中国科学: 物理学 力学 天文学 2026 年 第 56 卷 第 10 期: 109525
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文

量子图像鲁棒零水印算法

叶天语[1,2*], 曹嘉鹏[1], 杨胜天[1]

1. 浙江工商大学信息与电子工程学院, 杭州 310018
2. 赤峰工业职业技术学院, 赤峰 024000
*联系人, E-mail: yetianyu@zjgsu.edu.cn

收稿日期: 2026-02-18; 接受日期: 2026-03-19; 网络出版日期: 2026-09-11
国家自然科学基金(编号: 62071430)和浙江省属高校基本科研业务费专项(编号: JRK21002)资助项目

摘要 量子图像水印算法的鲁棒性与不可感知性往往相互制约. 为了解决这一矛盾, 本文提出一种基于数字图像新型增强量子表示(Novel Enhanced Quantum Representation, NEQR)模型的量子图像鲁棒零水印算法, 并为其设计了相应的量子线路. 该算法利用图像子块像素灰度值均值与图像所有像素灰度值均值之间的大小比较产生鲁棒特征零水印. 该算法的量子线路复杂度为$O(k^2)$, 其中k为正方形图像的高或宽, 相比于经典计算机的运行有着明显的优势. 而且, 该算法针对各种不同类型攻击总体上具备较强的鲁棒性.

关键词 量子图像水印, 鲁棒水印, 零水印, 均值, 量子线路复杂度

PACS: 03.67.Lx, 42.30.Va, 42.30.Sy

1 引言

量子计算利用量子叠加和纠缠等特性, 将量子力学与经典计算结合起来, 在因子分解、组合优化等问题上已表现出优于经典计算的性能[1]. 量子计算的发展为量子图像处理带来了新的机遇, 目前已衍生出量子图像滤波、量子图像加密、量子图像隐写、量子图像水印等新领域.

量子图像水印近些年吸引了越来越多研究人员的关注. 根据抗攻击性能, 量子图像水印算法可被划分为量子图像鲁棒水印算法、量子图像脆弱水印算法和量子图像半脆弱水印算法. 在量子图像鲁棒水印算法方面, 2017年, Zhou等人[2]提出一种基于Arnold置乱和最低有效位(Least Significant Bit, LSB)隐写的量子图像鲁棒水印算法; 2018年, Luo等人[3]提出一种增强型LSB量子图像鲁棒水印算法; 2019年, Hu等人[4]提出一种基于量子图像灵活表示(Flexible Representation of Quantum Images, FRQI)模型和Haar小波变换的量子图像鲁棒水印算法; 2019年, Hu等人[5]提出一种基于Gray码变换和LSB隐写的量子图像鲁棒水印算法; 2021年, Zeng等人[6]提出一种基于最大像素灰度值差分分割、LSB替换和Tent映射的量子图像鲁棒水印算法; 2022年, Zeng等人[7]提出一种基于量子Haar小波变换和Henon映射的量子图像鲁棒水印算法; 2024年, 孙文韬等人[8]提出了一种基于图像子块分类和LSB替换的高容量量子图像鲁棒水印算法; 2024年, Xing等人[9]

引用格式: 叶天语, 曹嘉鹏, 杨胜天. 量子图像鲁棒零水印算法. 中国科学: 物理学 力学 天文学, 2026, 56: 109525
Ye T-Y, Cao J-P, Yang S-T. Quantum image robust zero-watermarking algorithm (in Chinese). Sci Sin-Phys Mech Astron, 2026, 56: 109525, doi: 10.1360/SSPMA-2026-0101

© 2026《中国科学》杂志社

提出了一种基于子块位平面中心对称扩张以及亮度水印嵌入和提取机制的多模量子图像鲁棒水印算法; 2024年, Zhou等人[10]提出了一种量子离散余弦变换和Baker映射的量子图像鲁棒水印算法; 2025年, Qiu等人[11]提出了一种基于DNA编码和量子纠错的量子图像鲁棒水印算法.

不难发现, 以上量子图像鲁棒水印算法都是将外在水印图像嵌入到原始载体图像以实现抗攻击鲁棒性. 然而, 量子图像水印算法的鲁棒性与不可感知性往往相互制约. 为了解决这一矛盾, 本文借鉴经典零水印思想[12]提出一种新颖的量子图像鲁棒零水印算法, 并为其设计了相应的量子线路. 该算法利用"图像子块像素灰度值均值与图像像素灰度值均值之差的符号在被扰动前后存在稳定性"这一特点来从原始载体图像产生原始特征鲁棒零水印. 仿真实验结果表明, 该算法针对各种不同类型攻击均具备较强的鲁棒性. 就我们所知, 本文算法是目前首个量子图像鲁棒零水印算法.

2　基础知识

2.1　算法的数学理论基础

灰度数字图像从数学角度可被视为一个二维矩阵. 假设灰度数字图像A的大小为$M\times L$, 那么其可被表示为

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1L} \\ a_{21} & a_{22} & \cdots & a_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ a_{M1} & a_{M2} & \cdots & a_{ML} \end{bmatrix}, \tag{1}$$

其中a_{ij}为A的第i行第j列的像素的灰度值, $i\in\{1,2,\cdots,M\}$且$j\in\{1,2,\cdots,L\}$. 对图像采取的添加噪声、滤波等操作本质上可被视为对其施加的扰动. 假设对数字图像A施加的扰动为E, 那么施加扰动后的图像为

$$\widehat{A}=A+E. \tag{2}$$

根据文献[13], 此时存在

$$\text{average}(\widehat{A})-\text{average}(A)=\text{average}(E), \tag{3}$$

其中average(·)为计算图像像素灰度值均值的函数, 被定义为

$$\text{average}(A)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{L}a_{ij}}{ML}. \tag{4}$$

根据式(3)和赫尔德不等式, 存在

$$|\text{average}(\widehat{A})-\text{average}(A)|=|\text{average}(E)|\leqslant\frac{\|E\|}{\sqrt{ML}}, \tag{5}$$

其中$\|E\|$代表计算E的范数. 根据式(5), 当$\sqrt{ML}\gg\|E\|$时, 存在$\text{average}(\widehat{A})\approx\text{average}(A)$, 这说明数字图像$A$在被扰动前后的像素灰度值均值具有稳定性.

