文章编号: 1671-5896(2022)02-0219-12

基于格雷码映射和 LSB 的彩色图像量子隐写算法

肖 红, 陈欣燕
(东北石油大学 计算机与信息技术学院, 黑龙江 大庆 163318)

摘要: 针对现有基于 LSB(Least Significant Bit)的量子图像隐写方案嵌入容量较低的问题, 提出了一种基于格雷码规则的彩色图像量子隐写方案。首先将秘密信息置乱, 然后将其划分为 6 比特段, 最后使用格雷码规则将前 3 位嵌入载体图像 RGB(Red Green Blue)通道的第 2 LSB 中, 其余 3 位嵌入到载体图像 RGB 通道的 LSB 中。按照嵌入规则, 隐写图像的 LSB 与嵌入秘密比特的差异高达近 50%, 提高了嵌入信息的安全性; 提取是嵌入的逆过程。设计了相关操作的量子线路, 在经典计算机上的仿真结果表明, 该方案的嵌入容量高达每像素6 bit, 不仅在嵌入容量方面优于现有方案, 同时也有较高的安全性, 这表明采用格雷码规则实施量子隐写的研究方案是可行的。

关键词: 量子图像处理; 量子图像隐写; 格雷码; 最低有效位; 嵌入容量
中图分类号: TP391 **文献标识码:** A
DOI:10.19292/j.cnki.jdxxp.20220411.006

Quantum Steganography Based on Reflected Gray Code and LSB for Color Images

XIAO Hong, CHEN Xinyan
(School of Computer and Information Technology, Northeast Petroleum University, Daqing 163318, China)

Abstract: In order to solve the problem of low embedding capacity of the existing quantum image stegography schemes based on LSB(Least Significant Bit), a novel color image quantum stegography scheme based on reflected Gray code rule is proposed. The secret information is scrambled first, and then it is divided into 6-bit segments. Finally, the first 3 bits are embedded in the second LSB of the RGB channel of the cover image, and the remaining 3 bits are embedded in the LSB of the RGB channel of the cover image using reflected-Gray code rules. According to the embedding rules, the difference between the embedded secret bit and the LSB of the stego-image is almost as high as 50%, which further guarantees the security of embedded information. Extracting is the inverse process of embedding. A quantum circuit for related operations is designed. The simulation results on the classical computer show that the embedding capacity of this scheme is as high as 6 bits per pixel, which is superior to the existing scheme in terms of embedding capacity, and has higher security. Therefore, it is feasible to implement the research scheme of quantum steganography by using Gray code rule.

Key words: quantum information processing; quantum image steganography; gray code; least-significant-bit; embedding capacity

0 引 言

1982 年 Feynman[1] 首次提出量子计算概念, 其作为一种新的计算方法以其高度的并行性受到越来越多国内外学者的关注。量子图像处理(QIP: Quantum Image Processing)是一个新兴的子学科[2], 它专注于

收稿日期: 2021-06-29
基金项目: 黑龙江省自然科学基金资助项目(JJ2019LH0212)
作者简介: 肖红(1979—), 女, 黑龙江大庆人, 东北石油大学副教授, 博士, 主要从事量子信息处理研究, (Tel) 86-13904861067 (E-mail) xh_daqing@126.com。

将传统的图像处理任务和操作扩展到量子计算框架中。量子图像处理领域的研究始于对量子图像的表示。2003 年，Venegas-Andraca 等[3] 提出了 Qubit Lattice 模型；2005 年，Latorre[4] 提出了 Real Ket 模型；随后，Le 等[5-6] 提出了 FRQI(Flexible Representation of Quantum Images) 模型。这 3 个模型堪称量子图像表示先驱[7]，之后提出的各种模型都是对这 3 个模型的修改或扩展。关于量子图像表示详细的发展脉络可参见文献[7]。

隐写是实现图像信息隐蔽传输的一种重要技术[8]。Qu 等[9] 对关于量子图像隐写进行了相关研究。在灰度载体图像方面，2015 年，Jiang 等[10] 首次提出了基于 Moire Pattern 的水印算法。Wang 等[11] 提出了基于 LSB(Least Significant Bit) 的信息隐藏算法。2016 年，Jiang 等[12] 提出了两种盲 LSB 隐写算法，一种使用消息位直接代替像素的 LSB；另一种将消息位嵌入到一个图像块的多个像素中。2017 年，Naseri 等[13] 提出了一种同时采用 LSB 和 MSB(Most Significant Bit) 的量子隐写算法，该算法实际上只有一半秘密信息嵌入到载体图像中，其余一半被当作密钥。Zhou 等[14] 提出了一种基于 Arnold 置乱和 LSB 的新隐写算法。在彩色载体图像方面，2016 年，Sang 等[15] 研究了经典图像 LSB 信息隐藏算法在量子计算机上的可行性。2017 年，Heidari 等[16] 研究了 3 种基于 LSB 的量子彩色图像隐写算法。Heidari 等[17] 提出了一种新的基于量子 LSB 的彩色图像格雷码隐写方法，但在该方法中格雷码的优势并未得到充分利用。Heidari 等[18] 提出了一种新的基于 RGB 图像中所有者签名的盲量子版权保护法，该方法利用其中一个 RGB 通道作为指示符，并利用两个剩余通道嵌入关于所有者的信息。

