计算机科学
COMPUTER SCIENCE

一种新的基于量子小波变换的图像水印算法

苏永红, 夏婷, 王绪梅, 钱小红

引用本文

苏永红, 夏婷, 王绪梅, 钱小红.一种新的基于量子小波变换的图像水印算法[J]. 计算机科学, 2023, 50(6A): 220300034-8.

SU Yonghong, XIA Ting, WANG Xumei, QIAN Xiaohong. New Image Watermarking Algorithm Based on Quantum Wavelet Transform [J]. Computer Science, 2023, 50(6A): 220300034-8.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220300034

一种新的基于量子小波变换的图像水印算法

苏永红　夏　婷　王绪梅　钱小红
武汉华夏理工学院　武汉 430223
(461782640@qq.com)

摘　要　图像水印是一种将特定信息嵌入载体图像中的技术,用于版权保护。研究了一种新的基于量子小波变换的图像水印方案,包括置乱过程、嵌入过程和提取过程。其中采用改进的量子 Arnold 置乱方法对二值图像进行置乱,置乱后的水印图像应用于载体图像的最低有效分块量子位,对载体灰度图像采用量子 Haar 小波变换和量子最低有效位(LSB)分块技术,将置乱后的水印图像嵌入量子小波系数。首先从嵌入图像中提取置乱水印图像,然后利用改进的量子 Arnold 逆置乱方法进行逆置乱,获取原始水印图像。仿真技术验证了基于该量子图像水印方法水印的不可见性和高鲁棒性。通过峰值信噪比(PSNR)检验证明了该方案的不可见性。通过误码率(BER)检验和归一化相关系数(NC)检验了该方案的高鲁棒性。仿真结果表明,该水印方案不仅具有可接受的视觉质量,而且对不同类型的攻击具有良好的抵抗能力。

关键词:量子小波变换;图像水印;置乱;量子最低有效位分块;不可见性;鲁棒性
中图法分类号　TP319

New Image Watermarking Algorithm Based on Quantum Wavelet Transform

SU Yonghong,XIA Ting,WANG Xumei and QIAN Xiaohong
Wuhan Huaxia Institute of Technology,Wuhan 430223,China

Abstract　Image watermarking is a technology that embeds specific information into the carrier image for the purpose of copyright protection. A new image watermarking scheme based on quantum wavelet transform is studied, including scrambling process, embedding process and extraction process. The improved quantum Arnold scrambling method is used to scramble the binary image. The scrambled watermark image is applied to the least effective block qubit of the carrier image. For the carrier gray image, the quantum Haar wavelet transform and quantum least significant bit(LSB) blocking technology are used to embed the scrambled watermark image into the quantum wavelet coefficient. In the extraction process, firstly, the scrambled watermark image is extracted from the embedded image, and then the improved quantum Arnold inverse scrambling method is used to obtain the original watermark image. Simulation technology verifies the invisibility and high robustness of the watermark based on the quantum image watermarking method. The invisibility of the scheme is proved by peak signal-to-noise ratio(PSNR) test. The high robustness of the scheme is tested by bit error rate(BER) test and normalized correlation coefficient(NC). Simulation results show that the watermarking scheme not only has acceptable visual quality, but also has good resistance to different types of attacks.

Keywords　Quantum wavelet transform, Image watermarking, Scrambling, Quantum least significant bit blocking, Invisibility, Robustness

1　引言

自推出第一个量子密钥分发协议以来,许多研究人员对经典媒体的量子力学表示和处理做出了贡献[1]。包括数字水印在内的量子信息隐藏和隐写术是安全数字信息传输和处理的有效工具。2015 年,Mou 等[2]提出基于量子 Haar 小波变换的量子水印算法,其算法思路首先考虑了将文本的经典图像信息用量子图像信息的矩阵形式表示出来,然后对量子化后的矩阵做量子 Haar 小波变换,最后将文本水印信息嵌入量子小波系数中。Wang 等[3]提出了一套基于最低有效位的量子图像水印方案,在实现该图像水印方案的过程中,嵌入者将首先通过置换某量子载体图像灰度值中的至少某一个比特数而把该水印图像嵌入包含该量子载体图像上信息的某些特定的像素数中,这些特定的像素数量是由其中每一个比特数私钥决定的。Jiang 等[4]提出基于 Moiré 条纹的量子信息隐藏方案,该方案使用形变操作处理原始载体图像和待隐藏的消息图像,获得莫尔模式,使用去噪操作将莫尔模式转变为含有隐藏信息的载体图像。2018 年,Li 等[5]利用新型增强量子图像表示法,提出一种基于含水印量子图像的自适应量子隐写算法。Ji 等[6]在基于量子图像的柔性表示法中,提出一种大容量量子图像水印协议,借助连分式算法来加强水印图像的不可见性。2020 年,Qu 等[7]提出了一种安全可控的量子图像隐写算法,该方案采用一种新的受控量子图像柔性表示的受控量子访问机制,帮助发送方控制信息传输的整个过程。综合以上量子水印的研究现状,量子水印技术的研究有非常广阔的前景,且目前处在起步阶段。本文提出了

基金项目:湖北省教育厅科学技术计划指导性项目(B2017397)
This work was supported by the Guiding Project of Science and Technology Plan of Hubei Provincial Department of Education(B2017397).
通信作者:夏婷(29446074@qq.com)

一种新的基于量子小波变换的图像水印算法，包括置乱过程、嵌入过程和提取过程。通过仿真分析，不仅验证了该方案的不可见性，而且验证了该方案的鲁棒性。

本文第 2 节介绍了方案中使用的预备知识；第 3 节介绍了量子小波变换水印方案；第 4 节对方案进行了软件仿真和分析；最后总结全文并展望未来。

2 预备知识

2.1 数字图像的量子表示

一种新的数字图像增强量子表示方法（New Enhanced Quantum Representation，NEQR）由 Zhang 等于 2013 年提出[8]。基于 NEQR 方案，给出了一个 $2^n \times 2^n$ 大小的量子图像，如式(1)所示：

$$|I\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle,\ |c_i\rangle=|c_i^{q-1}\cdots c_i^1 c_i^0\rangle,\ c_i^k\in\{0,1\},$$
$$k=q-1,\cdots,1,0,\ i=0,1,\cdots,2^{2n-1}-1 \tag{1}$$

