引用格式：刘恒瑞, 董玉民. 基于 CSS 类稳定子码的彩色与灰度图像水印算法 [J]. 电子科技大学学报, 2026, 55(2): 289-300.
LIU H R, DONG Y M. Color and grayscale image watermarking algorithm based on CSS class stable subcode[J]. Journal of University of Electronic Science and Technology of China, 2026, 55(2): 289-300.

基于 CSS 类稳定子码的彩色与灰度图像水印算法

刘恒瑞，董玉民*

（重庆师范大学计算机与信息科学学院，重庆 401331）

摘要：量子计算理论的研究成果预示着量子计算机有超高并行计算能力的优势，也为图像的安全保护带来了新的方向。回顾现有的研究结果，量子图像水印算法在嵌入量和鲁棒性方面仍然存在不足之处。几类不同的量子系统在运行过程中都不可避免地会受到环境的干扰，导致量子计算过程出错或信息丢失，含水印的载体图像遭遇噪声攻击后又会导致粒子发生量子比特翻转。因此，提出了基于 CSS（calderbank-shor-steane）类稳定子码的彩色与灰度图像水印算法，保证纠错能力的同时降低了量子比特的消耗。将二值水印图像嵌入算法扩展到彩色与灰度图像的嵌入，使算法更具通用性。

关键词：量子计算；量子图像处理；图像水印；量子图像水印；量子纠错码
中图分类号：TP309; O413 **文献标志码：**A DOI: 10.12178/1001-0548.2025081

Color and grayscale image watermarking algorithm based on CSS class stable subcode

LIU Hengrui and DONG Yumin*

(College of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China)

Abstract: Quantum computing, with its ultra-high parallelism, offers new opportunities for image security, yet existing quantum image watermarking algorithms still suffer from limitations in embedding capacity and robustness. Environmental interference in quantum systems and noise attacks on watermarked carrier images can lead to quantum bit errors and information loss, further restricting the practical application of such algorithms. To address these challenges, this paper proposes a color and grayscale image watermarking algorithm based on calderbank-shor-steane (CSS) stabilizer codes, which achieves error correction capability while reducing qubit overhead. By extending binary watermark embedding to color and grayscale images, the algorithm gains improved versatility.

Key words: quantum computing; quantum image processing; image watermark; quantum image watermarking; quantum error-correcting code

当前保护信息安全的手段主要分为信息加密[1-3]和信息隐藏[4-6]。信息加密技术是指利用密钥或者加密函数对秘密信息重新编码，使之看起来像毫无意义的乱码，在信息传播的过程中攻击者无法获取和看懂秘密信息的真实内容。信息隐藏技术的研究方向主要分为隐写术[7-8]和数字水印技术[9-10]。虽然两者都是数据隐藏的形式且有一些共同的基础，但因其应用的目标不同，因此又有一些关键性差异。

2003 年，文献 [11] 首次提出了 Qubit Lattice 模型，但可惜没有使用量子的叠加、纠缠等特性，需要较多的量子比特数来存储图像，实用性不高。2005 年，文献 [12] 提出了 Real Ket 模型，让量子叠加态特性首次出现在大众视野。2010 年，文献 [13] 提出 Entangled Image 模型，该模型使用纠缠态表示图像像素之间的关系，将量子图像带到了新的高度。文献 [14] 在 2015 年提出了 INEQR

收稿日期：2025−04−23
基金项目：国家自然科学基金（61772295）；重庆市自然科学基金创新发展联合基金重点项目（CSTB2023NSCQ-LZX0139）；重庆市教育委员会科学技术重大项目（KJZD-M202000501）
作者简介：刘恒瑞，主要从事量子水印方面的研究。
*通信作者 E-mail: dym@cqnu.edu.cn

（improved NEQR）模型，该模型改变了图像的长宽比例，使得不同比例的图像都能够被处理。2016 年，文献 [15] 在 FRQI 的基础上改进，提出了 FRQCI 模型（fexible representation for quantum color image），此模型使用概率幅度或相位来存储图像像素的 RGB 信息。2017 年，文献 [16] 提出了一种新型的量子水印算法，此算法同时采用了 LSB 和 MSB 的方式。2018 年，文献 [17] 提出了 BRQI 模型（bitplane representation of quantum images）对 NEQR 进行改进，将每个像素的灰度值分成 8 个二进制比特，并将灰度图像分解成 8 个二进制图像。2019 年，文献 [18] 提出了一种新的彩色图像量子表示模型 QRCI（quantum representation model of color digital images），此模型使用量子位序列的基态对图像的颜色信息进行编码。2020 年，文献 [19] 提出了一种傅里叶变换表示模型 FTQR（Fourier transform representation），以一种新的方式存储图像。同年，文献 [20] 提出了一种双量子彩色图像表示模型 DQRCI（double quantum color images representation），此模型可以将两幅彩色数字图像同时存储为一个量子叠加态。2021 年，文献 [21] 设计了一种将量子计算和 LSB 相结合的新型量子水印算法，此算法使用 Python 编程语言和 Qiskit 量子线路模拟框架，能够将子图像嵌入到图像中实现隐写。

近年来，关于量子图像表示的研究得到了快速发展，许多量子图像表示模型被提出。然而，目前研究仍存在一些限制和挑战，因此，未来需要进一步探索和发展量子图像表示技术以解决这些问题。由于编码量子信息的物理系统和环境存在不可避免的相互作用，这种作用会导致编码系统的环境纠缠，使得编码在系统中的信息散失到环境中。不同于经典信息中唯一可能发生的错误是位翻转错，量子信息中除了可能发生位翻转错外，还可能发生相位错。因此，目前已知的量子图像的水印算法在安全性方面仍有较大的改进空间。

本文提出了基于 CSS 稳定子码的图像水印算法，能够快速构造出编码线路和纠错线路。解决了量子计算系统中粒子与环境发生退相干的问题，在保证纠错能力的同时，减少了昂贵的量子比特消耗，而且可以方便按照固定的流程根据稳定子生成元快速构造出编码线路和纠错线路。

1 相关工作

1.1 NEQR 表示模型

用一个实数矩阵来定义经典的$N\times N$图像，其定义如下：

$$\boldsymbol{F}=\begin{bmatrix} f_{00} & f_{01} & \cdots & f_{0(N-1)} \\ f_{01} & f_{11} & \cdots & f_{1(N-1)} \\ \vdots & \vdots & & \vdots \\ f_{0(N-1)} & f_{1(N-1)} & \cdots & f_{(N-1)(N-1)} \end{bmatrix} \tag{1}$$

NEQR 模型将图像像素的灰度值存储于量子位序列的叠加态中，利用张量积使存储位置与灰度值的量子位序列产生量子纠缠，将位置与颜色互相对应，从而存储整幅图像的信息[22-23]。

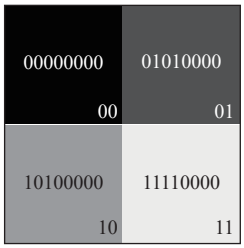
对于一幅大小为$2^n\times 2^n$颜色、范围为$[0,2^m-1]$的图像，将位置(Y,X)处的颜色值$f(Y,X)$用二进制序列$C_{YX}^mC_{YX}^{m-1}\cdots C_{YX}^2C_{YX}^1$来编码，即：

$$f(Y,X)=C_{YX}^mC_{YX}^{m-1}\cdots C_{YX}^2C_{YX}^1$$
$$C_{YX}^k\in[0,1],\ f(Y,X)\in[0,2^m-1] \tag{2}$$