针对量子彩色图像的隐写，笔者提出的算法在嵌入容量[8] 方面做了较大的改进。该算法将秘密信息划分为多个 6 比特段，每个 6 比特段根据其自身的值和格雷码映射规则嵌入到载体图像 RGB 通道的第 2LSB 和 LSB 中。最后采用不同的秘密图像和载体图像作为仿真对象，与其他方法进行对比，结果表明该方案在嵌入容量和安全性两方面均有较大优势。

1 预备知识

1.1 彩色图像的量子表示

笔者基于 QRMW(Quantum Representation of Multi Wavelength Images)[19] 提出了一种新的彩色图像量子表示方法，该模型使用 3 组纠缠量子位序列，分别对每个像素的颜色、通道和位置信息进行编码。第 1 量子位序列用于编码像素的颜色值，需要 8 个量子比特；第 2 量子位序列用于编码 RGB 通道，需要2 个量子比特，这两个量子比特处于 3 个基态 $|00\rangle$、$|01\rangle$、$|10\rangle$(分别表示 R、G、B 3 通道) 的均衡叠加态中，具体量子线路如图 1 所示；第 3 量子位序列用于编码像素位置。

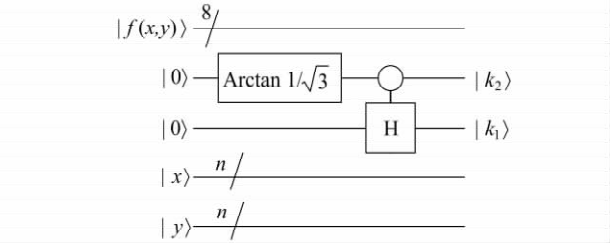


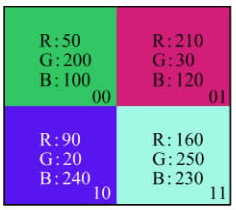
图 1 2 个量子比特产生 3 个均衡叠加态的量子线路

Fig. 1 Two qubits produce a quantum circuit with three equilibrium superposition states

因此，对一幅 $2^n \times 2^n$ 且 RGB 3 通道颜色值范围均为{0,1,…,255} 的彩色图像，仅需要 $2n+10$ 个量子比特。可描述为

$$|CI\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|f(y,x)\rangle|yx\rangle \rightarrow \frac{1}{2^n\sqrt{3}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left(\begin{array}{l}\bigotimes_{k=0}^{7}|r_{yx}^k\rangle|00\rangle + \\ \bigotimes_{k=0}^{7}|g_{yx}^k\rangle|01\rangle + \\ \bigotimes_{k=0}^{7}|b_{yx}^k\rangle|10\rangle\end{array}\right)|yx\rangle \tag{1}$$

一幅彩色图像及其对应的量子描述如图 2 所示。



$$|I\rangle=\frac{1}{2\sqrt{3}}\begin{pmatrix}(|50\rangle|00\rangle+|200\rangle|01\rangle+|100\rangle|10\rangle)|00\rangle+\\(|210\rangle|00\rangle+|30\rangle|01\rangle+|120\rangle|10\rangle)|01\rangle+\\(|90\rangle|00\rangle+|20\rangle|01\rangle+|240\rangle|10\rangle)|10\rangle+\\(|160\rangle|00\rangle+|250\rangle|01\rangle+|230\rangle|10\rangle)|11\rangle\end{pmatrix}$$

$$=\frac{1}{2\sqrt{3}}\begin{pmatrix}(|00110010\rangle|00\rangle+|11001000\rangle|01\rangle+|01100100\rangle|10\rangle)|00\rangle+\\(|11010010\rangle|00\rangle+|00011110\rangle|01\rangle+|01111000\rangle|10\rangle)|01\rangle+\\(|01011010\rangle|00\rangle+|00010100\rangle|01\rangle+|11110000\rangle|10\rangle)|10\rangle+\\(|10100000\rangle|00\rangle+|11111010\rangle|01\rangle+|11100110\rangle|10\rangle)|11\rangle\end{pmatrix}$$

