

Quantum watermarking based on threshold segmentation using quantum informational entropy

Jia Luo(罗佳), Ri-Gui Zhou(周日贵), Wen-Wen Hu(胡文文), YaoChong Li(李尧翀), and Gao-Feng Luo(罗高峰)
Citation: Chin. Phys. B, 2022, 31 (**4**): 040302. DOI: 10.1088/1674-1056/ac2803
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Quantum simulation of lattice gauge theories on superconducting circuits: Quantum phase transition and quench dynamics

Zi-Yong Ge(葛自勇), Rui-Zhen Huang(黄瑞珍), Zi-Yang Meng(孟子杨), and Heng Fan(范桁)
Chin. Phys. B, 2022, 31 (**2**): 020304. DOI: 10.1088/1674-1056/ac380e

Fast qubit initialization in a superconducting circuit

Tianqi Huang(黄天棋), Wen Zheng(郑文), Shuqing Song(宋树清), Yuqian Dong(董煜倩), Xiaopei Yang(杨晓沛), Zhikun Han(韩志坤), Dong Lan(兰栋), and Xinsheng Tan(谭新生)
Chin. Phys. B, 2021, 30 (**7**): 070310. DOI: 10.1088/1674-1056/abff2b

Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme

Jing-Wen Zhang(张静文), Xiu-Bo Chen(陈秀波), Gang Xu(徐刚), and Yi-Xian Yang(杨义先)
Chin. Phys. B, 2021, 30 (**7**): 070309. DOI: 10.1088/1674-1056/ac003b

Universal quantum control based on parametric modulation in superconducting circuits

Dan-Yu Li(李丹宇), Ji Chu(储继), Wen Zheng(郑文), Dong Lan(兰栋), Jie Zhao(赵杰), Shao-Xiong Li(李邵雄), Xin-Sheng Tan(谭新生), and Yang Yu(于扬)
Chin. Phys. B, 2021, 30 (**7**): 070308. DOI: 10.1088/1674-1056/ac01c3

Interaction induced non-reciprocal three-level quantum transport

Sai Li(李赛), Tao Chen(陈涛), Jia Liu(刘佳), and Zheng-Yuan Xue(薛正远)
Chin. Phys. B, 2021, 30 (**6**): 060314. DOI: 10.1088/1674-1056/abee0c

---

Quantum watermarking based on threshold segmentation using quantum informational entropy

Jia Luo(罗佳)[1,2], Ri-Gui Zhou(周日贵)[1,2,†], Wen-Wen Hu(胡文文)[1,2], YaoChong Li(李尧翀)[1,2], and Gao-Feng Luo(罗高峰)[3]

[1] *College of Information Engineering, Shanghai Maritime University, Shanghai* 201306, *China*
[2] *Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai* 201306, *China*
[3] *College of Information Engineering, Shaoyang University, Shaoyang* 422000, *China*

(Received 29 July 2021; revised manuscript received 3 September 2021; accepted manuscript online 18 September 2021)

We propose a new quantum watermarking scheme based on threshold selection using informational entropy of quantum image. The core idea of this scheme is to embed information into object and background of cover image in different ways. First, a threshold method adopting the quantum informational entropy is employed to determine a threshold value. The threshold value can then be further used for segmenting the cover image to a binary image, which is an authentication key for embedding and extraction information. By a careful analysis of the quantum circuits of the scheme, that is, translating into the basic gate sequences which show the low complexity of the scheme. One of the simulation-based experimental results is entropy difference which measures the similarity of two images by calculating the difference in quantum image informational entropy between watermarked image and cover image. Furthermore, the analyses of peak signal-to-noise ratio, histogram and capacity of the scheme are also provided.

Keywords: quantum image watermarking, threshold segmentation, quantum informational entropy, quantum circuit

PACS: 03.67.–a, 03.67.Ac, 03.67.Dd, 03.67.Lx **DOI:** 10.1088/1674-1056/ac2803

1. Introduction

Quantum information processing is an interdisciplinary study that combines information science and quantum physics. The essence of quantum information processing is solving complex problems according to properties of quantum mechanics, which are difficult for classical methods. The most famous application of quantum computing may be the quantum integer factoring algorithm proposed by Shor and Grover's algorithm for search of databases. The former can break the widely used RSA scheme in polynomial time, the latter can achieve quadratic speedup compared to the best classical algorithm.[1] Nowadays, other sub-disciplines complement the content about quantum information processing.[2] These sub-disciplines include an emerging realm, quantum image processing (QImP), which focuses on using quantum computing to solve conventional image processing tasks.