此处 $|c_i\rangle$ 和 $|i\rangle$ 指示颜色和对应的各个颜色位置，而且 $|i\rangle$ 包括两部分：垂直和水平部分。

$$|i\rangle=|y\rangle|x=y_{n-1},y_{n-2},\cdots,y_0\rangle|x_{n-1},x_{n-2},\cdots,x_0\rangle,$$
$$y_j x_j\in\{0,1\} \tag{2}$$

第一个 n 量子位 $|y_{n-1}\rangle,|y_{n-2}\rangle,\cdots,|y_0\rangle$ 沿垂直轴编码，第二个 n 量子位 $|x_{n-1}\rangle,|x_{n-2}\rangle,\cdots,|x_0\rangle$ 沿水平轴编码。因此，NEQR 模型需要 $q+2n$ 个量子位来表示灰度范围为 $2q$ 的 $2^n\times 2^n$ 大小的灰度图像。图 1 给出了一个 2×2 的图像及其 NEQR 表示，其中 8 个量子位用于表示 0～255 之间可能值的灰度范围的颜色信息。

$$|I\rangle=\frac{1}{2}[|00000000\rangle\otimes|00\rangle+01100110\rangle\otimes|01\rangle+$$
$$|10011001\rangle\otimes|10\rangle+|11001100\rangle\otimes|11\rangle]$$

图 1 一个简单的图像示例及其 NEQR 表示

Fig. 1 A simple image example and its NEQR representation

2.2 量子加法器

Arnold 图像置乱用到模 N 加法。量子模 N 加法器的实现是在量子计算机中实现这两种置乱变换的基础。Vedral 等[9]已经给出了量子模 N 加法器的实现方法。为了给出量子模 N 加法器，首先我们简要地介绍量子加法器。量子加法器是一个用于量子计算过程的逻辑线路，它可以计算存储在两个量子寄存器中的数据的值的和。假如这两个量子寄存器分别为 $|a\rangle$ 和 $|b\rangle$，则量子加法器实现的加法运算的功能为 $|a\rangle,|b\rangle\rightarrow|a,a+b\rangle$，即 a 和 b 是两个加数，计算出的和存储在原来 b 的位置。量子加法器（ADDER）如图 2 所示，其中的 SUM 表示加电路模块，CARRY 表示进位电路模块。

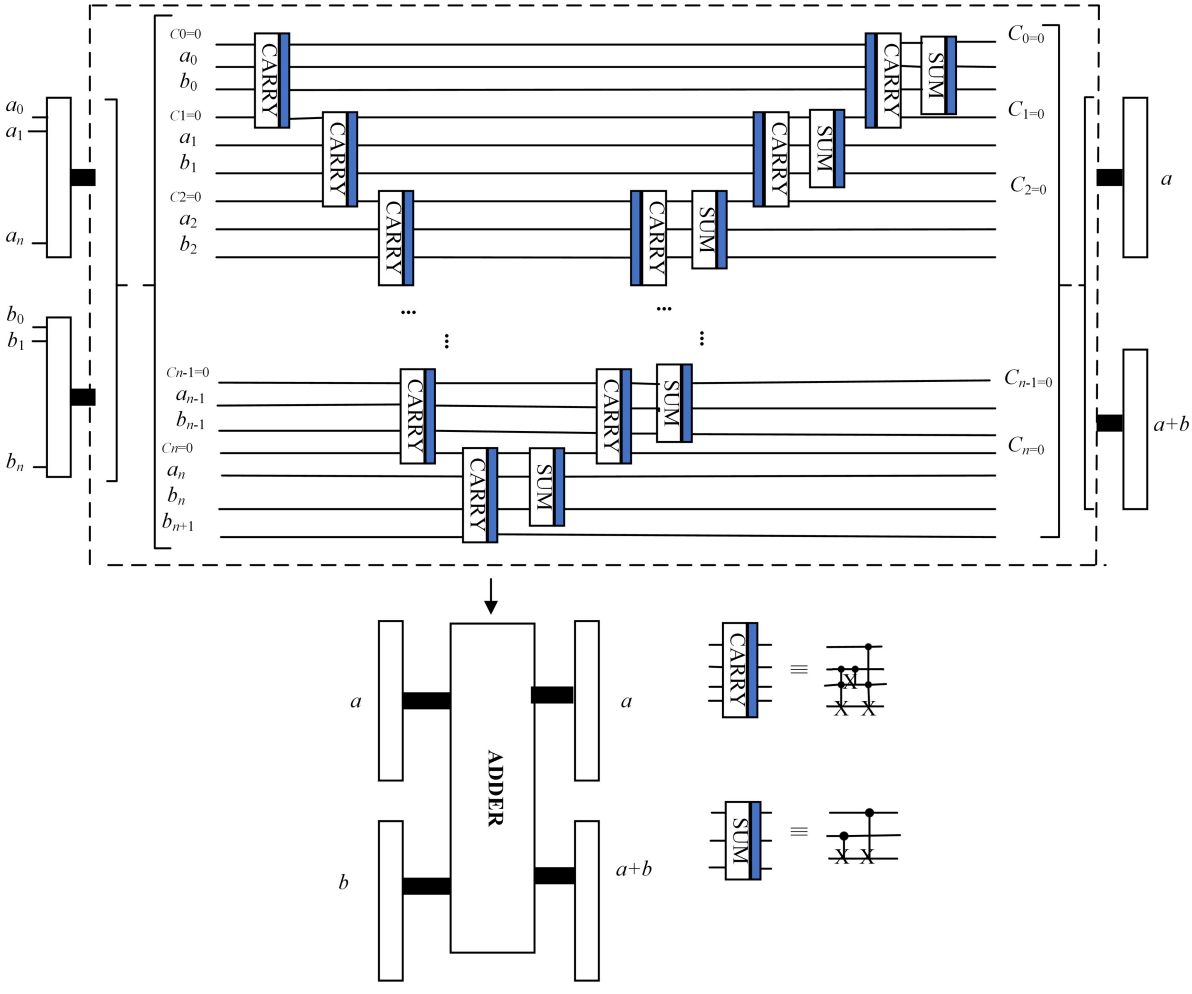


图 2 量子加法器和其中的电路模块

Fig. 2 Quantum adder and its circuit module

无论 SUM 还是 CARRY,表示模块的矩形中都有一个黑色的竖条,它表示模块中逻辑门的排列顺序。竖条在左侧的模块与竖条在右侧的模块中逻辑门的排列顺序方式是相反的。由于量子线路的幺正性,逻辑门排列顺序相反时意味着其逻辑功能正好相反。例如代表量子加法器的 ADDER 模块,如果其中的黑色竖条在左侧,则其功能变为与量子加法相反的功能,即变为一个量子减法器。当 $b \geqslant a$ 时,量子减法器可以被简单地描述为:

