RESEARCH ARTICLE OPEN ACCESS

A Secure and Novel Quantum Watermark Strategy

HaoLi[1]
[1](College of information science and technology, Jinan University, Guangzhou, China)

----------**********----------

Abstract:

The current development of classic computers is close to the limit. Therefore, it is necessary to study quantum computers.Although quantum computers do not exist yet, it is conceivable that on quantum computers, there is still a lot of information waiting to be processed.To ensure the security of information on quantum computers, watermarking is a good security strategy.This paper will present a novel watermarking strategy for quantum images.The sender first uses the NEQR quantum image expression to express the quantum image, then changes the carrier image and embeds the watermark by two keys, and the receiver extracts the watermark through these two keys.The experimental simulation results show that the scheme can successfully complete the process of embedding and extracting watermarks.

Keywords **—quantum information, NEQR, image watermark, information security**

----------**********----------

I. INTRODUCTION

The rapid development of modern society is inseparable from electronic computers.Since the advent of electronic computers, its performance has been constantly improving.However, due to the existence of Moore's Law[1], electronic computers are destined to not develop without restrictions. When the threshold is reached, the performance of the electronic computer cannot be improved, and there is no more powerful computing ability to cope with more complicated calculations. Therefore, people began to focus their research on quantum computers.Quantum computers have a powerful computing advantage over electronic computers (also known as classic computers)[2].The use of quantum superposition and entanglement principles can reduce the time and space complexity of the runtime.It is obvious that the research on quantum computers has important strategic significance.

Information security issues are considered when dealing with information on classic computers, and similar for quantum computers.Although the quantum computer is unlikely to be developed in the short term, scholars have begun to study quantum information security technology, and have achieved certain results.Information can only be transmitted by relying on the carrier. Currently, more information carriers are used for audio, image and video.Information security technologies for various multimedia carriers have been extensively studied on classical computers.In the field of quantum computers, scholars now mainly study information security technologies on quantum audio and quantum image.Among them, the research results of quantum image information security technology are mostly.

To study quantum image processing technology, we must first select the expression form of quantum image.Common quantum image representations include Entangled Image[3], Real Ke[4], FRQI[5], and NEQR[6]. Currently, FRQI and NEQR are more commonly used.In the field of classical image processing, digital image watermarking is one of the effective strategies to protect image information security.After embedding the watermark into the image, there is no obvious change in the image, so as to achieve the purpose of covert transmission.After the receiver extracts the watermark, it can also determine whether the image

is attacked by detecting the integrity of the watermark.In the field of quantum image processing, quantum image watermarking is also a direction that many people are currently studying.Zhang et al. proposed a quantum image watermarking algorithm based on quantum Fourier transform[7]. Song et al. proposed a quantum image watermarking algorithm based on wavelet transform[8]. Both these two algorithms are established on FRQI.On the NEQR representation, there is the LSB quantum image watermarking algorithm proposed by Jiang et al[9]. The robust watermarking algorithm under the color quantum image proposed by Heidari et al[10]. In addition to the above, there are other quantum image watermarking algorithms[11-13].In conclusion, the present study on quantum image watermark is still evolving.

This paper presents a novel and secure quantum image watermarking algorithm.The carrier image is first represented by NEQR. Then the carrier image is changeby using the key K1. K1 is related to the changing method.When the watermark is embedded, it is not directly embedded in the carrier image.The key K2 controls the method to embed watermark.After the embedding is completed, reverses the image again. Senders transmits the watermarked carrier image and the two keys K1、K2 to receivers.Receivers can extract the watermark by operations in the reverse order of embedding watermark.

II. THEORY BASIS

This chapter mainly introduces some theoretical knowledge.One 2^nx2^n images can be represented by $2n+q$ qubits in NEQR when in classic computers it needs 2^nx2^nbits. Expression of NEQR is:

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle \quad (1)$$

$$|c_i\rangle = |c_i^{q-1}\ldots c_i^1 c_i^0\rangle, \quad c_i^k \in \{0,1\}, k = q-1,\ldots,1,0 \quad (2)$$

$$|i\rangle = |y\rangle|x\rangle = |y_{n-1}y_{n-2}\ldots y_0\rangle \quad |x_{n-1}x_{n-2}\ldots x_0\rangle, |y_i\rangle|x_i\rangle \in \{0,1\} \quad (3)$$

i is coordinate information.x and y represent ordinate and abscissa, each consists of n qubits.c is color information, it can express2^qcolors.When$q$=8, 2^q=256, which is used to represent grayscale image.