将数字图像A分成一系列大小为$m\times l$的不重叠均匀子块, 记A的第s行第t列的子块为A_{st}, 其中$s\in\left\{1,2,\ldots,\frac{M}{m}\right\}$, $t\in\left\{1,2,\ldots,\frac{L}{l}\right\}$. 对应于式(3), 存在

$$\text{average}(\widehat{A}_{st})-\text{average}(A_{st})=\text{average}(E_{st}). \tag{6}$$

对应于式(5), 存在

$$\left|\text{average}(\widehat{A}_{st})-\text{average}(A_{st})\right|=\left|\text{average}(E_{st})\right|\leqslant\frac{\|E_{st}\|}{\sqrt{ml}}. \tag{7}$$

根据式(7), 当$\sqrt{ml}\gg\|E_{st}\|$时, 存在$\text{average}(\widehat{A}_{st})\approx\text{average}(A_{st})$.

根据文献[13], $\text{average}(E_{st})$近似地服从均值为$\text{average}(E)$、方差为σ^2的正态分布, 其中σ^2往往比较小. 根据切比雪夫不等式, 对于任意的$\delta>0$, 存在

$$P\left\{\left|\text{average}(E_{st})-\text{average}(E)\right|<\delta\right\}\geqslant 1-\frac{\sigma^2}{\delta}, \tag{8}$$

其中$P(x)$表示事件x发生的概率. 将式(3)和(6)代入式(8)可得,

$$\begin{aligned} &P\left\{\left|\left(\text{average}(\widehat{A}_{st})-\text{average}(A_{st})\right)\right.\right. \\ &\left.\left.-(\text{average}(\widehat{A})-\text{average}(A))\right|<\delta\right\} \\ &=P\left\{\left|\left(\text{average}(\widehat{A}_{st})-\text{average}(\widehat{A})\right)\right.\right. \\ &\left.\left.-\left(\text{average}(A_{st})-\text{average}(A)\right)\right|<\delta\right\} \\ &\geqslant 1-\frac{\sigma^2}{\delta}. \end{aligned} \tag{9}$$

式(9)说明, $\text{average}(\widehat{A}_{st})-\text{average}(\widehat{A})$依概率收敛于$\text{average}(A_{st})-\text{average}(A)$. 可以得出, $\text{sgn}\left(\text{average}(\widehat{A}_{st})-\text{average}(\widehat{A})\right)$依概率等同于$\text{sgn}(\text{average}(A_{st})-\text{average}(A))$, 其中sgn(·)为符号函数. 这说明图像子块像素灰度值均值与图像像素灰度值均值之差的符号在被扰动前后具有稳定性.

2.2　数字图像的新型增强量子表示模型

数字图像的新型增强量子表示(Novel Enhanced Quantum Representation, NEQR)模型在2013年被Zhang等人[14]首次提出. 根据NEQR模型, 一个大小为$2^k\times 2^k$的2^q灰度级图像I可被表示为

$$|I\rangle=\frac{1}{2^k}\sum_{Y=0}^{2^k-1}\sum_{X=0}^{2^k-1}|I_{YX}\rangle\otimes|YX\rangle, \tag{10}$$

其中,

$$|YX\rangle=|Y\rangle|X\rangle=|y_{k-1}y_{k-2}\cdots y_0\rangle|x_{k-1}x_{k-2}\cdots x_0\rangle, \tag{11}$$

为垂直位置Y和水平位置X一起构成的乘积态, 其中$y_i,x_i\in\{0,1\}$, $i=0,1,\ldots,k-1$;

$$|I_{YX}\rangle=|I_{YX}^{q-1}I_{YX}^{q-2}\ldots I_{YX}^{0}\rangle, \tag{12}$$

是水平位置为X和垂直位置为Y的像素灰度值I_{YX}对应的量子态, 且$I_{YX}^{j}\in\{0,1\}$, $j=0,1,\ldots,q-1$. 显然, NEQR模型使用$2k+q$个量子比特来构建一个大小为$2^k\times 2^k$的2^q灰度级图像, 其中$2k$个量子比特用于编码像素的位置信息, q个量子比特用于编码像素的颜色信息. 对于图1所示的2×2图像, 其NEQR模型可被表示为

$$\begin{aligned}|I\rangle=&\frac{1}{2}(|0\rangle|00\rangle+|255\rangle|01\rangle+|128\rangle|10\rangle+|65\rangle|11\rangle)\\=&\frac{1}{2}(|00000000\rangle|00\rangle+|11111111\rangle|01\rangle\\&+|10000000\rangle|10\rangle+|01000001\rangle|11\rangle).\end{aligned} \tag{13}$$

2.3　量子图像分块

只要将NEQR图像的部分垂直位置和部分水平位置都分别限定于特定值, 就可实现对其进行分块操作. NEQR图像的分块操作具体可被描述为: 文献[15]将大小为$2^k\times 2^k$的图像I划分为$2^{k-p_1}\times 2^{k-p_2}$个大小为$2^{p_1}\times 2^{p_2}$的不重叠子块, 需将垂直位置$Y$分成$|y_{k-1}y_{k-2}\cdots y_{p_1}\rangle$和$|y_{p_1-1}y_{p_1-2}\cdots y_0\rangle$两部分以及将水平位置$X$分成$|x_{k-1}x_{k-2}\cdots x_{p_1}\rangle$和$|x_{p_1-1}x_{p_1-2}\cdots x_0\rangle$两部分, 其中$p_1,p_2\in\{0,1,\cdots,k\}$, $|y_{k-1}y_{k-2}\cdots y_{p_1}\rangle$和$|x_{k-1}x_{k-2}\cdots x_{p_1}\rangle$是块间坐标, $|y_{p_1-1}y_{p_1-2}\cdots y_0\rangle$和$|x_{p_1-1}x_{p_1-2}\cdots x_0\rangle$是块内坐标.

00 00000000	01 11111111
10 10000000	11 01000001

图 1　2×2图像示例图
Figure 1　Example of a 2×2 image.