$|a,b\rangle \rightarrow |a,b-a\rangle$

当 $b<a$ 时,量子减法器可以描述为:

$|a,b\rangle \rightarrow |a,2n+b-a)\rangle$

量子模 N 加法器可以对两个数的和进行模运算:

$|a,b\rangle \rightarrow |a,(a+b) \bmod N\rangle$

Vedral 等[9]提出的量子模 N 加法器是基于量子加法器实现的,原理是当 $a+b$ 的结果大于 N 时,从 $a+b$ 中减去 N。

2.3 量子逻辑门

对量子位的态进行变换可以实现一些逻辑功能,变换所起的作用相当于逻辑门所起的作用,通常把在一个时间间隔内实现逻辑变换的量子装置称为量子逻辑门[10]。在数学描述上,量子逻辑门对应的就是一个酉矩阵,对用向量空间描述的量子态实现幺正变换,这样的计算过程是可逆的。根据量子门中量子位数目的不同,可分为一位门、二位门和多位门。

一位门 U 作用到一个量子位态 $|\varphi\rangle$ 上,输出态 $U|\varphi\rangle$,量子线路如图 3 所示。其中,水平线表示一个量子位,方框中的 U 表示对这个量子位进行幺正变换。线从左到右并不代表量子位的空间移动,而是表示时间进行方向。量子计算机中有多个量子一位 U 门,数学上用 2×2 的幺正矩阵表示,如恒等门(I 门)、非门(NOT 门)、Hadamard 门(H 门),如图 4－图 6 所示。Hadamard 门简称 H 门,其中,$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$,H 门对两个基矢 $|0\rangle$ 和 $|1\rangle$ 的作用为:

$$H|0\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \quad (3)$$

$$H|1\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \quad (4)$$

即当 H 门作用于 $|0\rangle$ 态时,会使得 $|0\rangle$ 和 $|1\rangle$ 以相同得概率出现。

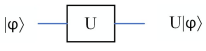


图 3 量子一位门

Fig. 3 Quantum one bit gate

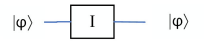


图 4 恒等门(I 门)

Fig. 4 Identity gate(gate I)

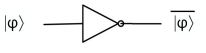


图 5 非门(NOT 门)

Fig. 5 non gate(not gate)

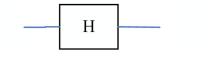


图 6 Hadamard 门(H 门)

Fig. 6 Hadamard door(H door)

量子二位门需要两个量子比特参与。一个重要的二位门是控制非门(CNOT),控制非门中一个量子比特称为控制位,另一个量子比特称为目标位,当且仅当控制位处在态 $|1\rangle$ 时,将目标位取非,即:

$$\begin{aligned}&\text{CNOT}|00\rangle=|00\rangle,\text{CNOT}|01\rangle=|01\rangle\\ &\text{CNOT}|10\rangle=|11\rangle,\text{CNOT}|11\rangle=|10\rangle\end{aligned} \quad (5)$$

控制非门如图 7 所示,控制非门的矩阵表示为:

$$\text{CNOT}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

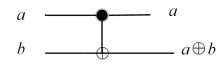


图 7 控制非门(CNOT 门)

Fig. 7 Control non gate(CNOT gate)

一个重要的三位门是 Toffoli 门,又称“控-控-非”门,如图 8 所示。它有两个控制位,一个目标位,当且仅当两个逻辑控制位都处在态 $|1\rangle$ 时,才对目标位执行逻辑非操作,相当于目标位和控制位的与进行异或操作。从 CNOT 门到 Toffoli 门,控制位个数从 1 增加到 2,实际上,控制位个数还可以继续增加到 n 个,我们称有 n 个控制位的逻辑非门为 n-CNOT 门。n-CNOT 门的控制位,可以是零控制,也可以是 1 控制,量子线路中分别用“。”和“·”表示。用 1 比特位对“。”和“·”编码。“。”编码为 0,“·”编码为 1,将 n-CNOT 门中所有控制位对应的编码按照从上到下的顺序连接成一个二进制数,这个二进制数就是该 n-CNOT 门的控制值。例如一个 5-CNOT 门,从上到下,它的 5 个控制位分别为“·。。·”,对应的编码为“10011”,将该编码看成一个二进制数,则控制值为二进制的 10011,即十进制的 19。

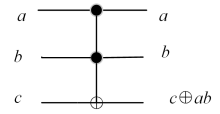


图 8 Toffoli 门

Fig. 8 Toffoli door

2.4 量子小波变换

傅里叶变换在许多科学领域都是一种有用且强大的工具,小波变换与傅里叶变换一样有用,可用于揭示信号的多尺度结构,对图像处理和数据压缩都非常有用。为了分析连续波,需要将连续波转换为数字信号并对其进行分析。有 3 种变换:傅里叶变换、短时傅里叶变换和小波变换。从变换对象本质定义上讲,小波定义的变换对象是在信号时间频率的范围内进行的一个局部变化信号分析,它也能同时通过伸缩运算与平移计算两种基本运算处理手段达到对信号空间的一个逐步的多维尺度上的进一步细化,最终它将达到一个对信号高频处时间范围的逐步细分,低频处频率范围的逐渐细分,能够更加自动快速地适应一个多时频信号分析的要求,从而信号可被自动地聚集到信号分析中的各个任意方向的细节,解决了傅里叶变换应用中常见的各种分析困难问题。