NEQR 定义如下：它的模型分别需要$2n$个量子比特来保存图像坐标信息，m个量子比特来保存灰度值，$|YX\rangle$存储图像的位置信息。

$$|I\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle=$$
$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|C_{YX}^mC_{YX}^{m-1}\cdots C_{YX}^2C_{YX}^1\right\rangle|YX\rangle \tag{3}$$

灰度图像需要 8 个量子比特存储颜色信息，图 1 展示了大小为2×2的灰度图像和其转化为 NEQR 描述模型的示例。



$$|I\rangle=\frac{1}{2}(|0\rangle\otimes|00\rangle+|80\rangle\otimes|01\rangle+|160\rangle\otimes|10\rangle+|240\rangle\otimes|11\rangle)$$
$$=\frac{1}{2}\begin{pmatrix}(|00000000\rangle\otimes|00\rangle+|01010000\rangle\otimes|01\rangle)\\+|10100000\rangle\otimes|10\rangle+|11110000\rangle\otimes|11\rangle)\end{pmatrix}$$

图 1 灰度图像的 NEQR 模型及其变换公式

1.2　不同 NEQR 描述方法

对于大小为$2^n\times 2^n$、颜色范围为$[0,2^m-1]$的图像，其 NEQR 模型需要$(2n+q)$个量子比特来存储，具体为：

$$|I_{YX}\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle=$$
$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|C_{IX}^{q}C_{IX}^{q-1}\cdots C_{YX}^{2}C_{YX}^{1}\right\rangle|YX\rangle \tag{4}$$

二值图像只包含黑色和白色像素，通常用于表示文字、线条、简单的图形等信息，具有图像处理中的简单性和高效性。在 NEQR 描述模型中，只需要用一个量子比特来表示颜色信息。对于$2^n\times 2^n$的二值图像，其 NEQR 表示为：

$$|I_{YX}\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle=$$
$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|C_{IX}^{q}C_{IX}^{q-1}\cdots C_{YX}^{2}C_{YX}^{1}\right\rangle|YX\rangle \tag{5}$$

彩色图像通常由 R、G、B 这 3 个分量构成[24]，它的 NEQR 描述模型可以用 24 个量子比特来存储颜色信息[25-26]。对于$2^n\times 2^n$的彩色图像，其 NEQR 表示为：

$$|I\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|R_{YX}\rangle|G_{YX}\rangle|B_{YX}\rangle|YX\rangle=$$
$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|R_{YX}\rangle|G_{YX}\rangle|B_{YX}\rangle|Y\rangle|X\rangle$$
$$|R_{YX}\rangle=\left|R_{YX}^{8}R_{YX}^{7}\cdots R_{YX}^{2}R_{YX}^{1}\right\rangle,|G_{YX}\rangle=$$
$$\left|G_{YX}^{8}G_{YX}^{7}\cdots G_{YX}^{2}G_{YX}^{1}\right\rangle,|B_{YX}\rangle=\left|B_{YX}^{8}B_{YX}^{7}\cdots B_{YX}^{2}B_{YX}^{1}\right\rangle \tag{6}$$

1.3　构造量子 [7,1,3] 稳定子码

[7,1,3] 码用 6 个稳定子，将 7 个物理比特编码为 1 个逻辑比特。这 6 个稳定子为：

$$K_1=IIIX_4X_5X_6X_7,K_2=X_1IX_3IX_5IX_7$$
$$K_3=IX_2X_3IIX_6X_7,K_4=IIIZ_4Z_5Z_6Z_7$$
$$K_5=Z_1IZ_3IZ_5IZ_7,K_6=IZ_2Z_3IIZ_6Z_7 \tag{7}$$

将2^7维的希尔伯特空间逐渐减小到 2 维子空间，所有合法的逻辑比特态都是这 6 个稳定子的+1本征态。这 6 个稳定子彼此对易，稳定子算符既是幺正算符又是厄米算符，意味着$\forall i,K_i^2=I$，且任意的两个稳定子算符相乘也是 [7,1,3] 码的稳定子（6 个稳定子作为生成元构成一个稳定子群）。

表 1 和表 2 展示了几类基本错误算符和稳定子算符的对易关系，对易与反对易关系与错误诊断有直接联系，比如在第 4 个量子比特发生相位翻转错误Z_4时，对K_1、K_2、K_3的测量结果分别是 −1、+1、+1，这是因为Z_4与K_1反对易，与K_2、K_3对易。

表 1　K_1、K_2、K_3稳定子对易表

稳定子	错误算符						
	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
K_1	对易	对易	对易	反对易	反对易	反对易	反对易
K_2	反对易	对易	反对易	对易	反对易	对易	反对易
K_3	对易	反对易	反对易	对易	对易	反对易	反对易

表 2　K_4、K_5、K_6稳定子对易表

稳定子	错误算符						
	X_1	X_2	X_3	X_4	X_5	X_6	X_7
K_4	对易	对易	对易	反对易	反对易	反对易	反对易
K_5	反对易	对易	反对易	对易	反对易	对易	反对易
K_6	对易	反对易	反对易	对易	对易	反对易	反对易

由于稳定子具有$\forall i,K_i^2=I$的性质，对于水印图像存储像素颜色信息的量子比特$|\psi_P\rangle$，任何形如$(I+K_i)|\psi_P\rangle$的态都是K_i的+1本征态，任何形如$(I-K_i)|\psi_P\rangle$的态都是K_i的−1本征态。所以 [7,1,3] 编码后的逻辑比特$|0_L\rangle$为：

$$|0_L\rangle=\prod_{i=1}^{7}(I+K_i)|0000000\rangle \tag{8}$$

实际上$I+K_4$、$I+K_5$、$I+K_6$本身就是初始态，所以只需要考虑$(I+K_1)(I+K_2)(I+K_3)$：

$$|0_L\rangle=(I+K_1)(I+K_2)(I+K_3)|0000000\rangle=\frac{1}{\sqrt{8}}(|000,0000\rangle+|011,0011\rangle+|101,0101\rangle+|110,0110\rangle+|000,1111\rangle+|011,1100\rangle+|101,1010\rangle+|110,1001\rangle) \tag{9}$$

同理可得：

$$|1_L\rangle=(I+K_1)(I+K_2)(I+K_3)|1111111\rangle=\frac{1}{\sqrt{8}}(|111,1111\rangle+|100,1100\rangle+|010,1010\rangle+|001,1001\rangle+|111,0000\rangle+|100,0011\rangle+|010,0101\rangle+|001,0110\rangle) \tag{10}$$

2 NEQR 模型下的灰度和彩色图像水印的二值化

本节分别设计了量子 NEQR 模型下灰度和彩色图像转化为二值图像的量子线路。将灰度与彩色图像水印的嵌入问题归结为二值图像的嵌入[27]。

2.1 灰度图像水印二值化

将$2^{n-2}\times2^{n-1}$的灰度图像在 NEQR 模型下用$(2n+5)$个量子比特存储。像素的位置信息存储为量子态$|y_{n-1}y_{n-2}\cdots y_1\rangle|x_{n-1}x_{n-2}\cdots x_2\rangle$，花费$(2n-3)$个量子比特。剩下 8 个量子比特$\left|c_{YX}^8c_{YX}^7\cdots c_{YX}^2c_{YX}^1\right\rangle$表示颜色信息。