QImP started in 1997, at that time Vlasov[3] proposed an analogue image recognition method of quantum systems. This was followed by Schutzhold's investigation of problems of linear patterns in unstructured picture.[4] In 2003, Beach *et al.*[5] demonstrated that common quantum algorithms are appropriate for image processing tasks, which is generally considered to be the beginning of today's description of QImP. Then, various models of how to store digital images in a quantum computer are proposed, such as qubit lattice,[6] real ket,[7] flexible representation of quantum images (FRQI),[8] a novel enhanced quantum representation of digital images (NEQR),[9] and a representation method for multidimensional color images, called an n-qubit normal arbitrary superposition state (NASS).[10]

Based on these models, the research of QImP has entered a fruitful stage.[11] Various types of quantum image processing tasks have been explored including quantum image scaling,[12–14] recognition,[15] edge detection,[16–18] segmentation,[19,20] and information hiding. A major thrust of current research is the quantum information hiding,[21] which is branched out into two fields, i.e., quantum image watermarking[22–25] and quantum image steganography.[26–30] Their purpose was to conceal secret message in a cover image without causing visual changes, so one must validate the proposed algorithm by some image quality measures. Many researchers are satisfied with employing the peak noise-to-signal ratio (PSNR) to evaluate similarity between quantum images. Moreover, probability-based image similarity measure was researched in Refs. [31,32], and wholly quantum-based image fidelity metric was also discussed in Refs. [33,34].

The scope of this paper is to propose a watermarking scheme based on threshold segmentation using quantum informational entropy. The threshold selection method we shall refer to belongs to the maximum entropy threshold of gray level distribution. The relative deficiency of von Neumann entropy for a pure state impels us to employ the quantum informational entropy proposed in Ref. [35]. The main idea of our scheme

†Corresponding author. E-mail: rgzhou@shmtu.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

is to embed information to the object and the background with different ways using the key obtained by the threshold segmentation of the cover image. Therefore, after the secret message is embedded, the target pixels can be changed less and the normal use of the image will not be affected. Finally, we define a method to measure the similarity of cover image and embedded image using entropy difference.

2. Quantum informational entropy

In quantum information theory, information is stored in the basic unit, the qubit or quantum bit. The most distinct property of a qubit is the existence of superposition, which means that a qubit can be a coherent superposition of both states simultaneously. In classical systems, however, a bit must be in one state or another. Obviously, the storage and processing of information in classical or quantum systems are quite different.

In a quantum system, the measure of informational entropy is also more complex than the classical system. It makes a big difference whether the measurement is adopted in pure or mixed quantum state. In a pure-state quantum system, the state is a coherent superposition of the basis states $|0\rangle$ and $|1\rangle$, which can be described by a point on the surface of Bloch sphere. A mixed state is a statistical combination or incoherent mixture of different pure states, and its entropy can be computed by the von Neumann entropy. However, according to the principle of von Neumann entropy, the entropy of a pure state is always zero.[35]

For the quantum representation of image, for example, the NEQR model is written as

$$\begin{aligned} |I\rangle &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_{YX}\rangle\otimes|YX\rangle \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{j=0}^{q-1}\left|C_{YX}^{j}\right\rangle\otimes|YX\rangle, \end{aligned} \tag{1}$$

where q-qubit subsystem $|C_{YX}\rangle = \left|C_{YX}^{q-1}\cdots C_{YX}^{1}C_{YX}^{0}\right\rangle$, $C_{YX}^{k}\in\{0,1\}$ encodes the grayscale value C_{YX} of the corresponding pixel (Y,X), and the subsystem $|YX\rangle = |y_{n-1}\cdots y_1y_0\rangle|x_{n-1}\cdots x_1x_0\rangle$ represents the information of vertical and horizontal coordinates, respectively. That is, the quantum state of image prepared by NEQR is a pure state. Hence we cannot employ the von Neumann entropy to measure the information of the quantum image.

Consider a quantum system consisting of the sum of its mixed and pure components, which is a combination of pure states $|\phi_i\rangle$ with probabilities p_i and a mixed state with the eigenvalues λ_i of density operator with probability p_0. The composite informational entropy[36] can be given by

$$S_{\mathrm{ci}}(\rho) = -p_0\sum_i\lambda_i\log\lambda_i + \sum_i p_iS_{\mathrm{p}}(\phi_i), \tag{2}$$

where $S_{\mathrm{p}}(\phi)$ indicates the entropy of the pure state $|\phi\rangle = \sum_k c_k|a_k\rangle$:

$$S_{\mathrm{p}}(\phi) = -\sum_k |c_k|^2\log|c_k|^2. \tag{3}$$

Thus, when we consider the case that there is no mixed state and the probability of pure state $|\phi\rangle$ is 1, this happens to be the state of quantum image, the informational entropy of quantum image $|\phi\rangle$ can be calculated by Eq. (3). The measurement experimental results of the grayscale value of every pixel can demonstrate the amplitude of q-qubit subsystem. This makes it possible to simplify the representation of the quantum image to measure the quantum informational entropy of image:

$$|I_{\mathrm{ci}}\rangle = \sum_{k=0}^{2^q-1}\sqrt{p_k}|C_k\rangle, \tag{4}$$

where $|C_k\rangle$ denotes the indices of pixel intensities and $\sqrt{p_k}$ represents its corresponding probability amplitude. Hence the quantum informational entropy of a quantum image $|I\rangle$ can be obtained by considering the function

$$S_I = -\sum_{k=0}^{2^q-1}p_k\log p_k. \tag{5}$$

3. Thresholding segmentation

Thresholding is a process in which an appropriate threshold that transforms all the levels to black or white is selected under some criteria, so as to extract objects from a background.[37] Thus, the pixels of an image are divided into a series of classes according to the following rules:

$$C\in M_i \quad \text{if} \quad t_{i-1}\le C < t_i, \tag{6}$$

where $C\in[0,2^q-1]$ denotes the gray level of image pixels, $\{t_i|i\in[1,N-1]\,\&t_0=0\}$ are the thresholds and $\{M_i|i\in[1,N]\}$ are classes of objects.

The reduced quantum representation of image is shown in Eq. (4), which contains the information about the pixel gray level, as well as their probability amplitude. Thus the informational entropies associated with each class are as follows:

$$S_{\mathrm{p}}(M_i) = -\sum_{j=t_{i-1}+1}^{t_i}q_j\log q_j, \tag{7}$$

where q_j represents the probability of the class and $q_j = p_j/\mu_i$; u_i is the summation of probability of pixels in class M_i, which can be written as

$$\mu_i = \sum_{j=t_{i-1}}^{t_i}p_j, \tag{8}$$

whereas p_j is given by

$$p_j = \left(\sqrt{p_j}\right)^2. \tag{9}$$

Let us define the sum of the entropies of all classes by Eq. (10). Then we maximize $\varphi(S)$ to obtain the maximum information between objects and background distributions in the image, and the set of values t_j is the threshold.

$$\arg\max_t \varphi(S) = \arg\max_t \sum_{i=1}^{N} S_{\mathrm{p}}(M_i). \tag{10}$$

For this study, we assume that only one object is extracted in the image. Now we derive from amplitudes of two categories, one defined for intensity level from 0 to t_1 and the other for intensity level from t_1+1 to 2^q-1. Consequently $\varphi(S)$ to be the discriminant criterion of threshold, we have the relation

$$\begin{aligned}&\arg\max_t (S_{\mathrm{p}}(1)+S_{\mathrm{p}}(2))\\ &= \arg\max_t \left(-\sum_{j=0}^{t_1} q_j \log q_j - \sum_{j=t_1+1}^{2^q-1} q_j \log q_j \right).\end{aligned} \tag{11}$$

According to the methods mentioned above, the quantum image threshold procedure is shown in Algorithm 1.

ALGORITHM 1 Quantum image threshold

Input: The reduced quantum representation $|I_{CI}\rangle$
Output: the threshold value t
for $t = 0,1,\ldots,2^q-1$ do
μ_1 = total probability of 0 to and μ_2 = total probability of $t+1$ to 2^q-1
$q_j = \sqrt{p_j}^2/\mu_{1 \text{ or } 2}$ is the probability distribution in class
calculate the informational entropies of two classes:
for $j = 0,1,\ldots,t$ do
    $S_{\mathrm{p}}(1) = S_{\mathrm{p}}(1) + (-q_j \log q_j)$
end for
for $j = t+1, t+2, \ldots, 2^q-1$ do
    $S_{\mathrm{p}}(2) = S_{\mathrm{p}}(2) + (-q_j \log q_j)$
end for
discriminant criterion is the sum of two entropies, that is , $\varphi(S)$
end for
maximize $\varphi(S)$ and obtain the threshold t

4. Watermarking scheme

As discussed above, having computed the threshold value of the quantum image, it can be used in the segmentation-based watermarking process in order to find a suitable authentication key. In this section, we will show how the key is prepared. Then the proposed scheme and algorithms for the embedding phase and the extraction phase are described detailedly.

4.1. Authentication key

The information is embedded to cover image using the authentication key that is later used for the recovery process too. As we can see in Section 3, the threshold t derived from the quantum informational entropy is acquired. On this basis, the authentication key is prepared as follows:

Step 1 Consider a cover image and calculate the threshold t.

Since the authentication key is determined by the object and background of the cover image, we need choose a cover image firstly. Then, by adopting Algorithm 1, the threshold t of partitioning the image to two parts is obtained.

Step 2 Depending on the threshold, one can construct the authentication key.