信号处理中两类有用的小波是 Haar 小波和 Daubechies 小波。参考文献[11]中提出了量子 Haar 和 Daubenchies 小波电路,量子 Haar 小波变换的整个量子电路如图 9 所示,其中给出了量子 Haar 小波变换的完整实现逻辑过程[12]。

$W=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$,$\prod 2^n=(I_{2^{n-2}}\otimes\prod_4)(\prod_{2^{n-1}}\otimes I_2)$,

$\Pi_4=\begin{bmatrix}1&0\\0&0\\0&1\\0&0\end{bmatrix}$，称为 XOR 门，$I_2=\begin{bmatrix}1&0\\0&1\end{bmatrix}$。

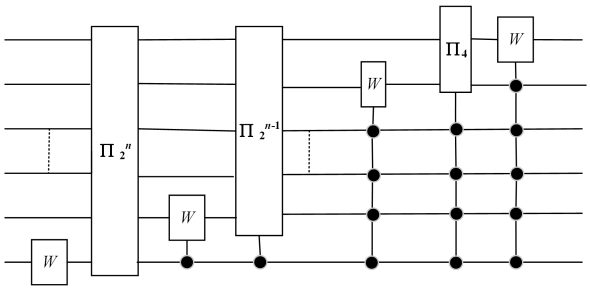


图 9 量子 Haar 小波变换的逻辑实现[12]

Fig. 9 Logical implementation of quantum Haar wavelet transform[12]

3 量子小波变换水印

本节提出了一种基于量子小波变换的量子水印算法，该方法将一幅 $2^n\times2^n$ 大小的二值图像嵌入到灰度图像中。该方案包括 3 个步骤：置乱、嵌入、提取。

3.1 量子置乱

在大多数图像处理算法中，置乱方法被视为预处理，一个图像被转换成另一个无序的图像。在提出的水印方案中，为了提高所提方法的安全性，采用了改进的量子 Arnold 置乱方法[13]。

假设图像采用 NEQR 表示方法，因为图像置乱只对位置信息进行操作，所以仅需要改变 NEQR 表示方法中的坐标信息$|YX\rangle$。我们定义 A 表示 Arnold 图像置乱操作，I 表示原始的量子图像，置乱后的量子图像用 I_A 表示，图像大小为 $2^n\times2^n$，则：

$$|I_A\rangle=A|I\rangle=\frac{1}{\sqrt{2}^{2n}}\left(\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{n-1}|C_{YX}^i\rangle A|YX\rangle\right) \tag{6}$$

其中，$A|YX\rangle=A|Y\rangle A|X\rangle$。

假设 $I(x,y)$代表原始图像，(x,y)是像素的位置坐标，$x,y=0,1,\cdots,2^n-1$，图像大小为$2^n\times2^n$，一个二维的 Arnold 表示：

$$\begin{bmatrix}x_A\\y_A\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}\ 2^n)$$
$$x_A=(x+y)\ \mathrm{mod}\ 2^n \tag{7}$$
$$y_A=(x+2y)\ \mathrm{mod}\ 2^n$$

其中，(x_A,y_A)是 Arnold 置乱后的坐标信息。根据式(7)有：

$$|x_A\rangle=A|X\rangle=|x+y\rangle\ \mathrm{mod}\ 2^n$$
$$|y_A\rangle=A|Y\rangle=|x+2y\rangle\ \mathrm{mod}\ 2^n \tag{8}$$

根据式(8)和二进制运算的特殊性：如果 $a+b=c$，c 是一个$(n+1)$bit 的二进制数，$c=c_nc_{n-1}c_{n-2}\cdots c_0$，$c_i\in\{0,1\}$，则：

$$(a+b)\ \mathrm{mod}\ 2^n=c_{n-1}c_{n-2}\cdots c_0 \tag{9}$$

该定理表明，模 2^n可以通过忽略和的最高位的进位来实现。

基于定理 7－定理 9，改进的 Arnold 置乱可表示为：

$$|x_A\rangle=|x_0x_1\cdots x_{n-1}+y_0y_1\cdots y_{n-1}\rangle\ \mathrm{mod}\ 2^n$$
$$|y_A\rangle=|x_0x_1\cdots x_{n-1}+y_1y_2\cdots y_{n-1}0\rangle\ \mathrm{mod}\ 2^n \tag{10}$$

因此，改进的 Arnold 置乱线路如图 10 和图 11 所示。

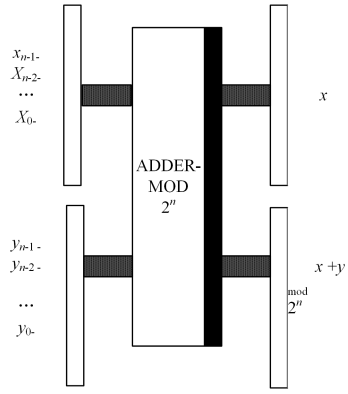


图 10 $|x_A\rangle$线路上

Fig. 10 $|x_A\rangle$ line

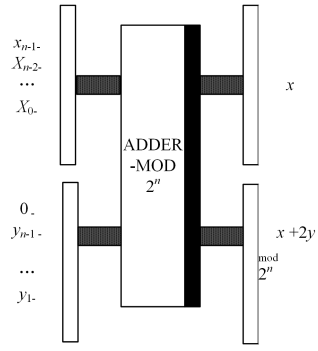


图 11 $|y_A\rangle$线路

Fig. 11 $|y_A\rangle$line

3.2 嵌入程序

考虑一个 $2^n\times2^n$ 大小的灰度载波图像，使用数字图像的新型增强量子表示 NEQR 模型，载体图像表示为：

$$|C\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\otimes|i\rangle$$
$$|c_i\rangle=|c_i^7\cdots c_i^1c_i^0\rangle,c_i^k\in\{0,1\},k=7,\cdots,1,0,i=0,1,\cdots,2^{2n}-1 \tag{11}$$