如表 3 所示，一个灰度图像的像素$\left|c_{YX}^8c_{YX}^7\cdots c_{YX}^2c_{YX}^1\right\rangle$可以转化为 8 个二值像素，对于像素坐标$(Y,X)$，转化后的像素坐标分别为$(2Y,4X)$、$(2Y,4X+1)$、$(2Y,4X+2)$、$(2Y,4X+3)$、$(2Y+1,4X)$、$(2Y+1,4X+1)$、$(2Y+1,4X+2)$、$(2Y+1,4X+3)$，颜色值分别为$\left|c_{YX}^8\right\rangle$、$\left|c_{YX}^7\right\rangle$、$\left|c_{YX}^6\right\rangle$、$\left|c_{YX}^5\right\rangle$、$\left|c_{YX}^4\right\rangle$、$\left|c_{YX}^3\right\rangle$、$\left|c_{YX}^2\right\rangle$、$\left|c_{YX}^1\right\rangle$。

表 3 灰度图像的 1 个像素转化为 8 个二值像素

横坐标	纵坐标			
	$4X$	$4X+1$	$4X+2$	$4X+3$
$2Y$	$\left\|c_{YX}^8\right\rangle$	$\left\|c_{YX}^7\right\rangle$	$\left\|c_{YX}^6\right\rangle$	$\left\|c_{YX}^5\right\rangle$
$2Y+1$	$\left\|c_{YX}^4\right\rangle$	$\left\|c_{YX}^3\right\rangle$	$\left\|c_{YX}^2\right\rangle$	$\left\|c_{YX}^1\right\rangle$

图 2 所示的量子线路图完成了 NEQR 模型下灰度图像的二值化，输入的灰度图像像素坐标存储在$|y_{n-1}y_{n-2}\cdots y_1\rangle|x_{n-1}x_{n-2}\cdots x_2\rangle$上，颜色值存储在$\left|c_{YX}^8c_{YX}^7\cdots c_{YX}^2c_{YX}^1\right\rangle$上。

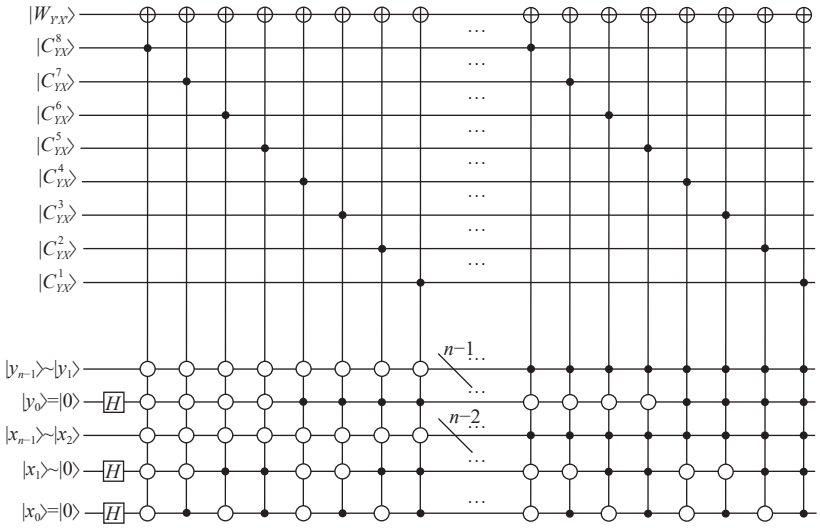


图 2 NEQR 模型下灰度图像向二值图像转化量子线路

制备 3 个初始态为$|0\rangle$的量子比特$|y_0\rangle$、$|x_1\rangle$、$|x_0\rangle$，通过 Hadamard 门制备成均衡叠加态来存储增加的像素坐标信息。制备一个量子比特$|W_{Y'X'}\rangle=|0\rangle$存储二值颜色信息。最后，$2^{n-2}\times2^{n-1}$的灰度图像为：

$$|W\rangle=\frac{1}{\sqrt{2^{2n-3}}}\sum_{Y=0}^{2^{n-1}-1}\sum_{X=0}^{2^{n-2}-1}\left|c_{YX}^8c_{YX}^7\cdots c_{YX}^2c_{YX}^1\right\rangle|YX\rangle \tag{11}$$

式中，$|YX\rangle=|y_{n-1}y_{n-2}\cdots y_1\rangle|x_{n-1}x_{n-2}\cdots x_2\rangle$。转化成了$2^n\times2^n$的二值图像$|W'\rangle$：

$$\left|W'\right\rangle=\frac{1}{2^n}\sum_{Y'=0}^{2^n-1}\sum_{X'=0}^{2^n-1}|W_{Y'X}\rangle\left|Y'X'\right\rangle \tag{12}$$

式中，$|Y'X'\rangle=|y_{n-1}y_{n-2}\cdots y_1y_0\rangle|x_{n-1}x_{n-2}\cdots x_2x_1x_0\rangle$。

如图 3 所示，128×256大小的灰度图像，转化

成了512×512大小的二值图像。

在后续的水印提取操作后，还需要将$2^n\times 2^n$的二值图像还原为$2^{n-2}\times 2^{n-1}$的灰度图像，还原线路与转化线路原理大致相同，只需要将控制非门的控制比特和目标比特对调，最后取$|y_{n-1}y_{n-2}\cdots y_1\rangle|x_{n-1}x_{n-2}\cdots x_2\rangle$表示灰度图像的像素坐标信息，$\left|c_{YX}^8c_{YX}^7\cdots c_{YX}^2c_{YX}^1\right\rangle$表示像素颜色信息，如图 4 所示。