In order to embed the information using the key, it must be first constructed it into a Boolean-valued one. Let us define a Boolean function B, whose mathematical formula is

$$B(C,t) = \begin{cases} 1, & \text{if } t \le C_{YX}, \\ 0, & \text{if } t > C_{YX}. \end{cases} \tag{12}$$

For a given gray value C_{YX}, the Boolean value of 1 represents that this pixel belongs to object. Similarly, the Boolean value of pixel to be 0 represents the background.

After applying the Boolean function to all the pixels in the cover image, the authentication key $|\mathrm{Key}\rangle$ is formed as follows:

$$|\mathrm{Key}\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |B\rangle \otimes |YX\rangle, \tag{13}$$

where $|YX\rangle$ and $|B\rangle$ denote the pixel position and Boolean value, respectively.

4.2. Embedding procedure

We can summarize the steps required to embed the watermark information onto a cover (original) image into two parts:

(1) The compound step, which is combining the cover image, the information image and the authentication key.

(2) The watermark embedding circuit generation step, wherein the appropriate embedding circuit is designed to realize the content of embedding algorithm.

In the former part of the procedure, the main consideration is the combination of subsystems about color information.

Assume that the secret information is a binary image and defined as

$$|\text{Infor}\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f\rangle\otimes|YX\rangle. \tag{14}$$

Accordingly, the composite system $|\text{CIK}\rangle$ can consist of q-qubit sequence gray value of cover image, one-qubit binary value of information image, one-qubit Boolean value of the key and $2n$-qubit of the position, that is, $|C_{YX}\rangle$, $|f\rangle$, $|B\rangle$ and $|YX\rangle$, respectively. From the representation of NEQR, $2n+q+2$ qubits are needed to construct the composite system.

The first step is preparing $2n+q+2$ qubits that are set as zero. The initial state is expressed as

$$|\psi\rangle_0 = |0\rangle^{2n+q+2}. \tag{15}$$

Then, two single-qubit matrices, identity matrix and Hadamard matrix in the following equation are used to transform $|\psi\rangle_0$ to the intermediate state $|\psi\rangle_1$, which has zero value in all positions:

$$I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \tag{16}$$

The operation of this process can be written as U_1 in

$$U_1 = I^{\otimes q+2}\otimes H^{\otimes 2n}. \tag{17}$$

The operator U_1 is applied to the initial state, so we obtain the intermediate state with position information,

$$\begin{aligned}U_1(|\psi\rangle_0) &= (I|0\rangle)^{\otimes q+2}\otimes(H|0\rangle)^{\otimes 2n}\\ &= \frac{1}{2^n}|0\rangle^{\otimes q+2}\otimes\sum_{i=0}^{2^{2n}-1}|i\rangle\\ &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}|0\rangle^{\otimes q+2}|ji\rangle = |\psi\rangle_1.\end{aligned} \tag{18}$$

Next, let us to set the three values for every pixel. The value-setting matrices, U_{YX}, with $Y,X = 0,1,\ldots,2^n-1$, are shown as follows:

$$\begin{aligned}U_{YX} &= \left(I^{\otimes q+2}\otimes\sum_{j=0,i=0}^{2^n-1}\sum_{ji\neq YX}^{2^n-1}|ji\rangle\langle ji|\right)\\ &\quad+\Omega_{YX}\otimes|YX\rangle\langle YX|,\end{aligned} \tag{19}$$

where Ω_{YX} is a quantum operation as shown in Eq. (20), which is the operation of setting the values in pixel (Y,X),

$$\Omega_{YX} = \bigotimes_{j=0}^{q+2}\Omega_{YX}^{j}. \tag{20}$$

Because there are q-qubit gray value of cover image, one-qubit binary value of information image and one-qubit Boolean value of the key, Ω_{YX} includes $q+2$ quantum oracles that comply the following form:

$$\Omega_{YX}^{j}:|0\rangle\rightarrow\begin{cases}|0\oplus B\rangle & j=0,\\ |0\oplus f\rangle & j=1,\\ \left|0\oplus C_{YX}^{i}\right\rangle & j=2,3,\ldots,q+2.\end{cases} \tag{21}$$

That is, if the target value is 1, Ω_{YX}^{i} is a multi-control-qubit NOT gate. Otherwise, it is a quantum identity gate that will not work on the quantum state. It is noting that the value-setting operation is a unitary matrix since $U_{YX}U_{YX}^{\dagger} = I^{\otimes 2n+q+2}$. Applying U_{YX} to the intermediate state $|\psi\rangle_1$ gives us

$$\begin{aligned}&U_{YX}(|\psi\rangle_1)\\ &= U_{YX}\left(\frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{i=0}^{2^n-1}|0\rangle^{\otimes q+2}|ji\rangle\right)\\ &= \frac{1}{2^n}U_{YX}\left(\sum_{j=0,i=0}^{2^n-1}\sum_{ji\neq YX}^{2^n-1}|0\rangle^{\otimes q+2}|ji\rangle+|0\rangle^{\otimes q+2}|YX\rangle\right)\\ &= \frac{1}{2^n}\left(\sum_{j=0,i=0}^{2^n-1}\sum_{ji\neq YX}^{2^n-1}|0\rangle^{\otimes q+2}|ji\rangle+\Omega_{YX}|0\rangle^{\otimes q+2}|YX\rangle\right)\\ &= \frac{1}{2^n}\left(\sum_{j=0,i=0}^{2^n-1}\sum_{ji\neq YX}^{2^n-1}|0\rangle^{\otimes q+2}|ji\rangle+|B\rangle|f\rangle|C_{YX}\rangle|YX\rangle\right).\end{aligned} \tag{22}$$