2.4　可逆并行加法器

可逆并行加法器(Reverse Parallel Adder, RPA)[16]的量子线路和示意图如图2所示, 其作用是求出A和B之和, 其中可逆半加法器(Reverse Half Adder, RHA)的量子线路和示意图如图3所示, 可逆全加法器(Reverse Full Adder, RFA)的量子线路和示意图如图4所示. 根据图2, 对于两个输入量子态序列$|A\rangle=|a_{n-1}a_{n-2}\cdots a_0\rangle$和$|B\rangle=|b_{n-1}b_{n-2}\cdots b_0\rangle$, RPA会输出量子态序列$|A+B\rangle=|r_{n-1}r_{n-2}\cdots r_0\rangle$, 从而得到$A$和$B$之和. 这里, $a_i,b_i,r_i\in\{0,1\}$, $i=0,1,\ldots,n-1$; V是非门的平方根, 被定义为

$$V=\frac{1+\mathrm{i}}{2}\begin{bmatrix}1 & -\mathrm{i}\\ -\mathrm{i} & 1\end{bmatrix}, \tag{14}$$

$V^{\dagger}$是V的厄米共轭矩阵.

2.5　除数为4的除法器

除数为4的除法器(Dividing 4, D4)[17]的量子线路和示意图如图5所示, 其作用是求出A除以4后的值. 根据图5, B为A除以4后的值, 通过$2n+1$个量子交换门实现. 这里, $A=a_{n-1}a_{n-2}\ldots a_0$, $B=b_{n-1}b_{n-2}\ldots b_0$, $a_i,b_i\in\{0,1\}$, $i=0,1,\ldots,n-1$.

2.6　量子比较器(Quantum Comparator, QC)

量子比较器[18]的量子线路和示意图如图6所示, 其作用是比较A和B的大小, 其中$A=a_{n-1}a_{n-2}\ldots a_0$, $B=b_{n-1}b_{n-2}\ldots b_0$, $a_i,b_i\in\{0,1\}$, $i=0,1,\ldots,n-1$. QC

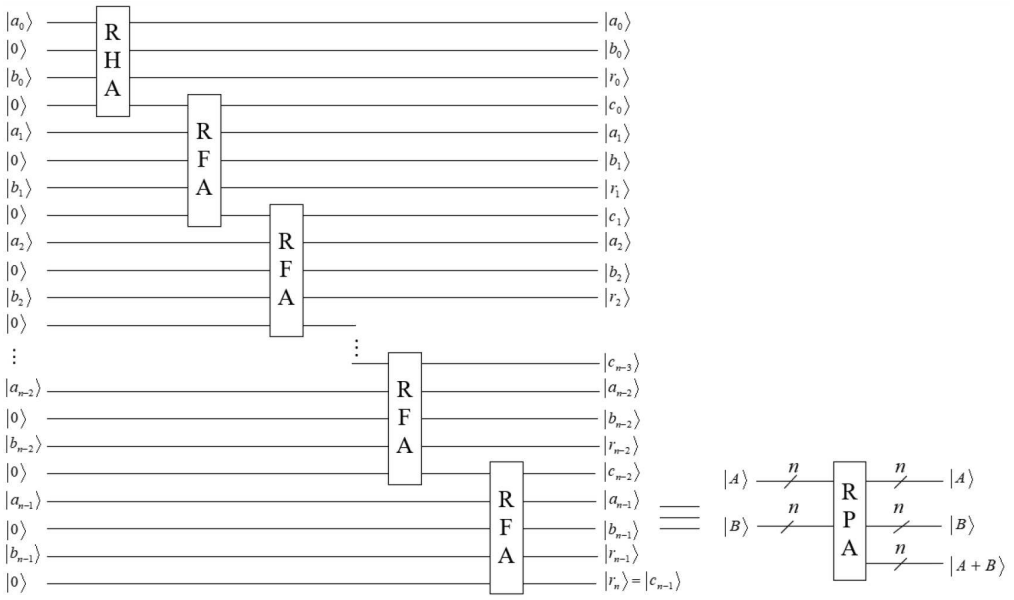


图 2　RPA的量子线路和示意图
Figure 2　Quantum circuit and schematic diagram of RPA.

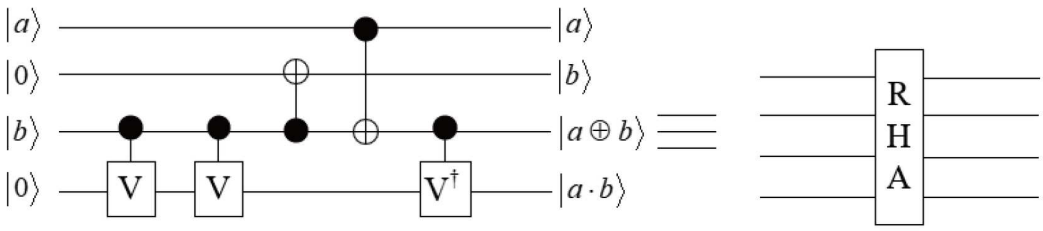


图 3　RHA的量子线路和示意图
Figure 3　Quantum circuit and schematic diagram of RHA.

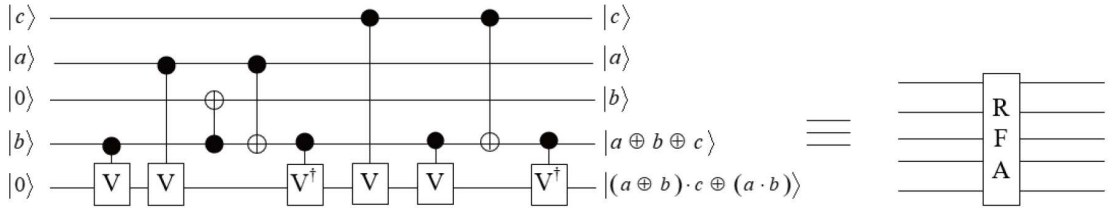


图 4　RFA的量子线路和示意图
Figure 4　Quantum circuit and schematic diagram of RFA.

输出c_1c_0=10则表明$A>B$, 输出c_1c_0=01则表明$A<B$, 输出c_1c_0=00则表明$A=B$.