图 3　灰度图像转化二值图像效果

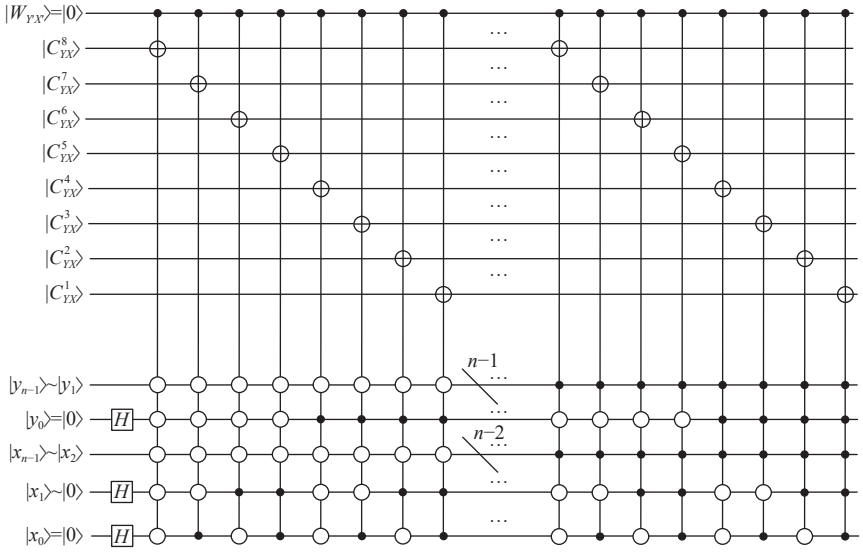


图 4　NEQR 模型下二值图像还原为灰度图像转化量子线路

2.2　彩色图像水印二值化

将$2^{n-3}\times 2^{n-2}$的灰度图像在NEQR模型下用$(2n+19)$个量子比特存储。花费$(2n-5)$个量子比特把像素的位置信息存储为量子态$|y_{n-1}y_{n-2}\cdots y_2\rangle|x_{n-1}x_{n-2}\cdots x_3\rangle$，剩下24个量子比特$\left|r_{YX}^8r_{YX}^7\cdots r_{YX}^2r_{YX}^1\right\rangle\left|g_{YX}^8g_{YX}^9\cdots g_{YX}^2g_{YX}^1\right\rangle\left|b_{YX}^8b_{YX}^7\cdots b_{YX}^2b_{YX}^1\right\rangle$表示颜色信息。将坐标为$(Y,X)$的彩色像素转化为8×4个二值像素，即可将$2^{n-3}\times 2^{n-2}$的彩色图像转换为$2^n\times 2^n$二值图像，如表 4 所示。转化线路如图 5 所示。制备 6 个新的量子比特$|y_1\rangle|y_0\rangle|x_2\rangle|x_1\rangle|x_0\rangle$存储新增的像素坐标，初始态都为$|0\rangle$，并通过 Hadamard 门制备成均衡叠加态。再制备一个量子比特$|W_{Y'X'}\rangle=|0\rangle$存储二值颜色信息。由此可以将彩色图像表示为：

$$|W\rangle=\frac{1}{\sqrt{2^{2n-5}}}\sum_{Y=0}^{2^{n-2}-1}\sum_{X=0}^{2^{n-3}-1}|R_{YX}\rangle|G_{YX}\rangle|B_{YX}\rangle|YX\rangle \quad (13)$$

式中，$|Y\rangle=|y_{n-1}y_{n-2}\cdots y_2\rangle$,$|X\rangle=|x_{n-1}X_{n-2}\cdots x_3\rangle$；

$$\begin{aligned}|R_{YX}\rangle&=\left|r_{YX}^8r_{YX}^7r_{YX}^6r_{YX}^5r_{YX}^4r_{YX}^3r_{YX}^2r_{YX}^1\right\rangle;\\ |G_{YX}\rangle&=\left|g_{YX}^8g_{YX}^7g_{YX}^6g_{YX}^5g_{YX}^4g_{YX}^3g_{YX}^2g_{YX}^1\right\rangle;\\ |B_{YX}\rangle&=\left|b_{YX}^8b_{YX}^7b_{YX}^6b_{YX}^5b_{YX}^4b_{YX}^3b_{YX}^2b_{YX}^1\right\rangle;\end{aligned} \quad (14)$$

转化为二值图像：

$$\left|W'\right\rangle=\frac{1}{2^n}\sum_{Y'=0}^{2^n-1}\sum_{X'=0}^{2^n-1}|W_{Y'}\rangle\left|Y'X'\right\rangle \quad (15)$$

式中，$|Y'\rangle=|y_{n-1}y_{n-2}\cdots y_2y_1y_0\rangle$；$|X'\rangle=|x_{n-1}x_{n-2}\cdots x_3x_2x_1x_0\rangle$。

表 4　灰度图像的一个像素转化为 8 个二值像素

横坐标	纵坐标							
	$8X$	$8X+1$	$8X+2$	$8X+3$	$8X+4$	$8X+5$	$8X+6$	$8X+7$
$4Y$	$\left\|r_{YX}^8\right\rangle$	$\left\|r_{YX}^7\right\rangle$	$\left\|r_{YX}^6\right\rangle$	$\left\|r_{YX}^5\right\rangle$	$\left\|r_{YX}^4\right\rangle$	$\left\|r_{YX}^3\right\rangle$	$\left\|r_{YX}^2\right\rangle$	$\left\|r_{YX}^1\right\rangle$
$4Y+1$	$\left\|g_{YX}^8\right\rangle$	$\left\|g_{YX}^7\right\rangle$	$\left\|g_{YX}^6\right\rangle$	$\left\|g_{YX}^5\right\rangle$	$\left\|g_{YX}^4\right\rangle$	$\left\|g_{YX}^3\right\rangle$	$\left\|g_{YX}^2\right\rangle$	$\left\|g_{YX}^1\right\rangle$
$4Y+2$	$\left\|b_{YX}^8\right\rangle$	$\left\|b_{YX}^7\right\rangle$	$\left\|b_{YX}^6\right\rangle$	$\left\|b_{YX}^5\right\rangle$	$\left\|b_{YX}^4\right\rangle$	$\left\|b_{YX}^3\right\rangle$	$\left\|b_{YX}^2\right\rangle$	$\left\|b_{YX}^1\right\rangle$
$4Y+3$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$