From Eq. (22), it is obvious that

$$U_2|\psi\rangle_1 = \left(\prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}U_{YX}\right)|\psi\rangle_1 = |\text{CIK}\rangle. \tag{23}$$

The composite representation can be written as

$$|\text{CIK}\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|B\rangle\otimes|f\rangle\otimes|C_{YX}\rangle\otimes|YX\rangle. \tag{24}$$

The latter part of the procedure focuses on using the appropriate circuit to embed the information to the cover image. In this study, we embed the information qubit to the second least significant bit of gray value in cover image using controlled swap operation when the key value is equal to 1. If the key value is 0, the information will be hidden in the least significant bit. If we define an operator U which carries out the controlled swap operation (CSO), the output form of the composite system after applying U is demonstrated as

$$\begin{aligned}&U|\text{CIK}\rangle\\ &= U\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|B\rangle\otimes|f\rangle\otimes|C_{YX}\rangle\otimes|YX\rangle\\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}(|0\rangle\otimes\left|C_{YX}^{0}\right\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}C_{YX}^{1}f\right\rangle\\ &\quad+|1\rangle\otimes\left|C_{YX}^{1}\right\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}fC_{YX}^{0}\right\rangle)\otimes|YX\rangle.\end{aligned} \tag{25}$$

Obviously, from Eq. (25), the operator U is just applied to the grayscale qubits. We only need two Fredkin (controlled swap) gates and a NOT-gate to construct the CSO model. Figure 1(a) shows the circuit realization of controlled swap operation.

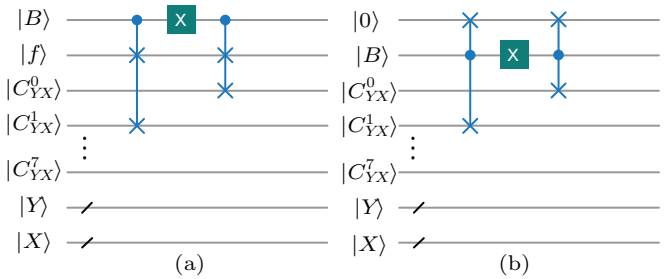


Fig. 1. Embedding and extraction circuits where (a) the information image is embedded to the cover image using two controlled swap gates and (b) the original information image is extracted from watermarked image by the reverse order of embedding circuit.

4.3. Extraction procedure

In terms of accessibility, the watermark extraction procedure is only available to the copyright owner, who uses the authentication key to authenticate the true ownership of a watermarked image. That is, if we want to extract the information image from watermarked image, it will be sufficient to use the authentication key without original image.

As mentioned in Subsection 4.2, the circuit model CSO is comprised by two Fredkin gates and one NOT gate, out of question, which is a reversible circuit. Exploiting this, the original information image can be restored by the inverse sequence of the embedded circuit. It is noted that an ancillary qubit with initial state $|0\rangle$ is adopted to store the extracted watermark. The detailed circuit is illustrated in Fig. 1(b). Thus, the operator $U_{\rm r}$ represents the reversible U operator that denotes a reversible controlled swap operation is defined as follows:

$$\begin{aligned}
&U_{\rm r}\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|\text{ancillary qubit}\rangle\otimes|B\rangle\otimes|C_{YX}\rangle\otimes|YX\rangle\\
&=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}U_{\rm r}(|0\rangle\otimes|0\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}C_{YX}^{1}f\right\rangle\\
&\quad+|0\rangle\otimes|1\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}fC_{YX}^{0}\right\rangle)\otimes|YX\rangle\\
&=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}(|f\rangle\otimes|0\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}C_{YX}^{1}0\right\rangle\\
&\quad+|f\rangle\otimes|1\rangle\otimes\left|C_{YX}^{q-1}\cdots C_{YX}^{2}0C_{YX}^{0}\right\rangle)\otimes|YX\rangle\\
&=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f\rangle\otimes|B\rangle\otimes\left|C'_{YX}\right\rangle\otimes|YX\rangle\,. \qquad (26)
\end{aligned}$$

4.4. Circuits complexity

The complexity of circuit depends on what is taken as the fundamental unit. For the complex unitary operations, it can be decomposed to unary operators and binary operators.[38] Therefore, the circuit complexity of any unary gates and binary gates is considered as fundamental unit. From Fig. 1, the embedding and extraction circuits are implemented by two Fredkin gates and one NOT gate in the same way. The decomposition circuit of Fredkin gate is given as shown in Fig. 2.