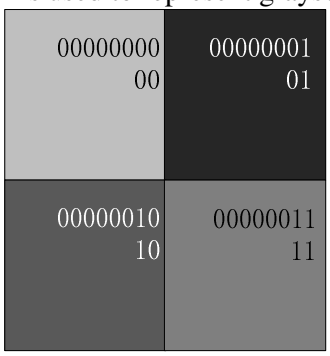

Fig.1 A sample 2x2 NEQR image

Fig.1 is a NEQR image, its expression is:

$$|I\rangle = \frac{1}{2}[|00000000\rangle\otimes|00\rangle] + |00000001\rangle\otimes|01\rangle + |00000010\rangle\otimes|10\rangle + |00000011\rangle\otimes|11\rangle$$

Some quantum logic gates will be used in this article[14].Xor gate (as shown in Fig.2) is used to change 0 to 1 or 1 to 0. SWAP gate(as shown in Fig.3) is used to exchange two values. N-cont gate (as shown in Fig.4) use n qubits to control the inverse process.

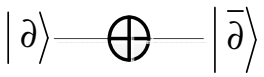

Fig. 2 Xor gate

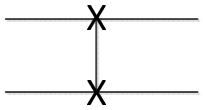

Fig.3 SWAP gate

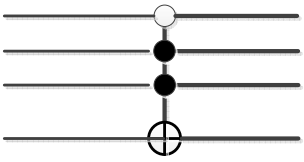

Fig.4 N-cont gate

In Fig.4.there are 3qubits to control the inverse process. Only these 3 qubits' value is"011"excutethe inverse operation.

III. ALGORITHM INTRODUCTION

This chapter introduces the novel and safe quantum image watermarking algorithm proposed in this paper. Fig.5 is the framework of the proposed algorithm.

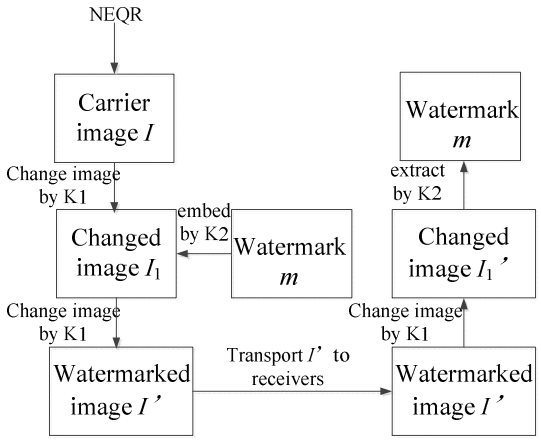

Fig.5 Framework of the proposed algorithm

A. *Watermark embed*

First select an image as a carrier. Then use NEQR to represent this carrier image, *I*is used to expressed this carrier image.In order to ensure the security of the transmission process, the carrier image is changed before the watermark information is embedded. Key K1 is used to control the method to change carrier image *I*. In this algorithm, K1 consists of two qubits. So there are four options for K1, each option corresponds to a different way of changing.Since the value of one qubit is only 0 and 1, four values of the key K1 are 00, 01, 10, 11 respectively.

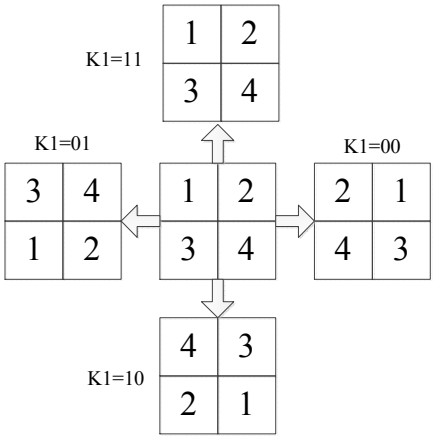

Fig.6 Using K1 to change to image

The method of changing the carrier image corresponding to each value is as shown in Fig.6. An image can be divided into four parts, use 1,2,3,4 to represent these four parts respectively. In Fig.6, the middle square is the original image. It is obvious that the value of K1 control the method of changing. For example, if K1 =00,the first half column and the second half column are interchanged.The corresponding quantum circuit diagram is shown in Fig.7.