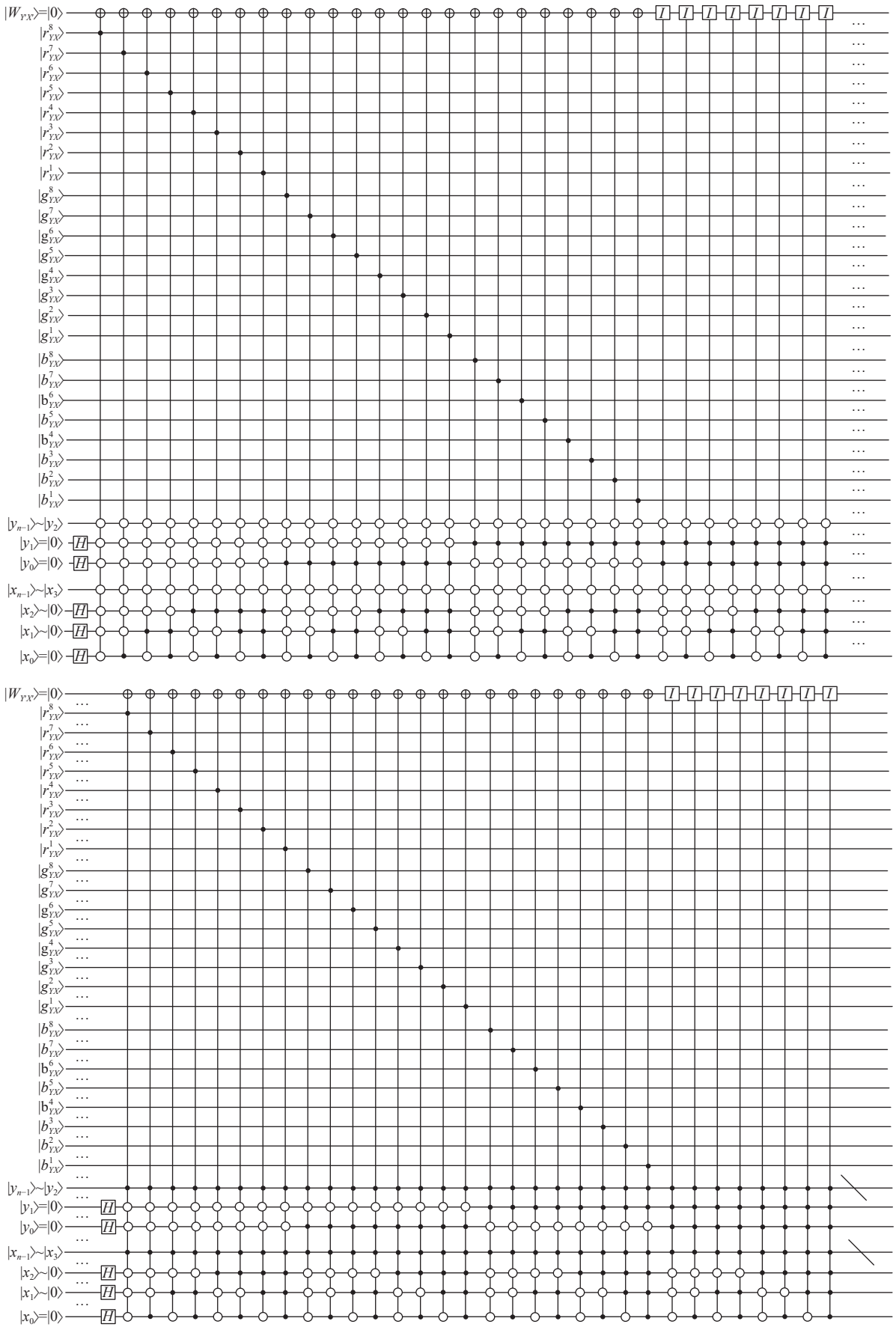


图 5 NEQR 模型彩色图像向二值图像转化量子线路

转化效果如图 6 所示，64×128 大小的彩色图像，转化为 512×512 尺寸的二值图像。



图 6　彩色图像转化二值图像效果

3　图像水印的嵌入与提取

灰度和彩色的图像水印经过上一节的二值化处理，就有了相同大小的彩色载体图像和二值水印图像。接下来讨论它们之间的嵌入和提取算法。

3.1　水印的嵌入

对于二值水印图像存储颜色的量子比特$|W_{XY}\rangle$，首先制备出 6 个量子比特，初始态为$|0\rangle$，得到$|\psi\rangle=|W_{XY}\rangle|000000\rangle$。首先，通过 6 个 CNOT 门（如图 7 所示）得到：

$$|\psi\rangle=|W_{XY}\rangle|000000\rangle=(\alpha|1\rangle+\beta|0\rangle)|000000\rangle \xrightarrow{6\text{ 个 CNOT 门}}=\alpha|000,0000\rangle+\beta|111,1111\rangle \tag{16}$$

通过算符$\prod_{i=1}^{7}(I+K_i)$把$|000,0000\rangle$编码为$|0_L\rangle$，把$|111,1111\rangle$编码为$|1_L\rangle$。由图 8 的量子线路图，最终对辅助比特的测量正好使得量子态有概率坍缩到想要的形式，具体过程为：

$$\begin{aligned}&|0\rangle|\psi\rangle \xrightarrow{\text{Hadamard}} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\psi\rangle\\ &\xrightarrow{\text{controlled }-U} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle+|1\rangle U|\psi\rangle)\\ &\xrightarrow{\text{hadamard}} \frac{1}{2}[(|0\rangle+|1\rangle)|\psi\rangle+(|0\rangle-|1\rangle)U|\psi\rangle]=\\ &\frac{1}{2}|0\rangle(|\psi\rangle+U|\psi\rangle)+\frac{1}{2}|1\rangle(|\psi\rangle-U|\psi\rangle)\\ &\xrightarrow{\text{measure anc qbit}}(I+U)|\psi\rangle\text{ or}(I-U)|\psi\rangle\end{aligned} \tag{17}$$

随后，只需要把上述线路重复 3 次就能实现$\prod_{t=1}^{7}(I+K_i)$。基于以上的讨论，水印的嵌入线路如图 9 所示。

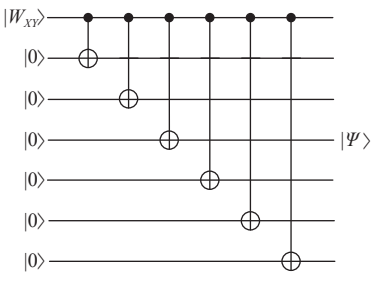


图 7　水印图像编码线路步骤一

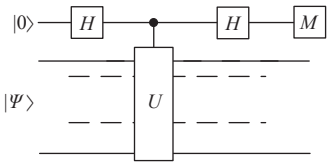


图 8　$(I+U)|\psi\rangle$的算符编码线路

对于 3 个辅助量子比特最后一步的测量是一个概率性的操作，编码块不一定会坍缩到想要的结果，有可能坍缩到$(I-U)|\psi\rangle$。对于测量出来的结果M_1、M_2和M_3，编码线路的实际算符为：

$$\left[I+(-1)^{M_3}K_3\right]\left[I+(-1)^{M_2}K_2\right]\left[I+(-1)^{M_1}K_1\right] \tag{18}$$

如果测量结果分别为 0、0、1，那线路的效果等价于：

$$(I-K_3)(I+K_2)(I+K_1) \tag{19}$$

这显然不是想要的效果，所以还需对结果进行修正。此处需要一个与K_3反对易，与K_2、K_1对易的力学量，查询表 1，选择Z_2：

$$\begin{aligned}&Z_2(I-K_3)(I+K_2)(I+K_1)=\\ &(I+K_3)(I+K_2)(I+K_1)Z_2\end{aligned} \tag{20}$$

总结对易关系表的规律，若测量结果为M_1、M_2和M_3，那么修正操作应为：

$$Z_i, i=1^{M_2}+2^{M_3}+4^{M_1} \tag{21}$$

为了抵消Z_i给$|111,1111\rangle$带来的-1 系数，再用一个$Z_L=Z_1Z_2Z_3Z_4Z_5Z_6Z_7$来修正。完整的过程为：

$$\begin{aligned}&Z_LZ_i\left[I+(-1)^{M_3}K_3\right]\left[I+(-1)^{M_2}K_2\right]\left[I+(-1)^{M_1}K_1\right](\alpha|000,0000\rangle+\beta|111,1111\rangle)=\\ &Z_L(I+K_3)(I+K_2)(I+K_1)Z_i(\alpha|000,0000\rangle+\beta|111,1111\rangle)=Z_L(I+K_3)(I+K_2)(I+K_1)(\alpha|000,0000\rangle-\beta|111,1111\rangle)=\\ &Z_L(\alpha|0_L\rangle-\beta|1_L\rangle)=\alpha|0_L\rangle+\beta|1_L\rangle\end{aligned} \tag{22}$$