3　所提出的量子图像鲁棒零水印算法

这里假设原始灰度载体图像I的大小为$2^k\times2^k$. 所提出的量子图像鲁棒零水印算法由原始鲁棒特征零水印产生过程和攻击后的鲁棒特征零水印产生过程构成.

(1) 原始鲁棒特征零水印产生过程

所提出算法的原始鲁棒特征零水印产生过程由以下四个步骤构成.

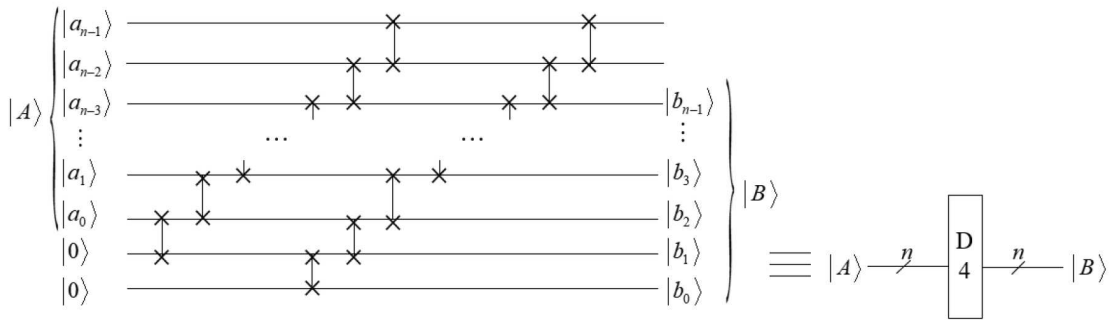


图 5　D4的量子线路和示意图
Figure 5　Quantum circuit and schematic diagram of D4.

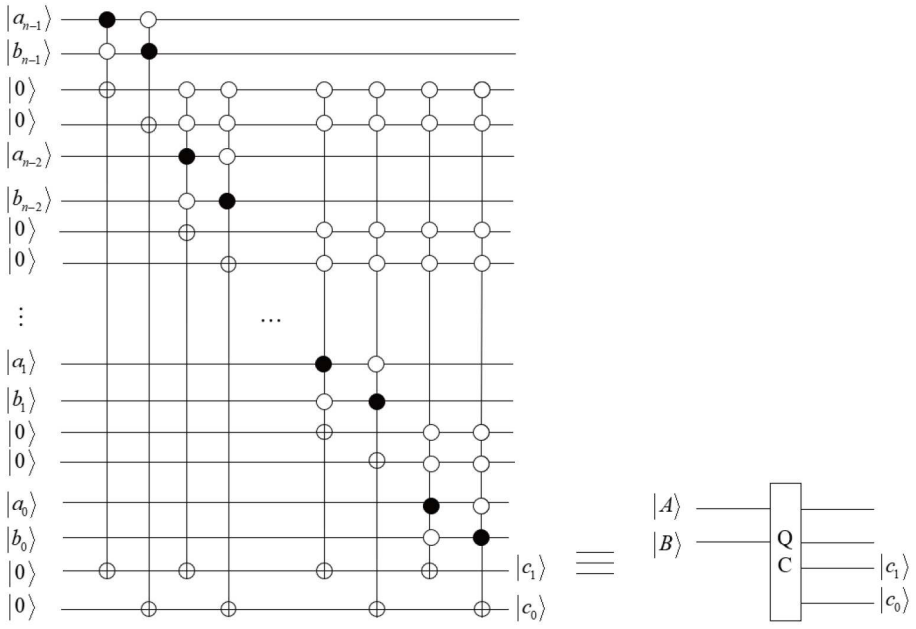


图 6　QC的量子线路和示意图
Figure 6　Quantum circuit and schematic diagram of QC.

步骤1: 将I转化为两幅相同的NEQR量子图像$|I\rangle$, 从而得到

$$|I\rangle = \frac{1}{2^k}\sum_{Y=0}^{2^k-1}\sum_{X=0}^{2^k-1}|I_{YX}\rangle\otimes|YX\rangle, \tag{15}$$

其中

$$|I_{YX}\rangle = |I_{YX}^{q-1}I_{YX}^{q-2}\ldots I_{YX}^{0}\rangle,$$
$$|YX\rangle = |Y\rangle|X\rangle = |y_{k-1}y_{k-2}\ldots y_0\rangle|x_{k-1}x_{k-2}\ldots x_0\rangle,$$
$$I_{YX}^{j}\in\{0,1\},\ j=0,1,\ldots,q-1,\ y_i,x_i\in\{0,1\},$$
$$i=0,1,\ldots,k-1.$$

步骤2: 计算一幅NEQR量子图像$|I\rangle$的所有像素灰度值的均值, 相应的量子线路如图7所示. 在图7(a)中, 首先利用文献[13]的方法将$|I\rangle$划分为$2^{2(k-1)}$个不重叠的2×2子块, 并通过3个RPA (即RPA1, RPA2和RPA3)和1个D4计算每个子块四个像素灰度值的均值, 最后再通过RPA4计算出$|I\rangle$的所有像素灰度值之和的四分之一. 这里, 第t个子块的结构如图8所示, 其中$|I_t(X,Y)\rangle$, $|I_t(X+1,Y)\rangle$, $|I_t(X,Y+1)\rangle$和$|I_t(X+1,Y+1)\rangle$为其四个像素, $t=1,2,\cdots,2^{2(k-1)}$; RPA4的左侧上面输入端需初始化为0. 在图7(b)中, 将图7(a)的最后输出作为第一个D4