为了嵌入，采用 LSB(Least Significant Bit，最低有效位)分块技术和载波图像的量子小波变换。图 12 给出了嵌入方案的概要设计。

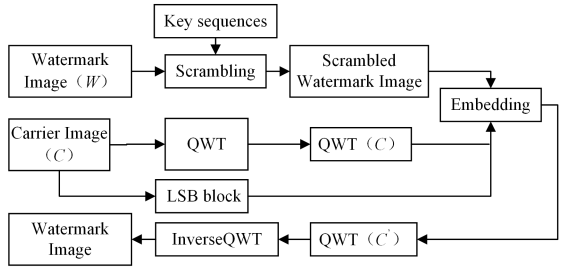


图 12 嵌入程序的概要图

Fig. 12 Overview of embedded program

LSB 信息隐藏的原理是用待隐藏的信息去替代载体的最低比特，比较简单，但鲁棒性不好，许多常见的处理方法如滤波、加噪、压缩等，都可以很容易将隐藏的信息去掉。为了提高 LSB 的健壮性和不可检测性，量子 LSB 分块信息隐藏将载体图像分为图像块，每个图像块中隐藏一个比特的消息。基于NEQR 量子图像的表示方法，能方便地对图像进行分块。如果部分位置信息被设定为特定的值，则一些像素将被挑选出来。以图 1 为例，这是一个$2^n\times2^n$的 NEQR 图像，每个

像素中第一行数字表示该像素的二进制颜色，第二行像素表示该二进制的坐标。量子 LSB 分块信息隐藏方案中，将$2^n\times2^n$的图像分成$2^{n-p_1}\times2^{n-p_2}$个大小为$2^{p_1}\times2^{p_2}$的块，其中 $p_1,p_2\in\{0,1,\cdots,n\}$，且定义 $p=p_1+p_2$。相应地，将图像的位置信息$|Y\rangle$和$|X\rangle$均分割成两部分，即$|y_{n-1}y_{n-2}\cdots y_{p_1}\rangle$和$|y_{p_1-1}\cdots y_1y_0\rangle$、$|x_{n-1}x_{n-2}\cdots x_{p_2}\rangle$和$|x_{p_2-1}\cdots x_1x_0\rangle$。我们将$|y_{n-1}y_{n-2}\cdots y_{p_1}\rangle$和$|x_{n-1}x_{n-2}\cdots x_{p_2}\rangle$称为外部坐标，将$|y_{p_1-1}\cdots y_1y_0\rangle$和$|x_{p_2-1}\cdots x_1x_0\rangle$称为内部坐标，或块内坐标。

块嵌入过程是将载体图像分割成$2^{n-p_1}\times2^{n-p_2}$个大小为$2^{p_1}\times2^{p_2}$的块，每一个图像块中隐藏一个比特的消息，该消息被重复$2^{p_1}\times2^{p_2}=2^p$次嵌入图像块的每一个像素中。嵌入程序过程分为 3 步。

第 1 步　定义空的二值图像 T。该图像用于对载体图像的 QWT 进行估值处理。

$$|T\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|t_i\rangle\otimes|i\rangle;t_i=0;i=0,1,\cdots,2^{2n}-1 \tag{12}$$

第 2 步　使用图 10 和图 11 中的量子置乱电路，将水印图像置乱，置乱后的水印图像应用于载体图像的 LSB 量子位。如果载体图像$|C\rangle$的位置信息$|y_{n-1}y_{n-2}\cdots y_{p_1}x_{n-1}x_{n-2}\cdots x_{p_2}\rangle$与水印图像$|W\rangle$的位置信息相同，则交换$|C\rangle$的最低比特位$|c_i^0\rangle$和$|W\rangle$的信息位$|w_{kl}\rangle$。

当t_i($t_i=0$)的值必须设置为 1 时，以下酉变换应用于空图像$|t\rangle$。

$$\Omega_i=I\otimes\Omega\otimes|i\rangle|i\rangle+I\otimes\left(\sum_{j=0,j\neq i}^{2^{2n}-1}|j\rangle|j\rangle\right) \tag{13}$$

在这里，$\Omega=\begin{bmatrix}0&1\\1&0\end{bmatrix}$。

上述酉变换是 CNOT 门，需要初始化空图像$|T\rangle$。

$$\text{If}\begin{cases}|c_i^0\rangle\otimes|c_i^1=0\text{ and }|w_i\rangle=1\\\qquad\text{or}\\|c_i^0\rangle\otimes|c_i^1=1\text{ and }|w_i\rangle=0\end{cases}$$

Then

$|t_i\rangle=1$

此外，当$|t_i\rangle=0$时，使用以下酉变换：

$$\Omega_j=I\otimes\left(\sum_{j=0}^{2^{2n}-1}|j\rangle|j\rangle\right)$$

通过应用该操作$\prod_{i=0}^{2^{2n}-1}\Omega_i$到图像$|T\rangle$，置乱水印图像$|w'\rangle$被复制到初始的纯空图像$|T\rangle$。

第 3 步　载体图像的量子小波变换。

定义如下：

$$\begin{aligned}|WC\rangle&=QWT(|C\rangle)\\&=QWT\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}c_i\rangle\otimes|i\rangle\right)\\&=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}wc_i\rangle\otimes|i\rangle\end{aligned} \tag{14}$$

在该步骤中，嵌入器嵌入置乱的量子水印图像$|W'\rangle$进入小波系数$|WC\rangle$：

For $i=0$ to $i=2^{2n}-1$;

If $|t_i\rangle=1$ then;

载波图像的量子小波变换修改为：

$$\sum_{i=0}^{2^{2n}-1}w'c_i'|i\rangle=\sum_{i=0}^{2^{2n}-1}(wc_i+\varphi)|i\rangle$$