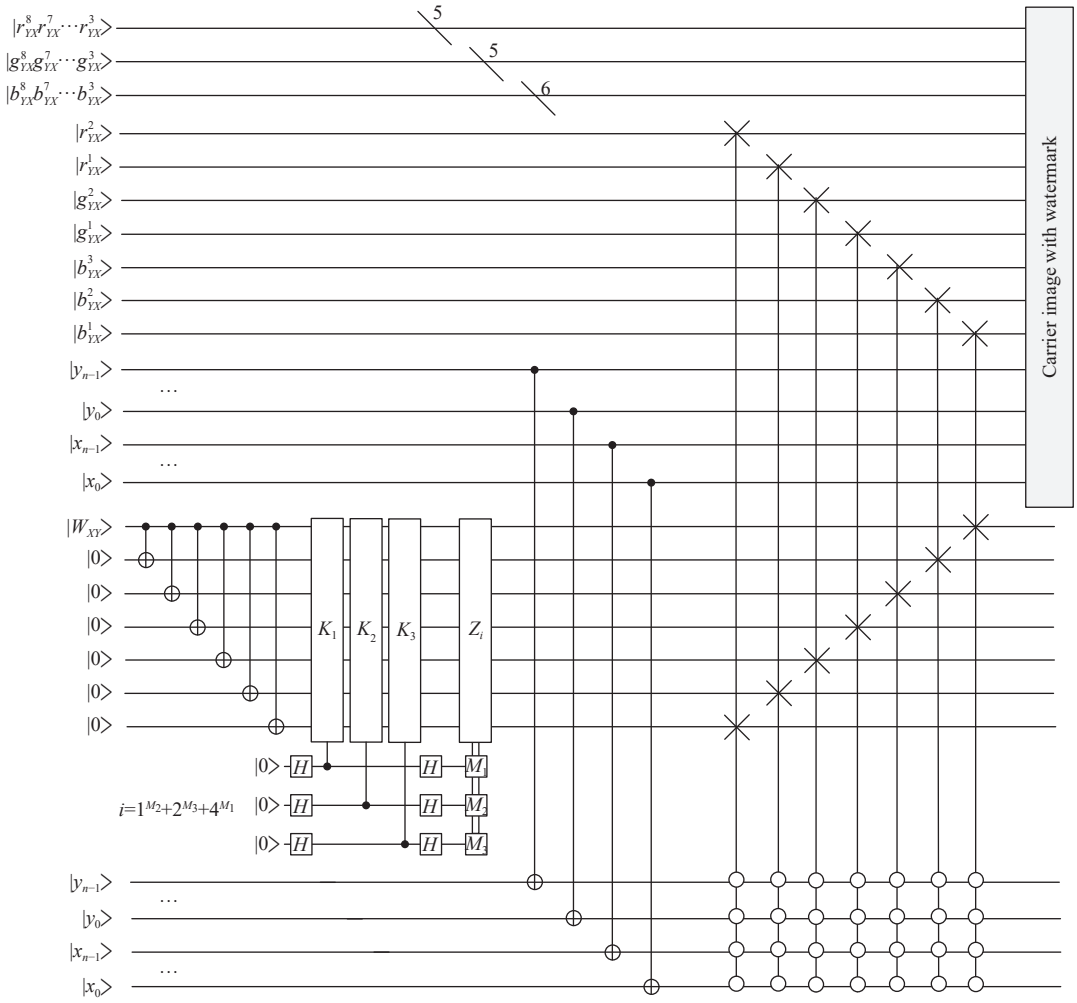


图 9 稳定子码编码后的水印嵌入线路

最后，取彩色载体图像像素坐标信息为控制位，用 $2n$ 个 CNOT 门把载体图像的像素位置映射到二值水印图像上，将编码后的 7 个量子比特，依次分别替换到 ***R*** 通道的前两位最低有效位，*G* 通道的前两位最低有效位和 *B* 通道的前 3 位最低有效位中。如图 10 所示，人眼在 *B* 通道中的低频敏感度显著低于 ***R*** 通道与 *G* 通道，所以插入更多的水印图像信息对含水印的载体图像隐蔽性影响最小。

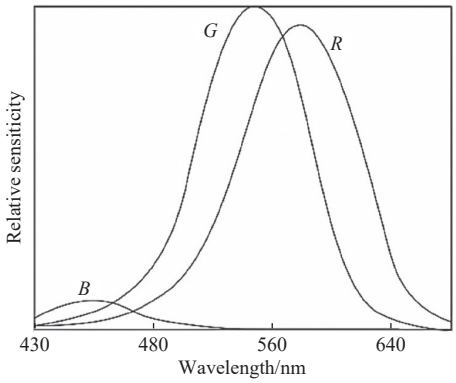


图 10 人眼彩色视觉中的颜色系统

3.2 错误诊断和纠错

稳定子码的纠错线路与编码线路基本相似，本质都是测量稳定子的过程。依旧使用图 11 和图 12 的基本结构，但是初始态变成了合法的态 $|\psi_L\rangle$。

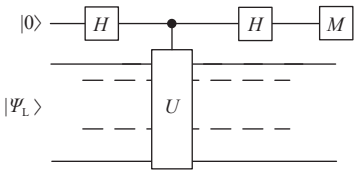


图 11 稳定子码纠错线路的基本结构

线路中测量 K_1 稳定子的一份基本结构的量子态变化为：

$$|0\rangle|\psi_L\rangle \xrightarrow{\text{hadamard}} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\psi_L\rangle \xrightarrow{\text{controlled}-K_1}$$
$$\frac{1}{\sqrt{2}}(|0\rangle|\psi_L\rangle+|1\rangle K_1|\psi_L\rangle) \xrightarrow{\text{hadamard}}$$
$$\frac{1}{2}[(|0\rangle+|1\rangle)|\psi_L\rangle+(|0\rangle-|1\rangle)K_1|\psi_L\rangle]=$$
$$\frac{1}{2}|0\rangle(I+K_1)|\psi_L\rangle+\frac{1}{2}|1\rangle(I-K_1)|\psi_L\rangle \tag{23}$$

若没有发生错误，$|\psi_L\rangle$仍是K_1的+1 本征态，则$(I-K_1)|\psi_L\rangle$自动消失，测量值M_1必为 0。若有与K_1反对易的错误发生，如Z_4、Z_5、Z_4是K_1的−1 本征态，则M_1测量结果必定为 1。以此类推，6 次测量，可以诊断出某一个物理比特的比特翻转或相位翻转，并予以纠正。

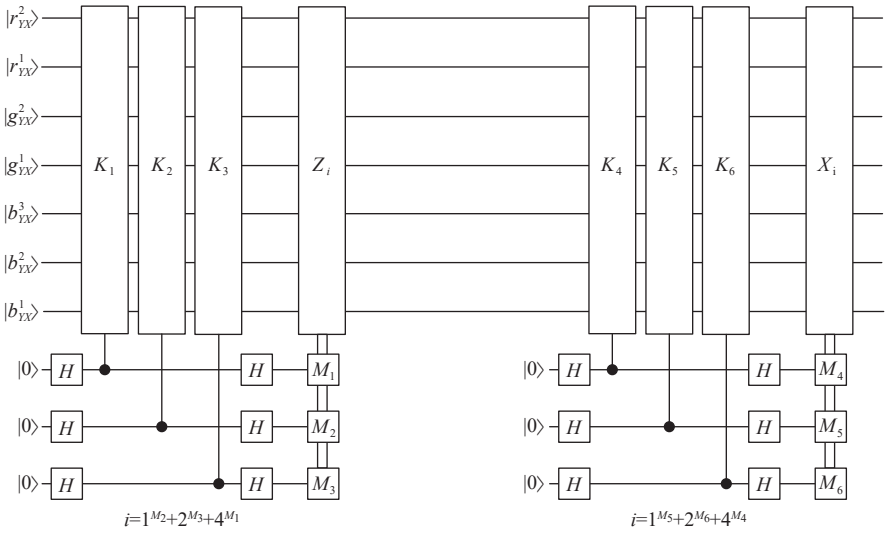


图 12　稳定子码完整纠错线路

3.3　水印的提取

图 13 的量子线路图展示了一个简单的量子计数器，对A，B，C这 3 个量子比特进行计数，当量子态为|1⟩的量子比特数量大于等于 2 时，$|w\rangle$置为|1⟩，否则为|0⟩。