图 2　一个 2 ×2 的彩色图像及其模型的表示方式

Fig. 2　A representation of a 2 ×2 size color image and its model

1.2　量子 Hilbert 置乱

1891 年，Hilbert 发明了二维空间中的一种遍历曲线，命名为 Hilbert 曲线[20]，并由 Hilbert 矩阵描述。沿着 Hilbert 曲线，图像可以被置乱，而且置乱效果更好。对一个 $2^n \times 2^n$ 的初始矩阵，从上到下、从左到右用 $1 \sim 2^{2n}$（表示从 $1 \sim 2^{2n}$ 的正整数，如 $1,2,3,\cdots,2^{2n}$）对其中的元素进行编号，得到

$$\boldsymbol{S}_n = \begin{bmatrix} 1 & 2 & \cdots & 2^n \\ 2^n+1 & 2^n+2 & \cdots & 2^{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ 2^{2n-1}+1 & 2^{2n-1}+2 & \cdots & 2^{2n} \end{bmatrix} \tag{2}$$

则 Hilbert 矩阵 $\boldsymbol{H}_n$ 是初始矩阵 $\boldsymbol{S}_n$ 的一个排列

$$\boldsymbol{H}_0 = [1],\quad \boldsymbol{H}_1 = \begin{bmatrix} 1 & 2 \\ 4 & 3 \end{bmatrix},\quad \boldsymbol{H}_2 = \begin{bmatrix} 1 & 2 & 15 & 16 \\ 4 & 3 & 14 & 13 \\ 5 & 8 & 9 & 12 \\ 6 & 7 & 10 & 11 \end{bmatrix}$$

在 $\boldsymbol{H}_n$ 中，可通过顺序连接元素 $1 \sim 2^{2n}$ 获得 Hilbert 曲线。

1.3　格雷码及其在 LSB 隐写中的应用

格雷码因 1953 年公开的弗兰克·格雷（Frank Gray）专利“Pulse Code Communication”而得名[21]，广泛应用于各种工程领域[22]。在格雷码中，任何两个相邻的代码只有一个不同的二进制数。此外，由于最大码和最小码之间只相差一位数字，即“首尾相连”，所以其也被称为循环码或反射码[23]。

二进制码 $b_n, b_{n-1}, \cdots, b_1$ 与其格雷码 $g_n, g_{n-1}, \cdots, g_1$ 之间的相互转换如下所示[23]

$$g_k = \begin{cases} b_k, & k = n, \\ b_{k+1} \oplus b_k, & 1 \leqslant k \leqslant n-1, \end{cases} \tag{3}$$

$$b_k = \begin{cases} g_k, & k = n, \\ b_{k+1} \oplus g_k, & 1 \leqslant k \leqslant n-1, \end{cases} \tag{4}$$

以 4 位格雷码为例（其他情况类似），实现二进制码和格雷码转换的量子线路如图 3 所示。2008 年，Chen 等[23]研究了格雷码在 LSB 图像隐写中的应用，该方法采用灰度图像作为载体，按照格雷码规则嵌入秘密信息。在嵌入过程中，函数 Gray(g) 对应为格雷码 g 的十进制数，其中 g 为像素值的后 4 位。如果嵌入消息位为 0，则修改载体像素的 LSB，使其后 4 位像素值为最接近其 Gray(g) 的偶格雷码；否则，修改载体像素的 LSB，使其后 4 位像素值为最接近其 Gray(g) 的奇格雷码。以 4 位格雷码为例，如果载体图像的像素值为 $197_{10} = 11000101_2$，取最后 4 位 $\text{Gray}(0101_2) = 6_{\text{Gray}}$。如果消息位为 1，则与该 Gray($g$) 的最近奇数为 $5_{\text{Gray}} = 0111_2$ 或 $7_{\text{Gray}} = 0100_2$。鉴于 0111_2 可能会给图像带来更大的失真，选择 0100_2 作为最好的解决方案，并通过修改 LSB，隐写图像像素值 $197_{10} = 11000101_2$ 被重写为 $196_{10} = 11000100_2$。如果消息位为 0，由于 $\text{Gray}(0101_2) = 6_{\text{Gray}}$ 就是一个偶数，所以无需更改像素值。

提取过程相对简单。当隐写图像像素的后 4 位像素值 Gray(g) 为奇数时，嵌入消息位为 1；当为偶数时，嵌入消息位为 0。例如，如果隐写图像像素的值是 $212_{10} = 11010100_2$，则从 $\text{Gray}(0100_2) = 7_{\text{Gray}}$ 可以得出嵌入消息位为 1。

a 将1个数的格雷码转换为相应的二进制码的量子线路　　b 将1个数的二进制码转换为相应的格雷码的量子线路

图3　实现二进制码和格雷码互相转换的量子线路

Fig. 3　The quantum circuits that implements the conversion between binary code and Gray code

尽管该方案中嵌入的秘密比特与隐写图像的 LSB 之间约有 50% 的差异，提高了嵌入信息的安全性，然而它的嵌入容量仅为 1 bit/pixel，且单纯依赖于秘密比特与 LSB 的差异不能保证嵌入信息的安全性。鉴于此，笔者将从进一步提升嵌入容量和嵌入信息的安全性两方面考虑，提出一种新的量子彩色图像隐写方案。