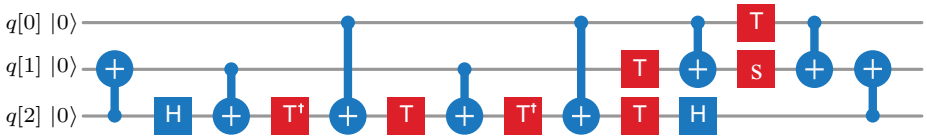


Fig. 2. The implementation of the Fredkin gate using Hadamard (H), phase (S), controlled Not and $\pi/8$ (T) gates.

Accordingly, the embedding circuit is decomposed to 35 basic gates, that is, the circuit complexity is $O(1)$. The same is true for the extraction circuit. Compared with the complexity related to image size in the classical counterpart, our algorithm has a larger improvement than the classical algorithm.

5. Experimental simulation

To appraise the property of the proposed scheme, a set of cover image comprising of 8 images with 8-bit in depth and a size of 256×256 is employed (presented in Fig. 3). They are from the network, for example, the website: http://sipi.usc.edu/database/. However, without a physical quantum computer, the experiments are limited in simulations of quantum images and circuits as discussed in the preceding sections.

5.1. Similarity between images

The watermarking scheme aims at embedding specific content, usually the information of owner, to a cover image for copyright protection. It is important that the scheme should not change the cover image visually so that no one can distinguish whether the public image is an original image or a watermarked one.

There is a great deal of available quantum image processing literature to utilize the PSNR metric to evaluate the fidelity of watermarked images. It is most easily defined by means of the mean squared error (MSE), we can define it for two $m\times n$ images (cover image and watermark image) as

$$\text{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[(I(i,j)-W(i,j))^2\right]. \qquad (27)$$

The PSNR is defined by

$$\text{PSNR}=20\log_{10}\left(\frac{\text{MAX}_I}{\sqrt{\text{MSE}}}\right), \qquad (28)$$

where MAX_I is the maximum pixel value of image I.

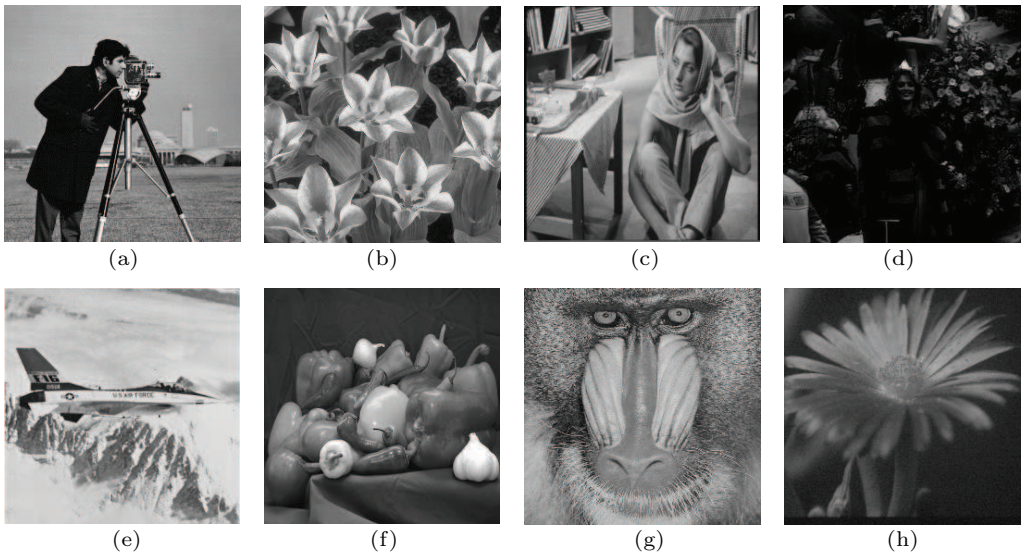


Fig. 3. Images for simulation: (a) cameraman, (b) tulips, (c) barbara, (d) carnev, (e) airplane, (f) pepper, (g) mandrill, (h) fiore.

Now we present a method to measure the similarity between watermarked image and cover image based on the quantum informational entropy. As mentioned before, the informational entropy is represented by Eq. (4), which can denote the information contained in an image, and we know that the process of watermark embedding will cause changes in image information. Therefore, the method is suitable for evaluating the similarity of images.