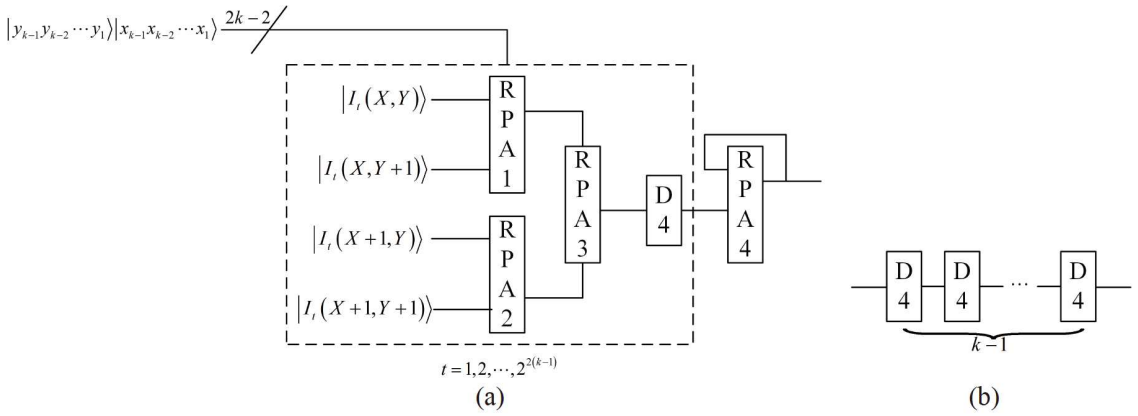


图 7　计算$|I\rangle$的所有像素灰度值的均值的量子线路. (a) 计算$|I\rangle$的所有像素灰度值之和的四分之一的量子线路. (b) $k-1$个D4级联的量子线路

Figure 7　Quantum circuit for calculating the average of all pixel grayscale values of $|I\rangle$. (a) Quantum circuit for calculating one quarter of sum of all pixel grayscale values of $|I\rangle$. (b) Quantum circuit for $k-1$ cascading D4 modules.

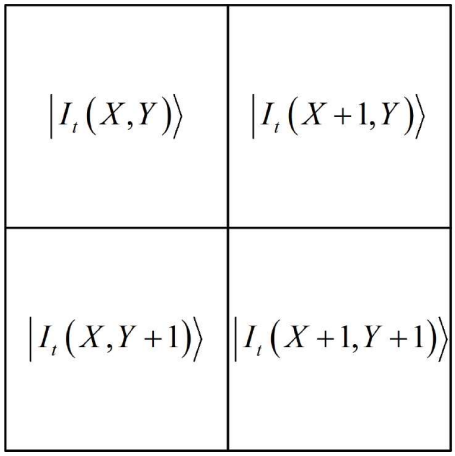


图 8　大小为2×2的原始载体图像块

Figure 8　Original carrier image block of size 2×2.

的输入，共经过$k-1$个D4计算出$|I\rangle$的所有像素灰度值的均值.

步骤3: 通过比较另一幅NEQR量子图像$|I\rangle$子块像素灰度值均值与图像所有像素灰度值均值之间的大小关系产生鲁棒特征零水印，相应的量子线路如图9所示. 在图9中，虚线框部分的量子线路用于计算第t个2×2子块四个像素灰度值的均值，然后通过QC将第t个子块四个像素灰度值的均值和$|I\rangle$所有像素灰度值的均值进行大小比较来产生第t个子块的鲁棒特征零水印比特W_t，其中QC的c_1输出便是W_t，$t=1,2,\cdots,2^{2(k-1)}$. 记$W=\{W_1,W_2,\cdots,W_{2^{2(k-1)}}\}$为从$|I\rangle$产生的鲁棒特征零水印.

(2) 攻击后的鲁棒特征零水印产生过程

记载体图像I遭攻击后被转变成$\hat{I}$. 用$\hat{I}$替换I, 然后重复上述三个步骤，就可从$\hat{I}$产生攻击后的鲁棒特征零水印$\hat{W}=\{\hat{W}_1,\hat{W}_2,\cdots,\hat{W}_{2^{2(k-1)}}\}$.

4　量子线路复杂度分析

量子线路的复杂度取决于基本量子门的数量，这是因为任意复杂的量子门都可由基本量子门组合而成. 非门、控制非(Controlled-Not, CNOT)门等都是基本量子门[19].

文献[20]指出，Toffoli门是由6个CNOT门构成; 控制量子比特均为1的n-CNOT门($n\geqslant 3$)是由$2(n-1)$个Toffoli门和1个CNOT门构成; 当n-CNOT门($n\geqslant 3$)的所有控制量子比特都是0时, 可使用$2n$个非门将它们都转变成1. 因此, n-CNOT门($n\geqslant 3$)的量子线路复杂度不会超过$2(n-1)\times 6+1+2n=14n-11$.

n量子比特RPA由1个RHA和$n-1$个RFA构成，而RHA包含5个CNOT门，RFA包含9个CNOT门，因此n量子比特RPA共包含$5+9(n-1)=9n-4$个CNOT门. n量子比特D4由$2n+1$个交换门构成，而交换门等价于3个CNOT门，因此n量子比特D4等价于$3(2n+1)$个CNOT门. 关于n量子比特QC, 文献[21]指出，其是由$24n^2+6n$个CNOT门构成.

接下来计算本文算法的量子线路复杂度. 在图7(a)中，RPA1和RPA2都是被$2k-2$个量子比特控制的q量子比特RPA (每个等价于1个被$2k-2$个量子比特控

制的RHA 和7个被$2k-2$个量子比特控制的RFA, 即$9q-4$个$2k-1$-CNOT门), RPA3是$q+1$量子比特RPA, D4是$q+2$量子比特D4, RPA4是$2k+q-3$量子比特RPA, 因此图7(a)共包含$2\times(9q-4)\times[14\times(2k-1)-11]+9\times(q+1)-4+3\times[2\times(q+2)+1]+q\times(2k+q-3)-4$个CNOT门, 其量子线路复杂度为$O(k)$. 在图7(b)中, D4都是$2k+q-2$量子比特D4, 因此图7(b)共包含$3\times[2\times(2k+q-2)+1]\times(k-1)$个CNOT门, 其量子线路复杂度为$O(k^2)$. 在图9中, RPA1和RPA2都是被$2k-2$个量子比特控制的$q$量子比特RPA (每个等价于1个被$2k-2$个量子比特控制的RHA 和7个被$2k-2$个量子比特控制的RFA, 即$9q-4$个$2k-1$-CNOT门), RPA3是$q+1$量子比特RPA, D4是$q+2$量子比特D4, QC是$q+2$量子比特QC, 因此图9共包含$2\times(9q-4)\times[14\times(2k-1)-11]+9\times(q+1)-4+3\times[2\times(q+2)+1]+24\times(q+2)^2+6\times(q+2)$个CNOT门, 其量子线路复杂度为$O(k)$. 综上所述, 本文算法的量子线路复杂度为$O(k^2)$.