2　基于格雷码的彩色图像量子隐写算法

在该方法中，使用大小为 $2^n \times 2^n$ 的 RGB 图像 $|CI\rangle$ 作为载体图像和大小为 $2^u \times 2^v$ 的灰度图像 $|SI\rangle$ 作为秘密图像，根据文献[24]，秘密图像的 GQIR(Generalized Quantum Image Representation) 可表示为

$$|SI\rangle = \frac{1}{\sqrt{2^{u+v}}}\sum_{y=0}^{2^u-1}\sum_{x=0}^{2^v-1}|f(y,x)\rangle|yx\rangle = \frac{1}{\sqrt{2^{u+v}}}\sum_{y=0}^{2^u-1}\sum_{x=0}^{2^v-1}\bigotimes_{k=0}^{7}|s_{yx}^k\rangle|yx\rangle = \frac{1}{\sqrt{2^{u+v}}}\sum_{y=0}^{2^u-1}\sum_{x=0}^{2^v-1}|s_{yx}^7 s_{yx}^6,\cdots,s_{yx}^0\rangle|yx\rangle \tag{5}$$

其中 $f(y,x) = s_{yx}^7 s_{yx}^6,\cdots,s_{yx}^0, s_{yx}^k \in \{0,1\}$ 且 $f(y,x) \in \{0,1,\cdots,2^8-1\}$。

笔者提出的隐写方案包括分割、嵌入、提取和恢复 4 个过程，如图 4 所示。

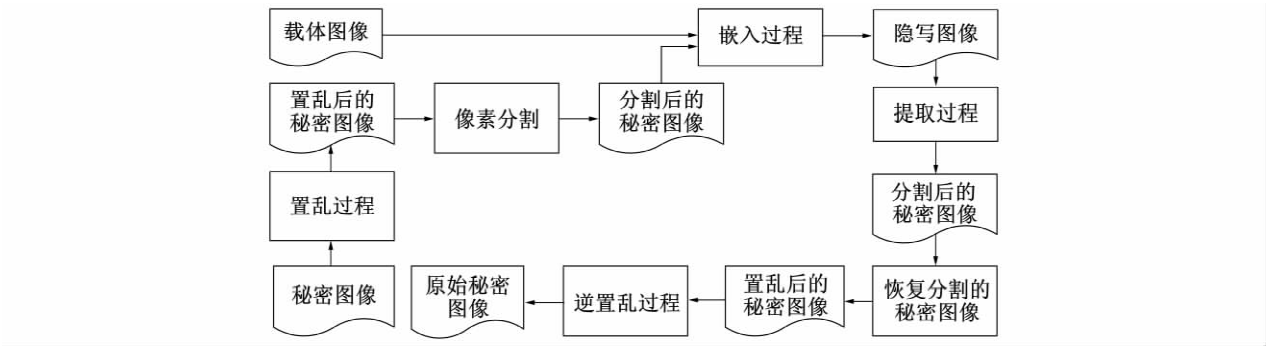


图4　本文中的隐写算法的流程图

Fig. 4　The outline of the steganographic scheme

2.1　秘密图像的置乱

秘密图像嵌入到载体图像中时首先要将秘密图像进行量子 Hilbert 置乱。置乱是使含隐藏信息的载体图像的最低位平面看上去类似噪声，以增强算法的不可检测性。如果不进行置乱操作，在不使用格雷码规则的前提下，含隐藏信息的载体图像的最低位平面就是消息图像，攻击者可以很容易找到这个信息[25]。而在使用格雷码嵌入规则的基础上，置乱为含隐藏信息的载体图像又增加了一定安全性，这就不容易引起攻击者的注意。

2.2　秘密图像的嵌入

2.2.1　秘密图像的像素分割

首先将置乱后 $|SI\rangle$ 中的量子比特视为 6 比特段，然后每个 6 比特段嵌入到载体像素的 RGB 通道中，其中 RGB 通道的 LSB 和第 2 LSB 分别容纳 3 bit。如果最后一段小于 6 bit，则用“0”填充。因此，为将 $|SI\rangle$ 嵌入到大小为 $2^n \times 2^n$ 的 $|CI\rangle$ 中，首先需要将 $|SI\rangle$ 转换成大小为 $2^{u+v+1-n} \times 2^n$、灰度范围为 2^6 的图