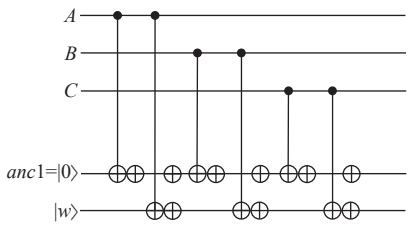


图 13　量子计数器线路

水印提取的量子线路如图 14 所示。

经过提取线路，含水印载体图像$|E\rangle$为：

$$|E\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|r^8_{YX}r^7_{YX}\cdots r^2_{YX}r^1_{YX}\right\rangle \left|g^8_{YX}g^7_{IX}\cdots g^2_{YX}g^1_{IX}\right\rangle\left|b^8_{IX}b^7_{YX}\cdots b^2_{YX}b^1_{YX}\right\rangle|YX\rangle \tag{24}$$

提取出水印$|W\rangle$：

$$|W\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|w_{XY}\rangle|YX\rangle,$$

$$|w_{XY}\rangle=\begin{cases}|1\rangle, & r^1_{YX}+r^2_{YX}+g^1_{YX}+g^2_{YX}+b^1_{YX}+b^2_{YX}+b^3_{YX}\geqslant 4\\ |0\rangle, & r^1_{YX}+r^2_{YX}+g^1_{YX}+g^2_{YX}+b^1_{YX}+b^2_{YX}+b^3_{YX}<4\end{cases} \tag{25}$$

4　实验仿真及结果分析

现阶段尚未研发出真正的通用量子计算机，由于经典计算机的运行是基于普通的存储单位，算法的量子并行性优势和对编码块中量子物理比特的相位翻转纠错能力难以体现。但可以通过经典计算机完成图像的嵌入结果仿真，验证本文水印算法的隐蔽性。

本次实验采用与上一节相同的彩色载体图像与二值水印图像，大小均为512×512，如图 15 所示。

嵌入后含水印的载体图像如图 16 所示。

峰值信噪比（PSNR）[28] 是一种衡量数字图像或视频质量的指标。它通过比较原始图像与压缩或失真后的图像之间的信噪比来计算，单位为 dB。

PSNR通过均方误差MSE进行定义。为定量描述彩色图像的可视化质量，对于$m\times n$大小的图像I和嵌入水印后的图像S，均方误差定义为：

$$\mathrm{MSE}=\sum_{x=1}^{m}\sum_{i=1}^{n}\sum_{k=1}^{3}[I(x,y,k)-S(x,y,k)]^2 \tag{26}$$

峰值信噪比定义为：

$$\mathrm{PSNR}=10\log_{10}\left(\frac{3mn\times 255^2}{\mathrm{MSE}}\right)=10\lg\left(\frac{3mn\times 255^2}{\mathrm{MSE}}\right) \tag{27}$$

误比特率BER[29] 定义为峰值信噪比PSNR的倒数：

$$\mathrm{BER}=\frac{1}{\mathrm{PSNR}} \tag{28}$$

结构相似性SSIM[30]常用于图像处理、计算机视觉等领域，考虑了人眼对图像结构和纹理的感知，符合人类视觉系统的特性。SSIM通过比较不同图像的亮度、对比度和结构信息 3 个方面来计算相似度，定义为：

$$\mathrm{SSIM}(x,y)=\frac{\left(2\mu_x\mu_y+C_1\right)\left(2\sigma_{xy}+C_2\right)}{\left(\mu_x^2+\mu_y^2+C_1\right)\left(\sigma_x^2+\sigma_y^2+C_2\right)} \tag{29}$$

式中，μ_x和μ_y表示两个图像的亮度均值；σ_x^2和σ_y^2表示亮度方差；σ_{xy}表示协方差；C_1和C_2^C是两个常数，用于避免分母为零的情况。 SSIM 的值越接近于 1，表示两个图像之间的结构相似性越高。

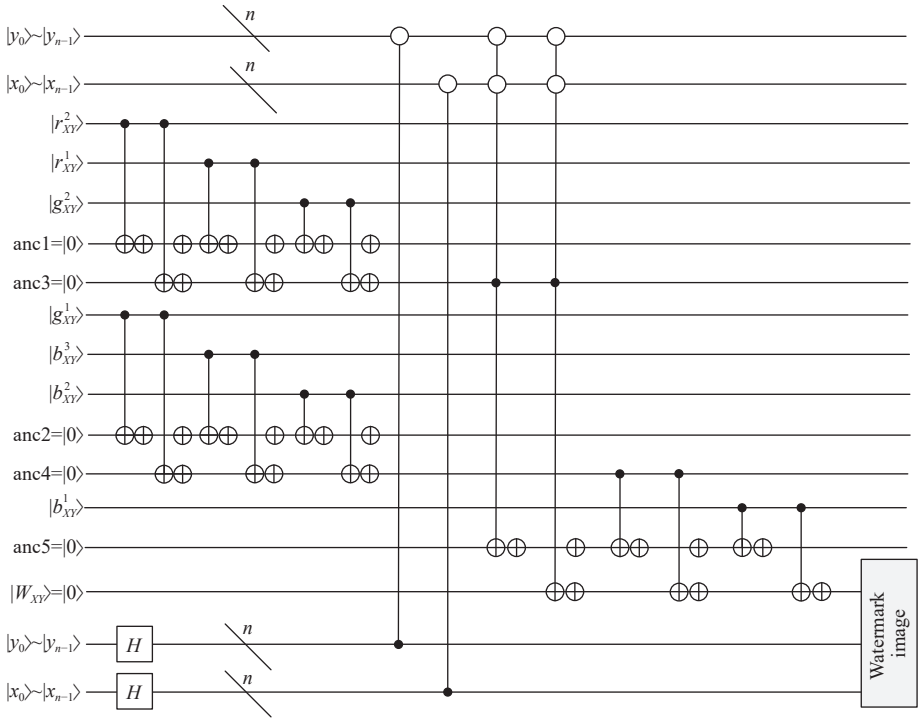


图 14　水印的提取线路



图 15　原始图像与水印图像

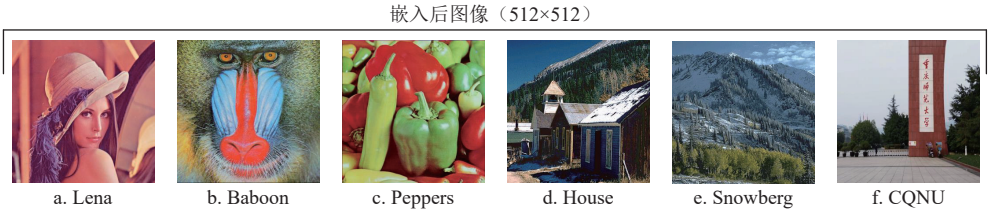


图 16　含水印的载体图像

表 5 和图 17 是每张图像的原始版本与嵌入二值水印后的 PSNR 、 SSIM 、BER值，其中 PSNR 在常见情况下，值越大表示图像质量越高，一般在30 dB以上被认为是高质量图像， SSIM 越接近 1 代表图像有很高的相似性，通常情况下在 0.9 以上被认为是高质量图像。

