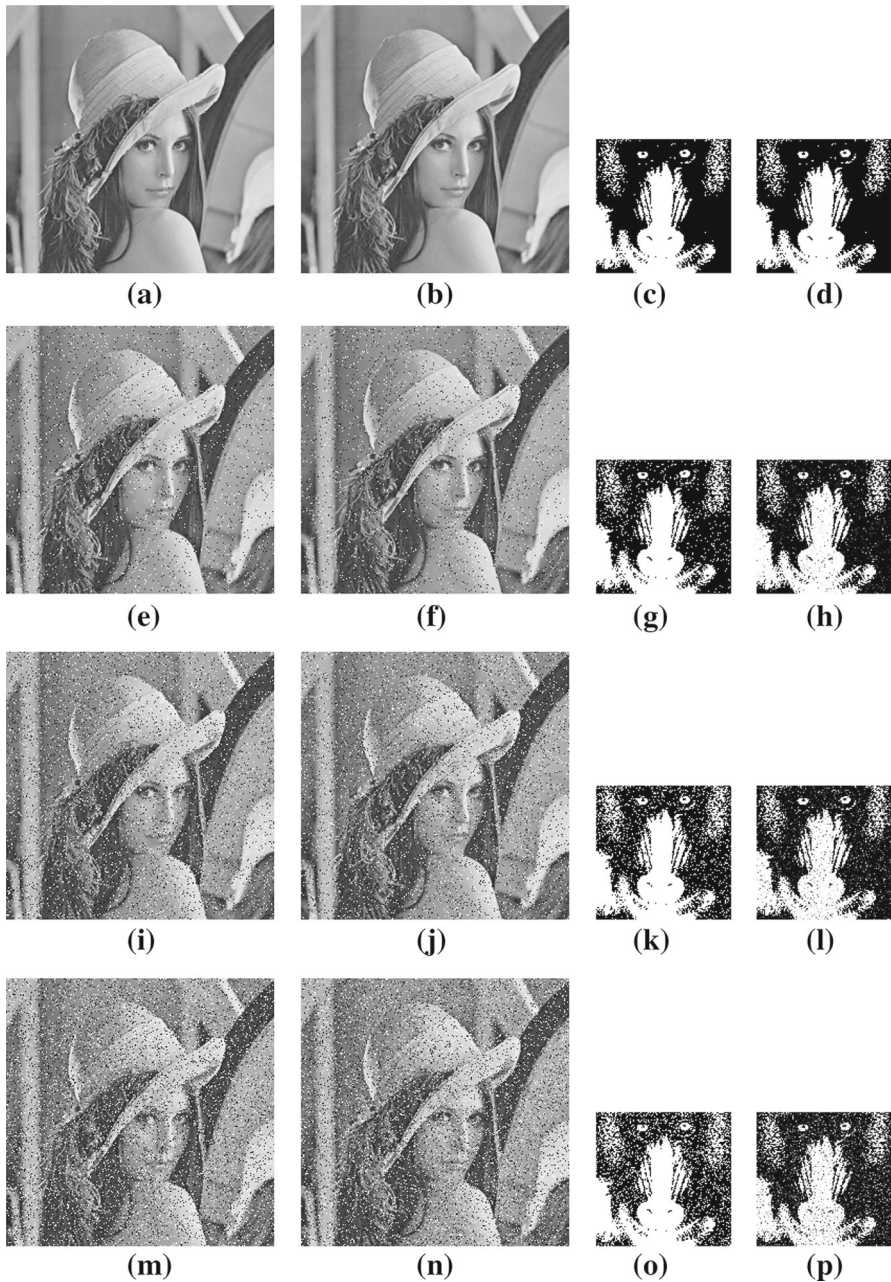


Fig. 14 Robustness performance under noises: on the each row from left to right, watermarked image in [16], watermarked image in proposed scheme, extracted watermark in [16], and extracted watermark in proposed scheme. Noise densities are (a–d) density=0, (e–h) density=0.05, (i–l) density=0.10, (m–p) density=0.15. **a** PSNR=32.73, **b** PSNR=45.20, **c** PSNR=Inf, **d** PSNR=Inf, **e** PSNR=18.25, **f** PSNR=18.44, **g** PSNR=15.03, **h** PSNR=19.30, **i** PSNR=15.41, **j** PSNR=15.48, **k** PSNR=12.15, **l** PSNR=16.34, **m** PSNR=13.59, **n** PSNR=13.67, **o** PSNR=10.20, **p** PSNR=14.37

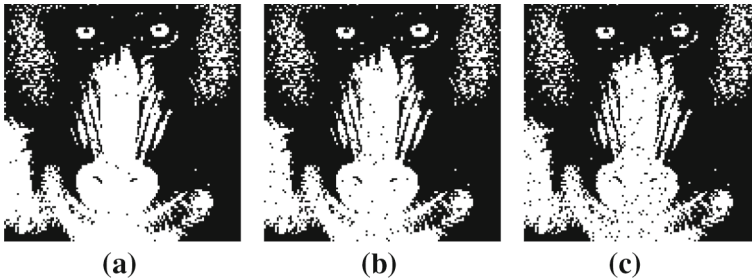


Fig. 15 Error correction for the extracted watermark images. **a** Figure 14h with density 0.05, **b** Fig. 14l with density 0.10, **c** Fig. 14p with density 0.15

4.3 Computational complexity

We discuss the computational complexity by comparing with that of the steganography approach using the same NEQR representation [16].