像，其中 $u+v+1\leqslant 2n$。以 $n=2$，$u=2$，$v=1$ 为例，实现秘密图像分割的量子线路如图 5 所示[26]。

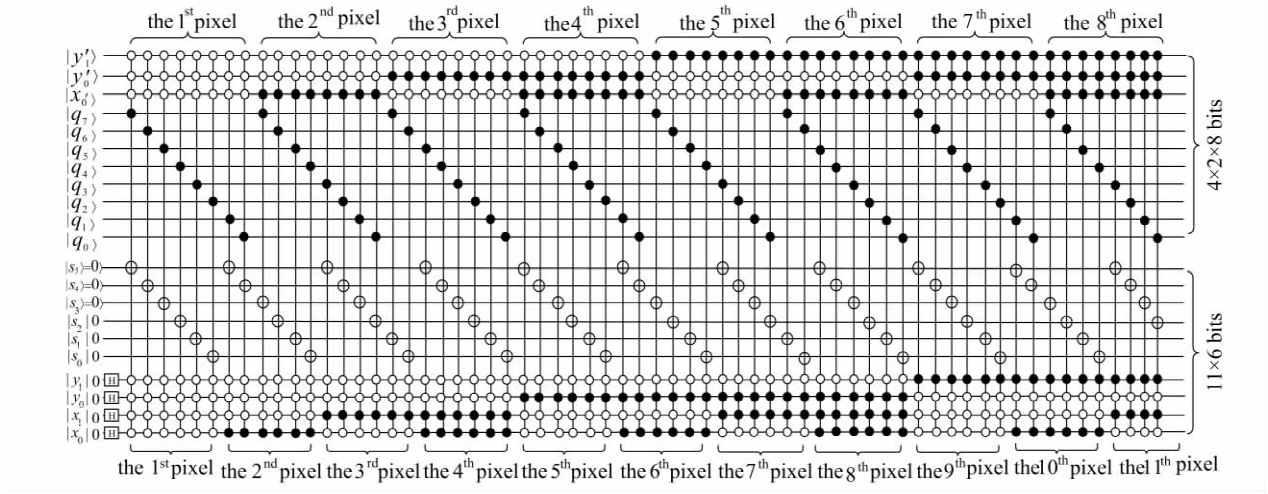


图 5　实现秘密图像转换的量子线路

Fig. 5　The quantum circuits of implementing the secret image conversion

图 5 中上半部分为原始秘密图像(灰度范围为 2^8)，下半部分为分割后的秘密图像(灰度范围为 2^6)。H 表示矩阵形式为 $\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ 的 Hadamard 门[27]，其作用是使位置量子比特处于平衡叠加态。

从秘密图像的分割过程中可以看出，分段后的秘密图像与载体图像的列数相同，行数小于等于载体图像的行数。以式(5)描述的秘密图像为例，分割后的秘密图像为

$$|S\rangle=\frac{1}{\sqrt{2^{u+v+1}}}\sum_{y=0}^{2^{u+v+1-n}-1}\sum_{x=0}^{2^n-1}|s_{yx}^5 s_{yx}^4 s_{yx}^3 s_{yx}^2 s_{yx}^1 s_{yx}^0\rangle\,|yx\rangle \tag{6}$$

经过像素比特分段后的秘密图像通常含有一些冗余像素，笔者将冗余像素灰度值设为 $|0\rangle$。

2.2.2　秘密图像的嵌入过程

秘密图像嵌入的基本思想可概括为：使用格雷码规则将秘密比特 s_{ij}^5，s_{ij}^4，s_{ij}^3 分别嵌入载体比特 r_{ij}^1，g_{ij}^1，b_{ij}^1 中，而 s_{ij}^2，s_{ij}^1，s_{ij}^0 分别嵌入到载体比特 r_{ij}^0，g_{ij}^0，b_{ij}^0 中。图 6 给出了具体的嵌入方案。其中 R3Last0、G3Last0、B3Last0 分别表示载体图像的 R、G、B 通道的后 4 比特。