由于k一般远远大于4, 根据表1, 在量子线路复杂度上, 本文算法优于文献[3–5,7,8]的算法, 等价于文献[6,10]的算法, 逊色于文献[2,9]的算法. 文献[2–11]的算法都需将外在水印嵌入原始载体图像, 而本文算法无需将外在水印嵌入原始载体图像, 从而会节省相应的量子操作. 另外, 经典计算机运行本文算法的线路复杂度为$O(2^{2k})$. 相比于经典计算机, 本文算法的量子线路复杂度有着明显的优势, 其原因在于量子计算的并行性.

5　仿真实验结果与分析

由于实用可靠量子计算机仍处于早期研究阶段, 受限于目前量子硬件条件短缺, 本文使用在经典计算机上运行MATLAB R2023b的方式对所提出的量子图像鲁棒零水印算法进行仿真实验. 实验所用原始载体图像是大小均为512×512的8位灰度图像Pepper.bmp, Baboon.bmp和Aerial.bmp, 分别如图10(a)–(c)所示. 这里采用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)来计算原始载体图像I和攻击后的载体图像$\hat{I}$之间的视觉差异, 以评价攻击强度; PSNR被定义为

$$\mathrm{PSNR}=20\log_{10}\frac{\mathrm{Max}I}{\sqrt{\dfrac{1}{MN}\sum\limits_{i=0}^{M-1}\sum\limits_{j=0}^{N-1}\left(I(i,j)-\hat{I}(i,j)\right)^2}}, \tag{16}$$

其中Max$I$是I的最大像素值, $M\times N$是I的大小, $I(i,j)$是I的第i行第j列的像素的灰度值. 同时, 这里采用归一化相关度(Normalized Correlation, NC)来计算原始鲁棒特征零水印W和攻击后提取的鲁棒特征零水印$\hat{W}$之间的相关程度, 以评价算法的鲁棒性; NC被定义为

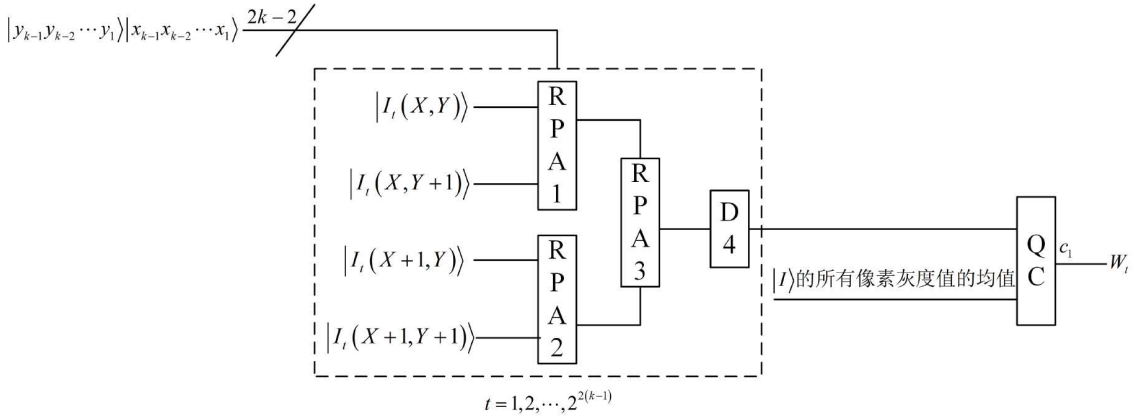


图 9　产生鲁棒特征零水印的量子线路

Figure 9　Quantum circuit for generating robust feature zero-watermark.

表 1　不同量子图像鲁棒水印算法的量子线路复杂度对比

Table 1　Comparison of quantum circuit complexity of different quantum image robust watermarking algorithms

本文算法	文献[2]的算法	文献[3]的算法	文献[4]的算法	文献[5]的算法	文献[6]的算法	文献[7]的算法	文献[8]的算法	文献[9]的算法	文献[10]的算法
$O(k^2)$	$O(k)$	$O(k2^{2k})$	$O(k2^{2k-2})$	$O(k2^{2k})$	$O(k^2)$	$O(k^3)$	$O(2^k)$	$O(k)$	$O(k^2)$

$$\mathrm{NC}=\frac{\sum_{t=1}^{T} W_t \widehat{W}_t}{\sqrt{\sum_{t=1}^{T} W_t^2}\sqrt{\sum_{t=1}^{T} \widehat{W}_t^2}}, \tag{17}$$

其中T为鲁棒特征零水印的总比特数. 在本文提出的算法中, $M=N=2^k$以及$T=2^{2(k-1)}$.

在无噪环境下, 本文算法提取出的特征水印和原始特征水印之间的NC为1. 由于量子图像在量子信道中传输时所遭受的攻击难以被刻画, 这里采用对经典图像发起攻击来进行鲁棒性检验仿真实验. 鲁棒性检验仿真实验结果被列在表1–5中, 其中"/"上方为NC, "/"下方为PSNR. 这里, 重采样使用Nearest插值法; 中间随机删除行是指从被删除行的下边第1行开始逐行向上移动且将空余行补全黑; 向下偏移行是指在图像下移几行后将最下面几行移出丢弃且将最上面几行补全黑; 向右偏移列是指在图像右移几列后将最右侧几列移出丢弃并将最左侧几列补全黑. 根据表2–6, 在抵抗添加椒盐噪声、添加高斯噪声、JPEG压缩攻击、

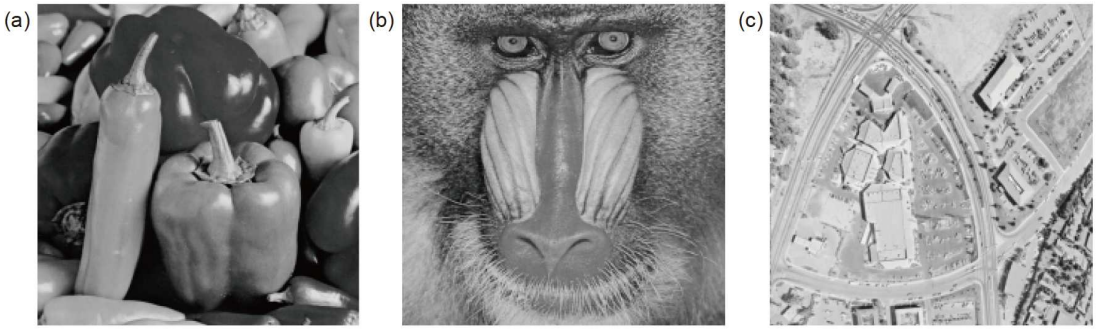


图 10　实验所用的三幅原始载体图像. (a) Pepper. (b) Baboon. (c) Aerial
Figure 10　Three original carrier images used in the experiments. (a) Pepper. (b) Baboon. (c) Aerial.