Here, though we neglect the complexity of the preparation for NEQR, that for NEQR is $\mathcal{O}(nq2^{2n})$. [9] On the other hand, the complexity for FRQI is $\mathcal{O}(2^{4n})$ [8, 9]. Thus the NEQR preparation is faster than that for FRQI.

In our proposed scheme, n SWAP gates for scrambling (Fig.8) and 2 CNOT gates for embedding (Fig. 10b) are required. The total number of gates are $n + 2$. On the other hand, the steganography approach [16] needs $3q + 2$ gates in total. “ q ” is the number of qubits for gray levels. Usually, $n = 8$ (256×256 size) and $q = 8$ are used. Thus our proposed scheme has lower complexity than that for the steganography.

In order to implement our proposed scheme in a classical computer, two 2-input multiplexers and one XOR gate are required for one controlled SWAP gate and one CNOT gate, respectively. In order to process one image with size $2^n \times 2^n$, the number of required gates are $2 \times 2^n \times 2^n = 2^{(2n+1)}$ for 2-input multiplexers and $1 \times 2^n \times 2^n = 2^{2n}$ for XOR gates, respectively. Thus the complexity is very low for quantum computing.

5 Conclusion

We propose a new quantum gray-scale image watermarking scheme by using simple and small-scale quantum circuits where the NEQR representation is utilized. We assume that the image sizes for carrier and watermark are $2n \times 2n$ and $n \times n$, respectively.

Proposed embedding procedure mainly consists of three steps. At first, a classical watermark with $n \times n$ image size and 8 bits gray scale is expanded to an image with $2n \times 2n$ image size and 2 bits gray scale. Then the expanded image is scrambled to be a meaningless image by the controlled SWAP gates. These SWAP gates are controlled by the keys only known to the operator. Lastly, the scrambled image is embedded into the carrier image by the CNOT gates (XOR operation). Extraction procedure mainly consists of two steps. At first, the scrambled image is extracted from the watermarked image and the carrier image by the CNOT gates. Then the scramble image is descrambled by using the private key in order to obtain the watermark.

We carried out simulation-based experiments in order to compare our proposed scheme with the steganography approach using the same NEQR representation [16] in terms of three items, visual quality, robustness performance under noises, and computational complexity. In any of the items, results show that our proposed scheme is excellent.

Next challenge is to extend our proposed watermarking scheme into that using the stabilizer formalism where the robustness performance under noises is enhanced.

References

1. Gea-Banacloche, J.: Hiding messages in quantum data. *J. Math. Phys.* **43**(9), 4531–4536 (2002)
2. Martin, K.: Secure communication without encryption? *IEEE Secur. Priv.* **5**(2), 68–71 (2007)
3. Mogos, G.: A quantum way to data hiding. *Int. J. Multimed. Ubiquitous Eng.* **4**(2), 13–20 (2009)
4. Ilyyasu, A.M., Le, P.Q., Dong, F., Hirota, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. *Inf. Sci.* **186**(1), 126–149 (2012)
5. Ilyyasu, A.M., Le, Q.P., HIROTA, K., et al.: Restricted geometric transformation and their applications for quantum image watermarking and authentication. In: *Asian Conference on Quantum Information Science 2010 (AQIS2010)*, pp. 96–97 (2010)
6. Shaw, B.A., Brun, T.A.: Quantum steganography with noisy quantum channels. *Phys. Rev. A* **83**(2), 022310-1–022310-8 (2011)
7. Williams, C.P.: *Explorations in Quantum Computing*, 2nd edn. Springer, London (2011)
8. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Inf. Process.* **10**(1), 63–84 (2011)
9. Zhang, Y., Lu, K., Gao, Y., Wang, M.: NEQR: a novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **12**(8), 2833–2860 (2013)
10. Zhang, W.W., Gao, F., Liu, B., Wen, Q.Y., Chen, H.: A watermark strategy for quantum images based on quantum Fourier transform. *Quantum Inf. Process.* **12**(2), 793–803 (2013)
11. Song, X.H., Wang, S., Liu, S., El-Latif, A.A.A., Niu, X.M.: A dynamic watermarking scheme for quantum images using quantum wavelet transform. *Quantum Inf. Process.* **12**(12), 3689–3706 (2013)
12. 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)
13. Yang, Y.G., Jia, X., Xu, P., Tian, J.: Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform. *Quantum Inf. Process.* **12**(8), 2765–2769 (2013)
14. Yang, Y.G., Xu, P., Tian, J., Zhang, H.: Analysis and improvement of the dynamic watermarking scheme for quantum images using quantum wavelet transform. *Quantum Inf. Process.* **13**(9), 1931–1936 (2014)
15. Yang, Y.G., Wang, Y., Zhao, Q.Q.: Letter to the Editor regarding Dynamic watermarking scheme for quantum images based on Hadamard transform by Song et al. *Multimed. Syst.* **20**(4), 379–388 (2014)
16. Jiang, N., Wang, L.: A novel strategy for quantum image steganography based on Moiré pattern. *Int. J. Theor. Phys.* **54**, 1021–1032 (2015)
17. Gottesman, D.: *Stabilizer Codes and Quantum Error Correction*. Ph.D. Thesis, California, Institute of Technology, Pasadena, California (1997). [arXiv:quant-ph/9705052](https://arxiv.org/abs/quant-ph/9705052)