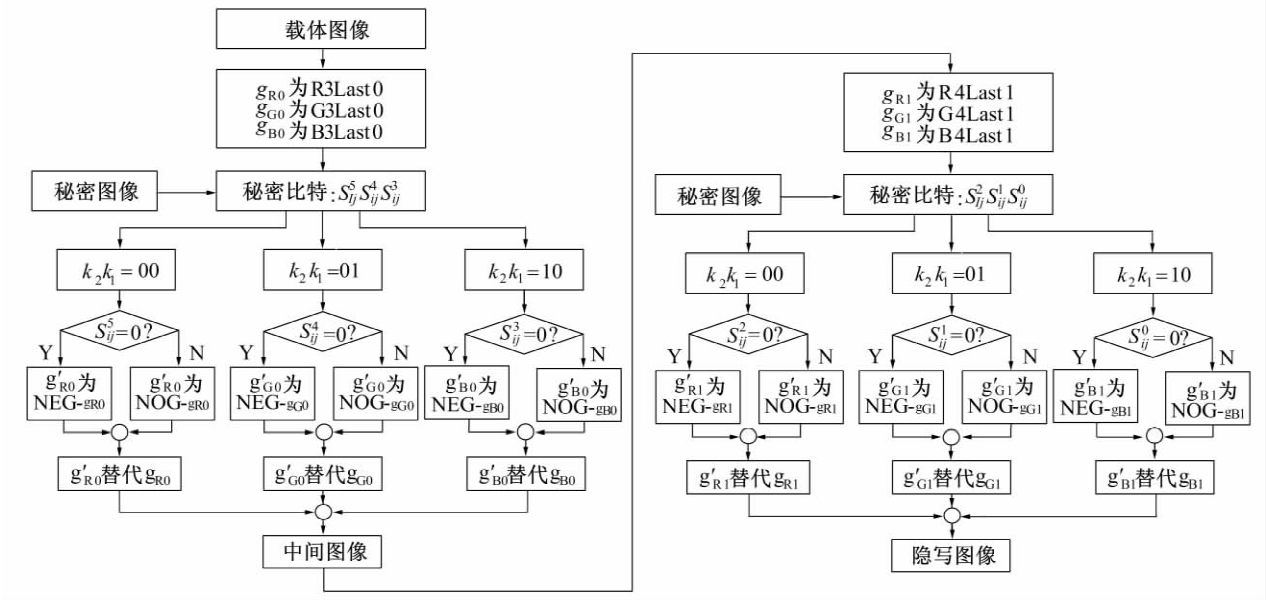


图 6　关于嵌入方案的概述

Fig. 6　The outline of the embedding scheme

NEG-g_{R0}、NOG-g_{R0}分别表示与载体像素 R 通道后 4 比特的格雷码最接近的偶格雷码和奇格雷码；NEG-g_{G0}、NOG-g_{G0}分别表示与载体像素 G 通道后 4 比特的格雷码最接近的偶格雷码和奇格雷码；NEG-g_{B0}、NOG-g_{B0}分别表示与载体像素 B 通道后 4 比特的格雷码最接近的偶格雷码和奇格雷码。R4Last1、G4Last1、B4Last1 分别表示载体图像的 R、G、B 通道的倒数第 5 位到第 2 位比特；NEG-g_{R1}、NOG-g_{R1}分别表示与载体像素 R 通道该 4 bit 的格雷码最接近的偶格雷码和奇格雷码；NEG-g_{G1}、NOG-g_{G1}分别表示与载体像素 G 通道该 4 bit 的格雷码最接近的偶格雷码和奇格雷码；NEG-g_{B1}、NOG-g_{B1}分别表示与载体像素 B 通道该 4 比特的格雷码最接近的偶格雷码和奇格雷码。c_{ij}^0,c_{ij}^1,c_{ij}^2,c_{ij}^3,c_{ij}^4为基于格雷码规则嵌入所需的5 个 bit，其余 3 个 bit 在嵌入过程中并没有使用，因此在此处不表示。实现上述方案的量子线路如图 7 所示。

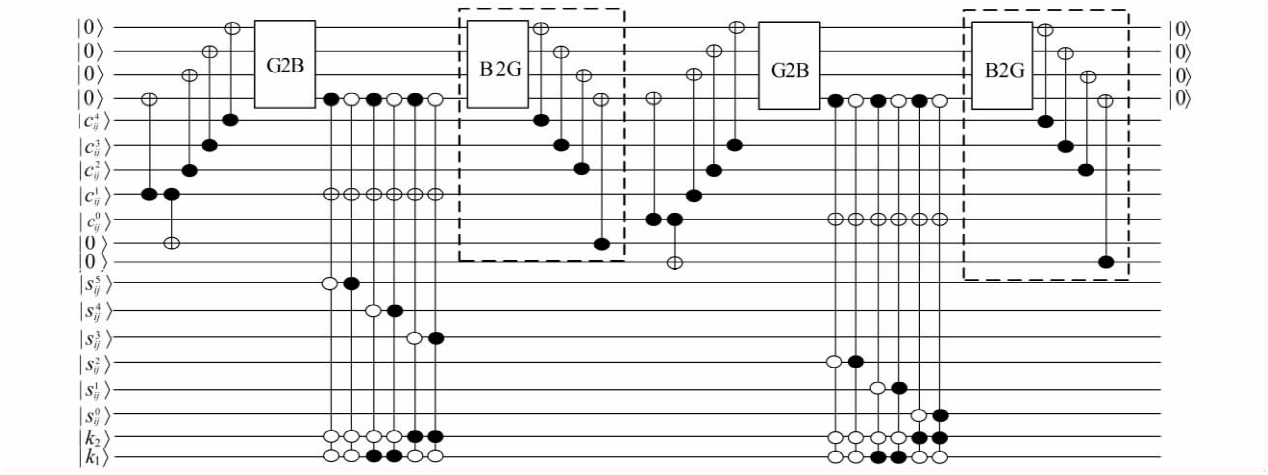


图 7 在载体图像中嵌入单个秘密像素的量子线路

Fig. 7 Quantum circuits for embedding a single secret pixel into cover image

2.3 秘密图像的提取过程

图 8 给出了具体的提取方案。以秘密图像中(i,j) 位置的像素为例，设其灰度值为 $|s_{ij}^5 s_{ij}^4 s_{ij}^3 s_{ij}^2 s_{ij}^1 s_{ij}^0\rangle$，下面给出从隐写图像中提取的详细描述。