Consider S and S' as the quantum informational entropy of the cover image and the watermarked one, respectively, which can be given as follows:

$$\begin{aligned} S &= -\sum_{i=0}^{2^q-1} p_i \log p_i, \\ S' &= -\sum_{i=0}^{2^q-1} p'_i \log p'_i, \end{aligned} \tag{29}$$

where p_i and p'_i indicate the probability amplitude of the original gray value qubits and the manipulated one, respectively. Then, we quantify the similarity between two images using the entropy difference (ED),

$$\begin{aligned} \mathrm{ED} &= \left|S - S'\right| \\ &= \left| \left(-\sum_{i=0}^{2^q-1} p_i \log p_i \right) - \left(-\sum_{i=0}^{2^q-1} p'_i \log p'_i \right) \right|. \end{aligned} \tag{30}$$

It would be obvious that the closer the ED is to 0, the more similar the two images being tested.

Since the probabilities must sum to one, the experiment can be simulated based on statistic of image pixels. We count the number of pixels in a classical image with particular intensity values, then the corresponding probabilities are obtained by dividing the total number of pixels. The results of PSNR and ED are summarized in Table 1, where the binary image 'Rice' is considered as the information image. In addition, for comparison, we give other entropy differences of image pairs in Table 2.

Table 1. The results of PSNR and ED.

Cover image	PSNR	ED
Cameraman	54.02	0.0340
Mandrill	52.85	0.0334
Fiore	54.14	0.0300
Barbara	53.43	0.0304
Airplane	54.07	0.0355
Pepper	55.28	0.0366
Tulips	53.25	0.0251
Carnev	55.08	0.0056

Table 2. The entropy difference of two images.

Image pairs	ED
Cameraman-tulips	0.6557
Barbara-carnev	2.6278
Airplane-tulips	0.9159
Fiore-tulips	0.7330

5.2. Capacity

The capacity of quantum watermarking scheme is defined as the ratio of the number of secret qubits and the number of cover image pixels. Thus, the capacity of the proposed scheme is given as follows:

$$\begin{aligned} C &= \frac{\text{Number of secret qubits}}{\text{Number of cover image pixels}} \\ &= \frac{2^{2n}}{2^{2n}} = 1\,(\text{bit/pixel}), \end{aligned} \tag{31}$$

where n is the qubits representing the size of cover image. Therefore, the capacity of the proposed scheme is 1 bit in every pixel.

5.3. Security

It is necessary to analyze the security under the attack of the illegal Eve for a quantum image watermarking algorithm.

There are some types of attack such as intercept-resend attack and denial of service attack.[39,40] The simplest type of possible attack is the intercept-resend attack, where Eve measures the quantum states (photons) sent by sender and then sends replacement states to receiver, prepared in the state she measures. As we know that the quantum image is expressed in a superposition state, if the image is collapsed into another state once Eve measures it, the receiver cannot get the correct result when measuring. Thus the receiver will notice the presence of Eve and abort the communication.

For a denial of service attack, due to the good imperceptibility between original image and watermarked image, Eve cannot discover the presence of watermark. If Eve attempts to cut off all communication channels at a great cost, the receiver can obtain the watermarked image from public space or by routing communication via alternate links. Consequently, the proposed algorithm has good security to resist on Eve attacks.

6. Conclusion

A watermarking scheme for quantum images based on maximum entropy threshold segmentation is proposed. Because the quantum representation of image is pure state, the entropy of the threshold problem employs the quantum informational entropy. After applying the threshold value to segment the cover image, a binary image which uses as the authentication key to embed and extract information image is obtained. Therefore, the modification of the image object will be smaller than the background, which is useful in the field about health information system and so on. For example, the sensitive information of the patients and the doctors can be embedded to the medical data instead of widely distributing on the open network. The embedded quantum circuit designed in the proposed scheme consists of two Fredkin gates and a NOT gate, and the verification quantum circuit is also the same composition. Obviously, the complexity of the quantum circuits used in our scheme is quite low. Finally, to assess the performance of the investigated scheme, an entropy difference measure together with other commonly used metrics is used.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 6217070290), the Shanghai Science and Technology Project (Grant Nos. 21JC1402800 and 20040501500), the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 21A0470), the Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ4557), and Top-Notch Innovative Talent Program for Postgraduate Students of Shanghai Maritime University (Grant No. 2021YBR009).