表 2　添加椒盐噪声和添加高斯噪声的实验结果
Table 2　Experimental results of adding salt & pepper noise and Gaussian noise

	添加椒盐噪声					添加高斯噪声				
	噪声密度为0.01	噪声密度为0.02	噪声密度为0.03	噪声密度为0.04	噪声密度为0.05	均值为0, 方差为0.001	均值为0, 方差为0.002	均值为0, 方差为0.003	均值为0, 方差为0.004	均值为0, 方差为0.005
Pepper	0.9922/ 24.9625	0.9862/ 21.9924	0.9797/ 20.2680	0.9742/ 19.0175	0.9667/ 18.1268	0.9903/ 30.0903	0.9872/ 27.1223	0.9839/ 25.4279	0.9813/ 24.1799	0.9795/ 23.2386
Baboon	0.9865/ 25.3572	0.9742/ 22.5210	0.9606/ 20.7125	0.9500/ 19.4220	0.9361/ 18.3240	0.9709/ 29.9630	0.9583/ 26.9765	0.9485/ 25.2170	0.9408/ 23.9694	0.9352/ 23.0340
Aerial	0.9825/ 25.0991	0.9659/ 22.0109	0.9463/ 20.2055	0.9298/ 18.9034	0.9137/ 17.9419	0.9718/ 30.0121	0.9600/ 26.9846	0.9518/ 25.2568	0.9433/ 24.0145	0.9354/ 23.0447

表 3　JPEG压缩攻击的实验结果
Table 3　Experimental results of JPEG compression attack

	JPEG压缩攻击									
	质量因子为10	质量因子为20	质量因子为30	质量因子为40	质量因子为50	质量因子为60	质量因子为70	质量因子为80	质量因子为90	质量因子为100
Pepper	0.9840/ 29.2447	0.9891/ 31.5356	0.9920/ 32.6743	0.9931/ 33.3581	0.9936/ 33.9084	0.9943/ 34.4395	0.9952/ 35.1300	0.9964/ 36.0656	0.9978/ 38.1971	0.9997/ 57.4620
Baboon	0.9257/ 22.5293	0.9507/ 24.3669	0.9636/ 25.5517	0.9687/ 26.4833	0.9730/ 27.3317	0.9773/ 28.2496	0.9818/ 29.5753	0.9865/ 31.6957	0.9928/ 36.1949	0.9991/ 57.5013
Aerial	0.9413/ 25.8052	0.9649/ 28.2308	0.9727/ 29.6114	0.9782/ 30.5896	0.9802/ 31.3926	0.9838/ 32.2281	0.9862/ 33.3967	0.9898/ 35.2051	0.9942/ 38.9503	0.9993/ 58.5020

表 4　高斯低通滤波、中值滤波和剪切的实验结果

Table 4　Experimental results of gaussian low-pass filtering, median filtering and cropping

	高斯低通滤波				中值滤波			剪切		
	窗口大小为2×2, 方差为0.5	窗口大小为3×3, 方差为0.5	窗口大小为4×4, 方差为0.7	窗口大小为5×5, 方差为0.7	窗口大小为3×3	窗口大小为4×4	窗口大小为5×5	左上角1/64	左上角1/32	左上角1/16
Pepper	0.9827/28.3623	0.9971/38.8811	0.9830/28.2917	0.9939/33.5423	0.9938/34.1210	0.9811/27.6769	0.9886/31.2445	0.9857/23.1847	0.9696/20.2390	0.9516/18.1556
Baboon	0.9258/22.5667	0.9805/30.7797	0.9240/22.3919	0.9580/25.3277	0.9403/22.8452	0.9018/20.7745	0.8924/20.4224	0.9729/23.0049	0.9450/19.8057	0.8982/16.9840
Aerial	0.9415/25.1340	0.9866/34.7709	0.9401/24.8919	0.9689/28.9634	0.9693/27.4293	0.9317/23.3774	0.9329/23.6122	0.9709/21.4994	0.9468/18.4508	0.8986/15.2226

表 5　重采样、随机删除行、逆时针旋转和向右偏移列的实验结果

Table 5　Experimental results of resampling, row random deletion, counterclockwise rotation and column rightward shifting

	重采样		随机删除行		逆时针旋转				向右偏移列	
	先缩小到0.8倍再放大到1.25倍	先缩小到0.5倍再放大到2倍	1行	2行	0.1°	0.2°	0.3°	0.4°	1列	2列
Pepper	0.9854/26.6974	0.9757/25.9784	0.9859/26.9748	0.9766/23.6739	0.9920/34.6495	0.9844/29.0001	0.9772/26.1763	0.9703/24.5584	0.9772/25.8296	0.9552/22.0107
Baboon	0.9441/22.9614	0.8883/19.4893	0.9439/21.9399	0.9057/19.6000	0.9565/26.1473	0.9118/20.6903	0.8761/18.3603	0.8500/17.6584	0.8999/20.1288	0.8296/17.0621
Aerial	0.9609/23.9557	0.9332/22.6191	0.9571/23.9466	0.9243/20.1492	0.9730/30.3887	0.9471/24.7245	0.9243/21.9638	0.9050/20.4561	0.9138/20.6583	0.8477/17.4197

表 6　随机删除列和向右下偏移行的实验结果

Table 6　Experimental results of column random deletion and row downward shifting

	随机删除列		向下偏移行	
	1列	2列	1行	2行
Pepper	0.9832/27.2780	0.9702/23.6604	0.9777/26.2531	0.9612/22.4340
Baboon	0.9395/22.6562	0.8943/19.5950	0.8789/17.7374	0.8071/15.9186
Aerial	0.9438/22.6699	0.9003/19.0653	0.9302/22.3767	0.8735/18.4297

高斯低通滤波、中值滤波、剪切、重采样、随机删除行、逆时针旋转、向右偏移列、向下偏移行和随机删除列上, 本文所提出的算法总体上具有较强的鲁棒性. 对于Baboon这种纹理较强的图像来说, 本文算法在向右偏移2列和向下偏移2行上的NC均小于0.84, 其抗攻击性能略差.