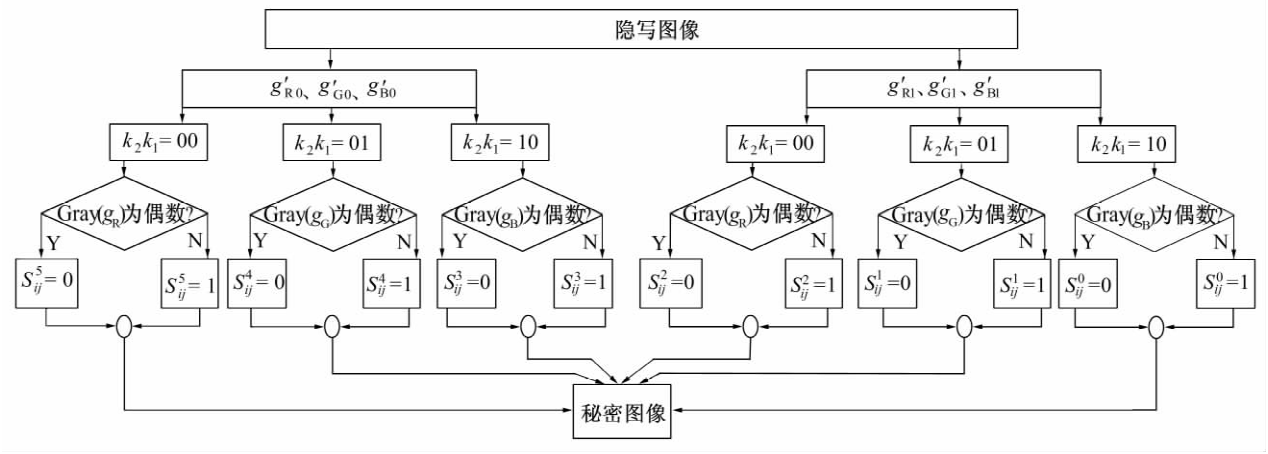


图 8 关于提取方案的概述

Fig. 8 The outline of the extracting scheme

在隐写图像中，设 $g_R = r_{ij}^4 r_{ij}^3 r_{ij}^2 r_{ij}^1$，$g_G = g_{ij}^4 g_{ij}^3 g_{ij}^2 \hat{g}_{ij}^1$，$g_B = b_{ij}^4 b_{ij}^3 b_{ij}^2 \hat{b}_{ij}^1$，$g_R' = r_{ij}^3 r_{ij}^2 \hat{r}_{ij}^1 \hat{r}_{ij}^0$，$g_G' = g_{ij}^3 g_{ij}^2 \hat{g}_{ij}^1 \hat{g}_{ij}^0$，$g_B' = b_{ij}^3 b_{ij}^2 \hat{b}_{ij}^1 \hat{b}_{ij}^0$。从嵌入过程中可以看到，格雷码 g_R,g_G,g_B 与 s_{ij}^5,s_{ij}^4,s_{ij}^3的奇偶性是一致的，g_R',g_G',g_B' 与 s_{ij}^2,s_{ij}^1,s_{ij}^0的奇偶性是一致的。因此根据格雷码 g_R,g_G,g_B,g_R',g_G',g_B' 的奇偶性可以直接得到 s_{ij}^5,s_{ij}^4,s_{ij}^3,s_{ij}^2,s_{ij}^1,s_{ij}^0。实现上述过程的量子线路如图 9 所示。