End For

其中，$(0<\varphi<1)$由嵌入方确定，在嵌入和提取过程中不变。用于嵌入的量子电路图如图 13 所示。

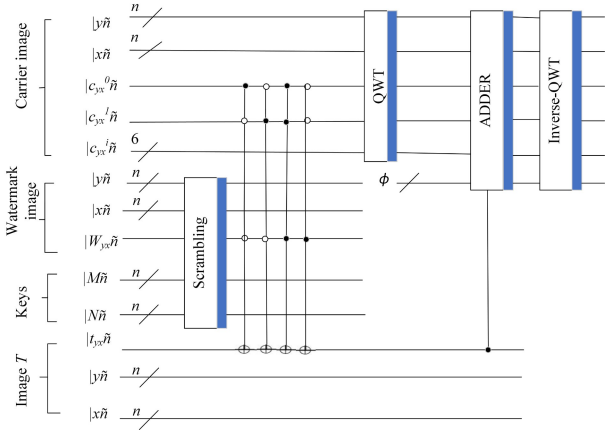


图 13　嵌入过程的量子电路

Fig. 13　Quantum circuit of embedding process

3.3　提取程序

从嵌入的图像中提取水印图像、原始载体图像、其量子小波变换形式和比例 φ。

第 1 步　从嵌入图像中提取置乱水印图像。一个 QWT 应用于两个原始载体图像$|C\rangle$和带水印的图像$|W_{\text{out}}\rangle$，提取过程如下：

$$\begin{aligned}|WC\rangle&=QWT(|C\rangle)=QWT\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle\right)\\&=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|wc_i\rangle|\otimes|i\rangle\\|WW\rangle&=QWT(|W_{\text{out}}\rangle)=QWT\left(\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|W_{\text{out}}\rangle\otimes|i\rangle\right)\\&=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|ww_i\rangle|\otimes|i\rangle\end{aligned} \tag{15}$$

假设$\Delta=|ww_i\rangle-|wc_i\rangle$，使用原始载体图像的两个 LSB（如$|c_0^i\rangle$，$|c_1^i\rangle$）水印位可按如下方式提取：

如果$\Delta=0$，水印位为$(c_0^i\oplus c_1^i)$，否则水印位为$\sim(c_0^i\oplus c_1^i)$。

第 2 步　先预处理一个空的二值图像，在这里：

$$|W_{ex}\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|w_{ex_i}\rangle\otimes|i\rangle,w_{ex_i}=0,i=0,1,\cdots,2^{2n}-1 \tag{16}$$

为了提取水印图像，酉变换 χ_i 定义如下：

$$\chi_i=I\otimes\chi\otimes|i\rangle\langle i|+I\otimes\left(\sum_{j=0,j\neq1}^{2^{2n}-1}|j\rangle\langle j|\right) \tag{17}$$

其中，$\chi=\begin{bmatrix}0&1\\1&0\end{bmatrix}$。然后，通过对空二值图像 W_{ex} 应用酉变换(χ_i)，将提取的水印位嵌入到 W_{ex} 上。通过应用操作$\prod_{i=0}^{2^{2n}-1}\chi_i$到图像$|W_{ex}\rangle$，可以提取置乱后的水印图像。

第 3 步　第 1 步完成后，置乱后的水印图像被提取。因此，为了获得原始水印图像，需要对提取的图像运行逆置乱程序。采用量子 Arnold 逆置乱。

根据前面介绍的 Arnold 置乱过程，其中(x_A,y_A)是置乱后的坐标信息，$\begin{bmatrix}1&1\\1&2\end{bmatrix}$称为置乱矩阵。Arnold 的逆置乱可以写为：

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} x_A \\ y_A \end{bmatrix} (\mathrm{mod}\ 2^n)$$
$$= \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_A \\ y_A \end{bmatrix} (\mathrm{mod}\ 2^n) \tag{18}$$

即：

$$\begin{aligned} x &= (2x_A - y_A)\ \mathrm{mod}\ 2^n \\ y &= (-x_A + y_A)\ \mathrm{mod}\ 2^n \end{aligned} \tag{19}$$

对于 Arnold 逆置乱中的$|x\rangle$，分为 3 个步骤实现：

$|x_A, x_A\rangle \rightarrow |x_A, 2x_A\rangle \rightarrow |y_A, 2x_A\rangle \rightarrow |y_A, (2x_A - y_A)\ \mathrm{mod}\ 2^n\rangle$

第 1 步使用量子加法器计算得到 $2x_A$；第 2 步用y_A代替x_A；第 3 步使用量子模 N 减法器得到$(2x_A - y_A)\ \mathrm{mod}\ 2^n$。

对于 Arnold 逆置乱中的$|y\rangle$，

$|x_A, y_A\rangle \rightarrow |x_A, (y_A - x_A)\ \mathrm{mod}\ 2^n$

它对应于一个量子模 N 减法器。提取程序的过程如图 14 所示。

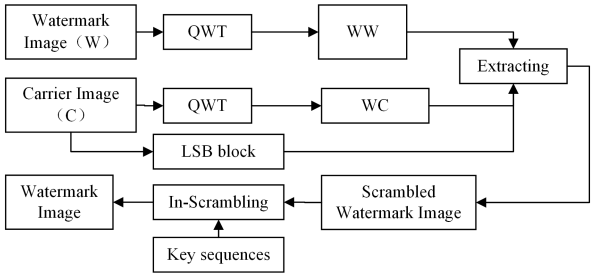


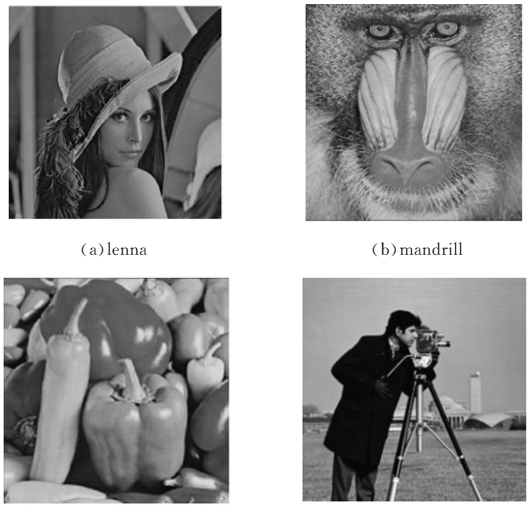
图 14 提取过程

Fig. 14 Extraction process

4 仿真与分析

这里要分析两个关键特性：不可见性和健壮性。从目前的量子硬件情况来看，无法使用量子计算机验证。为了分析这两个特性，我们在 MatlabR2018b 环境下，以 Intel(R)Core(TM)i7－4500u CPU 2.40 GHz、16.00 GB Ram 的计算机为例，对该方案进行了仿真。