References

[1] Grover L K, Labs B, Avenue M and Nj M H 1996 *Proceedings of the twenty-eighth annual ACM symposium on theory of computing* (Philadelphia, USA: Association for Computing Machinery) pp. 212–219
[2] Bennett C H and Shor P W 1998 *IEEE Trans. Inf. Theory* **44** 177
[3] Vlasov A Y 1997 arXiv:quant-ph/9703010 [hep-ph]
[4] Sch R 2002 *Phys. Rev. A* **67** 062311
[5] Beach G, Lomont C and Cohen C 2003 *Applied Imagery Pattern Recognition Workshop*, October 15–17, Washington DC, USA, 2003 pp. 2–7
[6] Venegas-Andraca S and Bose S 2003 *Proc. SPIE* **5105**, *Quantum Information and Computation* August 4 2003, Orlando, Florida, United States
[7] Latorre J I 2005 arXiv:quant-ph/0510031 [hep-ph]
[8] Le P Q, Dong F and Hirota K 2011 *Quantum Inf. Process.* **10** 63
[9] Zhang Y, Lu K, Gao Y and Wang M 2013 *Quantum Inf. Process.* **12** 2833
[10] Li H, Zhu Q, Li M and Ian H 2014 *Inf. Sci.* **273** 212
[11] Abura'ed N, Khan F S and Bhaskar H 2017 *ACM Comput. Surv.* **49** 75
[12] Jiang N and Wang L 2015 *Quantum Inf. Process.* **14** 1559
[13] Sang J, Wang S and Niu X 2016 *Quantum Inf. Process.* **15** 37
[14] Li P and Liu X 2018 *Int. J. Quantum Inf.* **16** 1850031
[15] Yan F, Iliyasu A M, Fatichah C, Tangel M L, Betancourt J P, Dong F and Hirota K 2012 *J. Quantum Inf. Sci.* **2** 55
[16] Yi Z, Kai L and Yinghui G 2015 *Sci. China Inf. Sci.* **58** 1
[17] Abdel-Khalek S, Abdel-Azim G, Abo-Eleneen Z A and Obada A S F 2016 *J. Russ. Laser Res.* **37** 141
[18] Yao X W, Wang H, Liao Z, Chen M C, Pan J, Li J, Zhang K, Lin X, Wang Z, Luo Z, Zheng W, Li J, Zhao M, Peng X and Suter D 2017 *Phys. Rev. X* **7** 031041
[19] Wang X, Yang C, Xie G S and Liu Z 2018 *Entropy* **20** 1
[20] Caraiman S and Manta V I 2014 *Theor. Comput. Sci.* **529** 46
[21] Lupo C, Wilde M M and Lloyd S 2016 *IEEE Trans. Inf. Theory* **62** 3745
[22] Bandyopadhyay S K, Bhattacharyya D and Das P 2008 *The 3rd IEEE Conference on Industrial Electronics and Applications*, June 3–5, 2008, Singapore, p. 959
[23] Iliyasu A M, Le P Q, Dong F and Hirota K 2012 *Inf. Sci. (Ny).* **186** 126
[24] Li P and Zhao Y 2017 *J. Comput.-Aided Design & Comput. Graph.* **29** 1624 (in Chinese)
[25] Luo G, Jia R Z, Wenwen L, Yang H and Ian H 2019 *Quantum Inf. Process.* **18** 1
[26] Mogos G 2008 *International Symposium on Computer Science and its Applications*, October 13–15, 2008, Hobart, TAS, Australia, pp. 187–190
[27] Jiang N, Zhao N and Wang L 2016 *Int. J. Theor. Phys.* **55** 107
[28] Heidari S and Farzadnia E 2017 *Quantum Inf. Process.* **16** 1
[29] Qu Z, Cheng Z, Liu W and Wang X 2019 *Multimed. Tools Appl.* **78** 7981
[30] Luo J, Zhou R G, Luo G F, Li Y C and Liu G Z 2019 *Sci. Rep.* **9** 15134
[31] Yan F, Le P Q, Iliyasu A M, Sun B, Garcia J A, Dong F and Hirota K 2012 *IEEE Congress on Evolutionary Computation*, June 10–15, 2012, Brisbane, QLD, pp. 1–6
[32] Zhou R and Sun Y 2015 *Quantum Inf. Process.* **14** 1605
[33] Iliyasu A M and Yan F 2016 *Entropy* **18** 360
[34] Peter W, Labs A B, Ave M and Hill M 1994 *Proceedings 35th Annual Symposium on Foundations of Computer Science*, November 20–22, 1994, Santa Fe, NM, USA, pp. 124–134
[35] Kak S 2007 *Int. J. Theor. Phys.* **46** 860
[36] Kak S 2016 *Int. J. Theor. Phys.* **55** 3017
[37] Kapur J N, Sahoo P K and Wong A K C 1985 *Comput. Vis. Graph. Image Procss.* **29** 273
[38] Barenco A, Bennett C H, Cleve R, Divincenzo D P, Margolus N, Shor P, Smolin J and Weinfurter H 1995 *Phys. Rev. A* **52** 3457
[39] Jiang S X, Zhou R G, Xu R and Luo G 2019 *IEEE Access* **7** 80530
[40] Qu Z, Cheng Z and Wang X 2019 *IEEE Access* **7** 35684