6　结论

本文首先从数学角度推导出“图像子块像素灰度值均值与图像像素灰度值均值之差的符号在被扰动前后具有稳定性”, 接着利用这一性质设计了一种新颖的基于NEQR模型的量子图像鲁棒零水印算法, 然后为其设计了相应的量子线路并计算出量子线路复杂度. 鲁棒性检验仿真实验结果表明, 所提出的算法针对各种不同类型攻击总体上具备较强的鲁棒性. 就我们所知, 所提出的算法是首个量子图像鲁棒零水印算法. 在未来, 我们将研究设计更多的性能优良的量子图像鲁棒零水印算法.

参考文献

1　Daley A J, Bloch I, Kokail C, et al. Practical quantum advantage in quantum simulation. Nature, 2022, 607: 667–676

2　Zhou R G, Hu W, Fan P. Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Inf Process, 2017, 16: 212

3 Luo G, Zhou R G, Hu W W, et al. Enhanced least significant qubit watermarking scheme for quantum images. Quantum Inf Process, 2018, 17: 299

4 Hu W W, Zhou R G, El-Rafei A, et al. Quantum image watermarking algorithm based on Haar wavelet transform. IEEE Access, 2019, 7: 121303–121320

5 Hu W W, Zhou R G, Luo J, et al. LSBs-based quantum color images watermarking algorithm in edge region. Quantum Inf Process, 2019, 18: 16

6 Zeng Q W, Wen Z Y, Fu J F, et al. Quantum watermark algorithm based on maximum pixel difference and tent map. Int J Theor Phys, 2021, 60: 3306–3333

7 Zeng Q, Ge H, Fu J, et al. Quantum watermarking algorithm based on quantum Haar wavelet transform and henon map. Int J Theor Phys, 2022, 61: 167

8 Sun W T, Wei Z H, Han M D, et al. An efficient quantum image watermarking protocol based on NEQR model (in Chinese). J North China Univ Technol, 2024, 36: 45 [孙文韬, 魏战红, 韩孟迪, 等. 一种基于NEQR模型的高效的量子图像水印协议. 北方工业大学学报, 2024, 36: 45]

9 Xing Z, Lam C T, Yuan X, et al. MMQW: Multi-modal quantum watermarking scheme. IEEE Trans Inform Forensic Secur, 2024, 19: 5181–5195

10 Zhou N R, Wu J W, Chen M X, et al. A quantum image encryption and watermarking algorithm based on QDCT and baker map. Int J Theor Phys, 2024, 63: 100

11 Qiu Y, Li T, Cui J, et al. Quantum watermarking scheme based on DNA encoding and quantum error correction. J King Saud Univ Comput Inf Sci, 2025, 38: 8

12 Wen Q, Sun T F, Wang S X. Concept and application of zero-watermark (in Chinese). Acta Electron Sin, 2003, 31: 214 [温泉, 孙锬锋, 王树勋. 零水印的概念与应用. 电子学报, 2003, 31: 214]

13 Li X D. Mean gray value based image watermarking algorithm (in Chinese). Geomat Inf Sci Wuhan Univ, 2007, 32: 556 [李旭东. 基于图像灰度平均值的数字水印算法. 武汉大学学报(信息科学版), 2007, 32: 556]

14 Zhang Y, Lu K, Gao Y, et al. NEQR: A novel enhanced quantum representation of digital images. Quantum Inf Process, 2013, 12: 2833–2860

15 Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. Int J Theor Phys, 2016, 55: 107–123

16 Hu W W, Zhou R G, Liu X A, et al. Quantum image steganography algorithm based on modified exploiting modification direction embedding. Quantum Inf Process, 2020, 19: 137

17 Wang M X, Yang H M, Jiang D H, et al. A novel quantum image watermarking scheme for tamper localization and self-recovery. Quantum Inf Process, 2022, 21: 277

18 Wang D, Liu Z H, Zhu W N, et al. Design of quantum comparator based on extended general Toffoli gates with multiple targets (in Chinese). Comput Sci, 2012, 39: 302 [王冬, 刘志昊, 朱皖宁, 等. 基于多目标扩展通用Toffoli门的量子比较器设计. 计算机科学, 2012, 39: 302]

19 Barenco A, Bennett C H, Cleve R, et al. Elementary gates for quantum computation. Phys Rev A, 1995, 52: 3457–3467

20 Nielson M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2000

21 Wang J, Jiang N, Wang L. Quantum image translation. Quantum Inf Process, 2015, 14: 1589–1604

Quantum image robust zero-watermarking algorithm

YE Tian-Yu[1,2*], CAO Jia-Peng[1] & YANG Sheng-Tian[1]

[1] *College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China*
[2] *Chifeng Industry Vocational Technology College, Chifeng 024000, China*
**Corresponding author (email: yetianyu@zjgsu.edu.cn)*

The robustness and imperceptibility of quantum image watermarking algorithms are often mutually restricted. To address this contradiction, this paper proposes a quantum image robust zero-watermarking algorithm based on the novel enhanced quantum representation (NEQR) model of digital images and designs the corresponding quantum circuit. This algorithm generates the robust feature zero-watermark by comparing the size relationship between the average of pixels' gray values in image sub-blocks and the average of all pixels' gray values of the image. The quantum circuit complexity of this algorithm is $O(k^2)$, where k is the height or width of a square image, demonstrating significant advantages over classical computing. Moreover, the algorithm exhibits strong robustness against various types of attacks as a whole.

quantum image watermarking, robust watermark, zero-watermarking, average value, quantum circuit complexity

PACS: 03.67.Lx, 42.30.Va, 42.30.Sy

doi: 10.1360/SSPMA-2026-0101