图 15 给出了模拟中使用的载体图像，图 16 给出了模拟中使用的水印图像。



(a) lenna (b) mandrill

(c) peppers (d) cameraman

图 15 载体图像

Fig. 15 Carrier images

图 16 水印图像

Fig. 16 Watermark image

4.1 不可见性

不可见性表示原始图像与嵌入了水印的图像之间的相似性。为了比较水印图像与原始图像的清晰度，通过峰值信噪比(PSNR)进行不可见性分析。峰值信噪比的定义如下：

$$PSNR = 20\log_{10}\left(\frac{MAX_C}{\sqrt{MSE}}\right) \tag{20}$$

其中，MAX_C是图像 C 的最大像素值，而 MSE 是均方误差。对于两幅 $m \times n$ 单色图像，定义如下：

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[(C(i,j) - CW(i,j)^2)] \tag{21}$$

其中，C 表示载体图像，CW 表示水印图像。C 和 CW 越接近，MSE 越小，则 $PSNR$ 越大。

具体到嵌入算法中，如果 C 和 CW 分别表示隐藏信息前后的载体，则$(C(i,j) - CW(i,j))^2$的取值只有两种可能：要么为 0，要么为 1。此时，MSE 可以看作是在嵌入操作中被改变的像素的数量与像素总数的比率。假定一个像素的比特位被改变和不被改变的概率各为 0.5，则 $MSE = 0.5$，即载体图像中有一半的像素被改变。而对于一个 8 比特的图像来说，$MAX_C \approx 255$，则：

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{0.5}}\right) = 51.1411$$

即使最极端的情况，载体的每个像素都改变了，此时 $MSE = 1$，$PNSR$ 仍然可以达到 48.1308。实际的测试结果与理论分析结果相符，如图 17 和表 1 所示。

注：第一行是原始载体，第二行是含有隐藏信息的载体

图 17 嵌入水印后的视觉效果

Fig. 17 Visual effect after embedding watermark

表 1 PSNR

Table 1 PSNR

Carrier	lenna	mandrill	peppers	cameraman
PSNR	50.8426	50.3786	50.8852	51.6169

4.2 鲁棒性

鲁棒性指水印在攻击中生存的能力。误码率(Bit Error Rate，BER)和归一化相关系数(Normalized Correlation，NC)是较为常用的衡量鲁棒性的两个值。

4.2.1 误码率

误码率(BER)定义为 PSNR 的倒数。

$$BER=\frac{1}{PSNR} \tag{22}$$

BER 决定原始图像在水印过程中的更改。例如 $PSNR$ 为 50 dB，则 BER 将为 0.02，即在水印过程中 2% 位已改变。表 2 列出了模拟误码率值的计算结果。

表 2 BER

Table 2 BER

Carrier	lenna	mandrill	peppers	School4
BER	0.019 668 54	0.019 849 7	0.019 652 08	0.019 373 50

4.2.2 归一化相关系数

为定量地评价提取水印与原始水印信号的相似性，可采用归一化相关系数作为评价标准。假设原始的水印为 W，提取的水印为 W'，其定义为：

$$NC(W,W')=\frac{\sum_{k=0}^{2^{n-p_1}}\sum_{l=0}^{2^{n-p_2}-1}(2w_{k,l}-1)\times(2w'_{k,l}-1)}{2^{2n-p_1-p_2}}$$

$$=1-2BER(W,W') \tag{23}$$

其中，$w_{k,l}-1$ 的作用是将水印比特 0 和 1 分别转换为 -1 和 $+1$。因此当 $w_{k,l}=w'_{k,l}$ 时，$(2w_{k,l}-1)(2w'_{k,l}-1)$ 的值为 1；当 $w_{k,l}\neq w'_{k,l}$ 时，$(2w_{k,l}-1)(2w'_{k,l}-1)$ 的值为 -1，因此有 $NC=1-2BER$ 这个关系。

在本文的仿真中，为了分析算法对攻击的抵抗力，我们考虑了用于水印图像上的 5 种不同类型的攻击(Crop 攻击、Filter 攻击、Noise 攻击、Resize 攻击、Rotate 攻击)。提取攻击后的标记图像并计算对应的 NC，可以获取初始和提取的水印图像之间的相似性。攻击后提取水印的归一化相关系数如图 18 所示，攻击后的图像如图 19 所示。

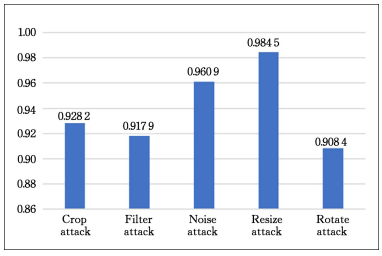


图 18 攻击后提取水印的归一化相关系数图

Fig. 18 Normalized correlation coefficient of extracted watermark after attack

图 19 遭受攻击后的图像

Fig. 19 Image after attack

分析图 18 和图 19 给出的结果，可以判断建议的水印方案具有良好的抗干扰能力。图 20 给出了攻击后提取的水印图像，表明该水印可以识别并且该算法具有良好的抗攻击性。

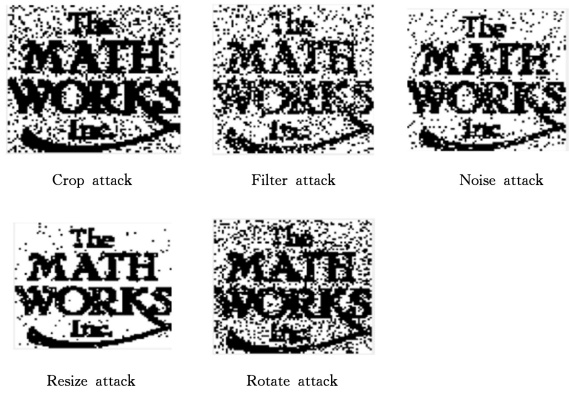


图 20 攻击后提取的水印

Fig. 20 Extracting watermark after attack

4.3 算法复杂度与安全性分析

量子计算的复杂性取决于基本量子门的个数，忽略复杂度的系数以及计算准备工作的复杂度，对大小为 $N=2^n$ 的矢量而言，传统离散小波变换的计算复杂度为 $O(2^n)$，量子小波变换的计算复杂度为 $O(n^2)$，大大提升了算法的时间复杂度。