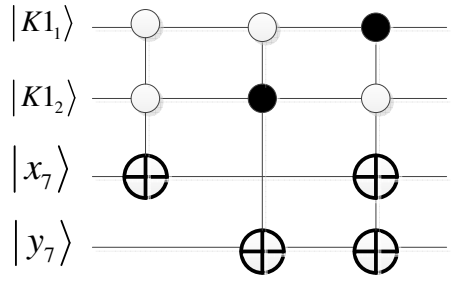

Fig.7 Quantum circuit diagram of changing image

In Fig.7 $K1_1$ and $K1_2$ are used to represent two qubits of K1.Suppose the size of the carrier image is 256x256. 2^8=256.So abscissa and ordinate can be represented by eight qubitsrespectively.Taking the abscissa as an example, the qubit sequence representing the abscissa is *X*, and the order of the eight qubits is $x_7x_6x_5...x_0$. The ordinate is the same.According to the changing method of Fig.6, it is only necessary to operate on x_7 and $y_7$which are representing the highest positions of the abscissa and the ordinate.For example, if K1 =00,the first half column and the second half column are interchanged. Just reverse x_7 if $K1_1$ and $K1_2$are 0. It's similarly when K1=01 or K1=10. If K1=11, the carrier image won't be changed. Therefore, the situation when K1=11 is not listed in the Fig.7.

After changing the carrier image, next step is to embed watermark information *m*. K2 is used to control the method of embedding watermark. K2 consists of two qubits, same as K1. Watermark information is embedded in pixel values. Suppose the carrier image is a grayscalewith size of 256x256. 2^8=256. So the pixel value is represented by eight qubits. Qubit sequence*C* expresses pixel value, and the order of the eight qubits is $c_7c_{6...}c_1c_0$.
$c_0$is the least significant bit(LSB) of pixel value *C*. $c_1$is the second last bit of pixel value *C*. Watermark information *m* is embedded inc_1 orc_0.

K2 consists of two qubits. It has four values: 00,01,10,11. When K2 = 00, watermark information *m*is embedded in c_0. When K2 = 01, inverse c_0 after embedding *m* in c_0.If K2 = 10, embeds *m* in c_1.If K2 = 11, inverse c_1 after embedding *m* in c_1.Fig.8 is the corresponding quantum circuit diagram.

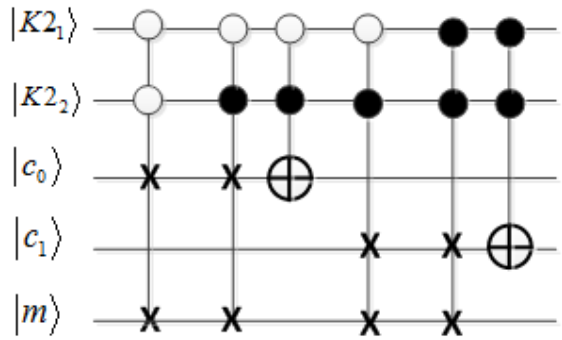

Fig.8Quantum circuit diagram of embedding watermark

In Fig.8 $K2_1$ and $K2_2$ are representing two qubits of K2. When $K2_1$ and $K2_2$have different values, embeds the watermark information *m* withthe corresponding method. Mainly use SWAP gate to embed *m*. Once the values of $K2_1$ and $K2_2$are the required values, execute the exchange operation. After the embedding process, *m* is embedding in c_1 orc_0.

Then use K1 to change the carrier image again to make its order back to its original state. A watermarked image *I'* can be obtained.

B. Watermark extract

The process of extracting watermark is simple. Usually receivers can obtain a watermarked image *I'*and two key K1 and K2. Since the watermark information *m*is embedded in the changed image, the watermark information *m* should be extracted from the changed image.

Therefore, the first step to extract watermark information *m* is to change the watermarked image *I'*by using K1. Changing method is the same with the process of embedding watermark.

Then the watermark information *m* could be extracted by using K2. The method of extracting watermark is similar with the method of embedding watermark. The difference is that the order of execution is the opposite. That means, when embedding watermark, execution order is from left to right in Fig.8.When embedding watermark, execution order is from right to left in Fig.8.

After successfully extracting the watermark information *m*, the entire algorithm is completed.