表 5　PSNR、SSIM 和 BER 的实验结果

参数	Lena	Baboon	Peppers	House	Snowberg	CQNU
PSNR	40.458 4	40.646 3	40.774 5	40.413 7	40.765 5	40.586 5
SSIM	0.916 2	0.904 0	0.913 6	0.907 0	0.906 1	0.904 1
BER	0.024 71	0.024 60	0.024 52	0.024 74	0.024 53	0.024 63

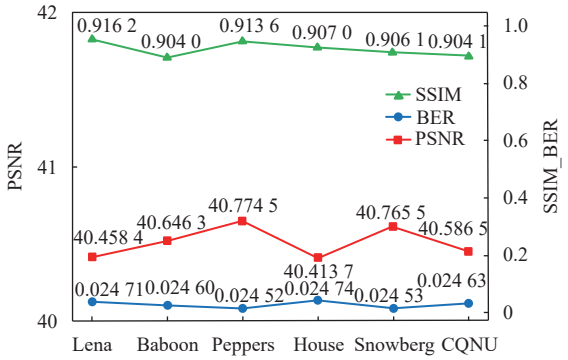


图 17　PSNR、SSIM 和 BER 的折线图

5　结束语

本文探讨了基于 CSS 类量子稳定子码的彩色和灰度图像水印算法的设计、实现和性能分析。扩展了水印技术的适用范围，实现了对彩色和灰度图像的水印嵌入和提取，并消耗了更少的量子比特对相位翻转和比特翻转错误进行诊断和纠正。最后，分别对算法中彩色图像和灰度图像的水印嵌入做了隐蔽性仿真实验，具有较好的通用性和实用性。

参 考 文 献

[1] STINSON D R, PATERSON M B. Cryptography: Theory and practice[M]. 4th ed. Boca Raton: CRC Press, 2018.

[2] SCHNEIER B. Applied cryptography[M]. [S.l.]: Wiley, 2015.

[3] 章照止. 现代密码学基础[M]. 北京: 北京邮电大学出版社, 2004.
ZHANG Z Z. Fundamentals of modern cryptography[M]. Beijing: Beijing University of Posts and Telecommunications Press, 2004.

[4] KATZENBEISSER S, PETITOLAS F. Information hiding techniques for steganography and digital watermarking[J]. EDPACS the EDP Audit, Control and Security Newsletter, 1999, 28(6): 1-2.

[5] 汪小帆. 信息隐藏技术: 方法与应用[M]. 北京: 机械工业出版社, 2001.
WANG X F. Information hiding technology: Method and application[M]. Beijing: China Machine Press, 2001.

[6] 王丽娜, 张焕国, 叶登攀. 信息隐藏技术与应用[M]. 2 版. 武汉: 武汉大学出版社, 2009.
WANG L N, ZHANG H G, YE D P. Information hiding technology and its application[M]. 2nd ed. Wuhan: Wuhan University Press, 2009.

[7] PARNAS D L. On the criteria to be used in decomposing systems into modules[J]. Communications of the ACM, 1972, 15(12): 1053-1058.

[8] JOHNSON N F, JAJODIA S. Exploring steganography: Seeing the unseen[J]. Computer, 31(2): 26-34.

[9] 孙圣和, 陆哲明. 数字水印处理技术[J]. 电子学报, 2000, 28 (8): 85-90.
SUN S H, LU Z M. Digital watermark processing technology [J]. Electronic Journal, 2000, 28 (8): 85-90.

[10] 王炳锡, 陈琦, 邓峰森. 数字水印技术[M]. 西安: 西安电子科技大学出版，2003.
WANG B X, CHEN Q, DENG F S. Digital watermarking technology[M]. Xi'an: Xi'an University of Electronic Science and Technology Press, 2003.

[11] VENEGAS-ANDRACA S E, BOSE S. Storing, processing, and retrieving an image using quantum mechanics[C]//Proceedings of the Quantum Information and Computation. [S.l.]: SPIE, 2003: 137-147.

[12] LATORRE J I. Image compression and entanglement [EB/OL]. [2025-01-12]. https://arxiv.org/pdf/quant-ph/0510031.

[13] VENEGAS-ANDRACA S E, BALL J L. Processing images in entangled quantum systems[J]. Quantum Information Processing, 2010, 9(1): 1-11.

[14] JIANG N, WANG L. Quantum image scaling using nearest neighbor interpolation[J]. Quantum Information Processing, 2015, 14(5): 1559-1571.

[15] LI P, XIAO H, LI B. Quantum representation and watermark strategy for color images based on the controlled rotation of qubits[J]. Quantum Information Processing, 2016, 15(11): 4415-4440.

[16] NASERI M, HEIDARI S, BAGHFALAKI M, et al. A new secure quantum watermarking scheme[J]. Optik, 2017, 139: 77-86.

[17] LI H S, CHEN X, XIA H Y, et al. A quantum image representation based on bitplanes[J]. IEEE Access, 2018, 6: 62396-62404.

[18] WANG L, RAN Q W, MA J, et al. QRCI: A new quantum representation model of color digital images[J]. Optics

Communications, 2019, 438: 147-158.
[19] GRIGORYAN A M, AGAIAN S S. New look on quantum representation of images: Fourier transform representation[J]. Quantum Information Processing, 2020, 19(5): 148.
[20] WANG L, RAN Q W, MA J. Double quantum color images encryption scheme based on DQRCI[J]. Multimedia Tools and Applications, 2020, 79(9): 6661-6687.
[21] TUDORACHE A G, MANTA V, CARAIMAN S. Quantum steganography using two hidden thresholds[J]. Advances in Electrical and Computer Engineering, 2021, 21(4): 79-88.
[22] ABDOLMALEKY M, NASERI M, BATLE J, et al. Red-green-blue multi-channel quantum representation of digital images[J]. Optik, 2017, 128: 121-132.
[23] SANG J Z, WANG S, LI Q. A novel quantum representation of color digital images[J]. Quantum Information Processing, 2016, 16(2): 42.
[24] TIRKEL A Z, RANKIN G A, VAN S R M, et al. Electronic watermark[J]. Digital Image Computing, Technology and Applications, 1993: 666-673.
[25] JIANG N, WU W Y, WANG L. The quantum realization of Arnold and Fibonacci image scrambling[J]. Quantum Information Processing, 2014, 13(5): 1223-1236.
[26] WU L L, ZHANG J W, DENG W T, et al. Arnold transformation algorithm and anti-Arnold transformation algorithm[C]//Proceedings of the 1st International Conference on Information Science and Engineering. [S.l.]: IEEE, 2009: 1164-1167.
[27] HUYNH-THU Q, GHANBARI M. Scope of validity of PSNR in image/video quality assessment[J]. Electronics Letters, 2008, 44(13): 800.
[28] POLLET T, VAN B M, MOENECLAEY M. BER sensitivity of OFDM systems to carrier frequency offset and Wiener phase noise[J]. IEEE Transactions on Communications, 43(2/3/4): 191-193.
[29] HORE A, ZIOU D. Image quality metrics: PSNR vs. SSIM[C]//Proceedings of the 20th International Conference on Pattern Recognition. [S.l.]: IEEE, 2010: 2366-2369.
[30] CHAN R H, CHUNG W A, NIKOLOVA M. Salt-and-pepper noise removal by Median-type noise detectors and detail-preserving regularization[J]. IEEE Transactions on Image Processing, 14(10): 1479-1485.

责任编辑 税 红