基于量子小波变换的图像水印算法可用于嵌入水印，达到版权保护的目的。如果是图像作为水印，则嵌入水印前还需要对水印图像进行置乱操作，置乱算法是可知的，但置乱所需要的密码只有嵌入者或版权所有者拥有，提取出来的水印也是乱码，只有经过置乱的逆操作才能恢复水印图片。

4.4 与其他算法的对比分析

一个较好的水印算法应该能够在给定条件下嵌入更多的隐秘信息。为了保证嵌入容量，设置量子小波变换级数为 2，阈值为 5，则经过一次嵌入后即可达到图像尺寸大小的嵌入量，表 3 列出了测试图像在该条件下嵌入水印后的 PSNR 值与 Mou 等[2]在相同嵌入容量下的 PSNR 值的对比结果。

表 3 相同嵌入率下的 *PSNR* 对比

Table 3 Comparison of *PSNR* under the same embedding rate

(单位：dB)

Picture name	Mou et al	Algorithm in this paper
lenna	46.397 6	50.842 6
mandrill	41.572 9	50.378 6
peppers	45.336 6	50.885 2
cameraman	46.303 6	51.616 9

从表 3 可以看出，在相同的嵌入率条件下，同样的图片，本文基于新的量子小波变换的图像水印算法具有更高的 $PSNR$ 值，即含水印的载体图像与原载体图像的匹配度更高。

结束语 任何适用的水印方案都必须具有两个关键特性：不可见性和鲁棒性。不可见性意味着在原始图像和带水印的图像之间存在可接受的相似性。鲁棒性指方案对攻击的抵抗力。在这里，我们介绍了一种新的基于量子小波变换的图像水印方案，其具有可接受的不可见性。在该方案中，采用量子小波变换，在灰度图像中嵌入一幅 $2^n\times 2^n$ 大小的二值图像，为了获得更好的安全性，在嵌入之前对水印图像进行置乱，然后采用量子 LSB 分块技术和对载体图像进行量子小波变换，将水印图像嵌入载体图像。通过对嵌入和置乱过程

进行版本设置，版权所有者可以简单地提取水印图像。

为了评估该方案的性能，对其进行了仿真，其中通过计算峰值信噪比(PSNR)确认了方案的不可见性特征，通过检查误码率(BER)数量和归一化相关系数(NC)证明了该方案的鲁棒性。利用量子计算的量子并行性使小波算法的时间复杂度大大提升了，从经典计算的指数级到现在的(n^2)。

综上所述，与之前的水印方案相比，本文方案的优点和有效性可总结为两点。1)通过引入置乱方法，将水印图像转换为置乱后的图像，该置乱后的图像具有良好的鲁棒性，表明原始水印图像不会被任何攻击者恢复，即使他提取了被扰乱的二进制图像。2)与之前的方案相比，我们的方案不仅满足不可见性，而且含水印的载体图像与原载体图像具有较高的匹配度。

本文只是对基于量子小波变换的图像水印算法进行初步探讨，还有许多算法需要进一步探索，如量子进化算法、量子进化算法与遗传算法相结合、量子进化算法与量子粒子群优化算法等。除此之外，还可以对现有算法进行改进，如改进量子进化算法的进化策略、改进量子图像表达策略等都是改进现有基于量子小波变换的图像水印算法的不错选择。

参 考 文 献

[1] ZHU J N. Research status and Prospect of quantum watermarking technology[J]. Journal of Higher Correspondence Education(Natural Science Edition), 2011, 24(5): 8-10.

[2] MOU Q G, JIANG T F, LIU J. Image watermarking algorithm based on quantum Haar wavelet transform[J]. Information Network Security, 2015, (6): 55-60.

[3] WANG N, LIN S. Quantum image watermarking based on quantum least significant bit[J]. Journal of Quantum Electronics, 2015, 32(3): 263-269.

[4] JIANG N, WANG L. A novel strategy for quantum image steganography based on Moire pattern[J]. International Journal of Theoretical Physics, 2015, 54(3): 1021-1032.

[5] LI T, HE H X, ZHAI Z G. An adaptive quantum steganography algorithm based on watermark quantum image[J]. Computer Application Research, 2018, 35(2): 503-506, 526.

[6] JI S, CHEN S Y, ZHAI Z G. A secure large capacity quantum image watermarking protocol[J]. Computer Engineering, 2018, 44(5): 234-239.

[7] QU Z G, CHEN S Y, WANG X J. A secure controlled quantum image steganography algorithm[J]. Quantum Information Processing, 2020, 19(10): 1531-1540.

[8] ZHANG Y, LU K, GAO Y H, et al. NEQR: a novel enhanced quantum representation of digital images[J]. Quantum Information Processing, 2013, 12(26): 2833-2860.

[9] VEDRAL V, BARENCO A, EKERT A. Quantum networks for elementary arithmetic operations[J]. Physical Review A, 1996, 54(1): 147-153.

[10] NIELSEN M A, CHUANG T L, ZHAO Q C. Quantum computing and quantum information(I)-quantum computing part [M]. Beijing: Tsinghua University Press, 2009.

[11] FIJANY A, WILLIAMS C P. Quantum Wavelet Transform: Fast Algorithm and Complete Circuit[C]// Quantum Computing and Quantum Communications. Berlin, Heidelberg: Springer, 1999: 10-33.

[12] ZHANG Z L, SUN L. Design and application of quantum Haar wavelet transform algorithm[J]. Computer Engineering and Design, 2008, 29(11): 2816-2820.

[13] JIANG N, WANG L. Analysis and improvement of the quantum Arnold image scrambling[J]. Quantum Information Processing, 2014, 13(7): 1545-1551.

SU Yonghong, born in 1980, master, lecturer. Her main research interests include network information security and information retrieval.

XIA Ting, born in 1983, master, associate professor. Her main research interests include embedded technology and artificial intelligence.