C. Simulation

This section is an experimental simulation of the algorithm.Since quantum computers are not yet available, simulation experiments can only be performed on classic computers.The experiment is mainly carried out with MATLAB2013. The carrier images are256x256 grayscale image.Binary images are use as watermark information,their size are 256x256. Fig.9 shows the carrier images. Fig.10 shows the watermark iamges.

a).lena b). peppers c).baboon d).barbara

Fig.9 Carrier images

a) b) c)

Fig10 Watermark images

Peak signal to noise ratio (PSNR) is used to evaluate the visual effect of the image. The PSNR is defined by the mean square error (MSE, calculated as (4)), which is calculated as (5).

$$MSE = \frac{1}{\mathrm{m\,n}} \sum_{i=0}^{2^{m-1}} \sum_{j=0}^{2^{n-1}} [(I(i,j) - K(i,j))^2] \quad (4)$$

$$PSNR = 20 \times \log_{10}(\frac{MAX_I}{\sqrt{MSE}}) \quad (5)$$

TABLE I
PSNR OF THE EXPERIMENT

	PSNR with watermark a) embedded	**PSNR with watermark b) embedded**	**PSNR with watermark c) embedded**
a).lena	50.26	52.87	51.46
b). peppers	45.21	44.94	45.67
c). baboon	42.43	42.35	41.95
d).barbara	48.25	48.36	47.86

The experimental PSNR values are shown in Table 1. It's obvious that lena image has the best performance. Baboon image has theworst

performance. The reason is lena image has smooth texture and baboon image has complex texture.Overall, after embedding watermark images, the PSNR values of four carrier imagesare not low. That means carrier imagesare not severely distorted. In addition, extracted watermark images are used to compare with the original. The results show that the two are the same. It is proved that the proposed algorithm can successfully extract the embedded information.

IV. CONCLUSIONS

The development of classic computers has gradually reached the limit. Therefore, researchers are currently interested in quantum computers.This has given birthto many new research topics. Quantum information is one of them.Similar to digital information, quantum information also need to consider about security. This paper proposes aa novel watermarking strategy for quantum images.NEQR is selected as the form of quantum image expression.To ensure security, carrier image need to be changed before embedding watermark. The changing method is controlled by key K1.Then embed watermark by using K2. If someone wants to extract the watermark, both K1 and K2 are needed. This means that even if the carrier image is stolen, without K1 and K2, watermark still won't beextracted. The experimental simulation results show that the proposed scheme can successfullyextract the watermark.

REFERENCES

[1] Moore GE. Cramming more components onto integrated circuits. Proceedings of the IEEE, 1998, 86(1): 82-85.

[2] Feynman R P. Simulating Physics with Computers[J]. International Journal of Theoretical Physics, 1982, 21(6-7):467-488.

[3] Venegas-Andraca SE, Ball JL. Processing images in entangled quantum systems. Kluwer Academic Publishers, 2010,9 (1) :.1-11.

[4] Latorre JI. Image compression and entanglement. Computer Science, 2005.

[5] Le PQ, Dong F, Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Kluwer Academic Publishers, 2011,10 (1) : 63-84.

[6] Zhang Y, Lu K, Gao Y, et al. NEQR: a novel enhanced quantum representation of digital images. Quantum Information Processing, 2013, 12(8): pp.2833-2860.

[7] Zhang WW, Gao F, Liu B, et al.A watermark strategy for quantum images based on quantum Fourier transform. Quantum Information Processing , 2013, 12(4), 793-803.

[8] Song XH, Wang S, Liu S, et al. A dynamic watermarking scheme for quantum images using quantum wavelet transform. Quantum Information Processing, 2013, 12(12),3689-3706

[9] Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. International Journal of Theoretical Physics,2016,55(1): .107-123.

[10] Heidari, S., Gheibi, R., Houshmand, M., Nagata, K.: A Robust Blind Quantum Copyright Protection Method for Colored Images Based on Owner's Signature, International Journal of Theoretical Physics. 2017,56(8), 2562-2578.

[11] Zhang, W., Gao, F., Liu, B., Jia, H.: A Quantum Watermark Protocol. Int. J. Theor. Phys. 2013, 52(2), 504-513.

[12] Heidari, S., Naseri, M.: A Novel LSB Based Quantum Image Watermarking, Int J Theor Phys, 2016, 55(10), 4205-4218.

[13] Iliyasu, A., Le, P., Dong, F., Hitora, K.: Watermarking and authentication of quantum images based on restricted geometric transformations. Inf. Sci. 2012,186(1), 126-149.

[14] Deutsch, D. Quantum Computational Networks[J]. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 1989, 425(1868):73-90.