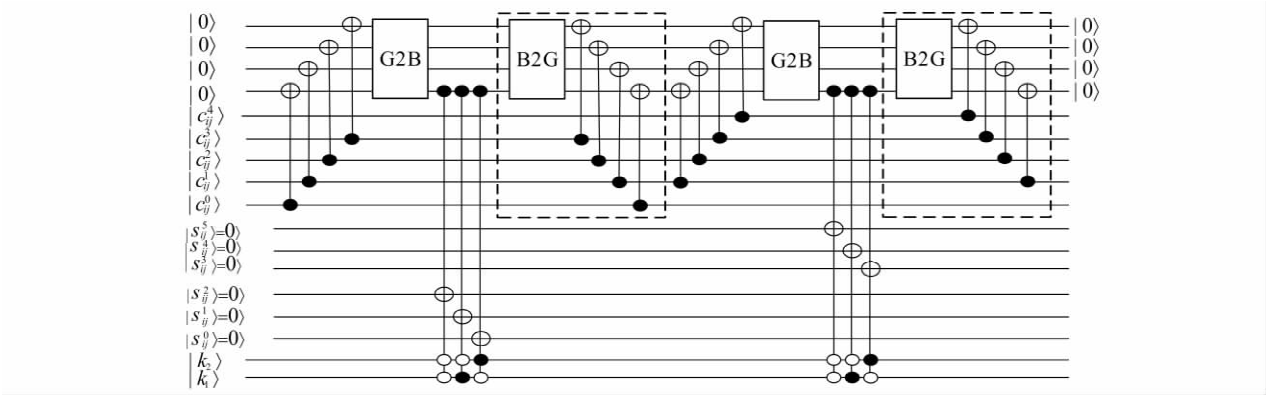


图 9　在载体图像中提取单个秘密像素的量子线路

Fig. 9　Quantum circuits for extracting a single secret pixel from stego-image

值得指出的是，直接从隐写图像中提取的秘密图像是一个大小为 $2^{u+v+1-n}\times 2^{n}$、灰度范围为 2^{6} 的图像，需要进一步恢复成大小为 $2^{u}\times 2^{v}$、灰度范围为 2^{8} 的图像。以 $n=2$，$u=2$，$v=1$ 为例，实现这个过程的量子线路如图 10 所示。这个量子线路类似于图 6 中的量子线路。最后再经过量子 Hilbert 逆置乱恢复成原始秘密图像。

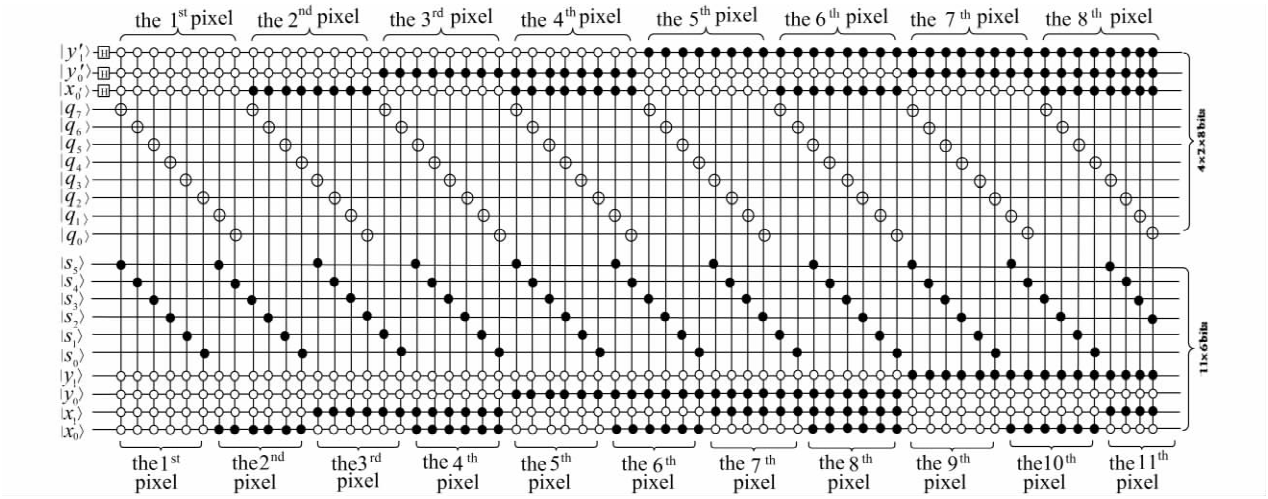


图 10　实现秘密图像恢复的量子线路

Fig. 10　Quantum circuits for secret image restoration

3　经典计算机上的仿真结果及分析

为验证笔者隐写方案的优势，将其与参考文献[15-17]中的隐写方案在嵌入量相同和嵌入量不同两种情况下进行比较。具体对比项包括：隐写图像的峰值信噪比和安全性评价。模拟中使用的 6 张 512 × 512 像素大小的彩色图像作为载体图像，如图 11 所示。

图 11　实验中使用的 6 幅载体图像

Fig. 11　Six cover images used in the experiments

对512×512像素大小的载体图像，由于文献[16]和文献[17]的嵌入容量是2 bit/pixel，即最多可嵌入512×512×2=256×256×8个秘密比特，因此嵌入的秘密图像最大为256×256像素。同样，文献[15]的隐写方案嵌入容量为3 bit/pixel，即最多可嵌入512×512×3=384×256×8个秘密比特，因此嵌入的秘密图像最大为384×256像素。笔者所提出的隐写方案嵌入容量为6 bit/pixel，即最多可嵌入512×512×6=768×256×8个秘密比特，因此嵌入的秘密图像最大为768×256。模拟中使用3张256×256像素、3张384×256像素和3张768×256像素大小的灰度图像作为秘密图像，如图12~图14所示。

图12 文献[16-17]中使用的3幅秘密图像

Fig. 12 Three secret images used in reference [16-17]

图13 文献[15]中使用的3幅秘密图像

Fig. 13 Three secret images used in reference [15]

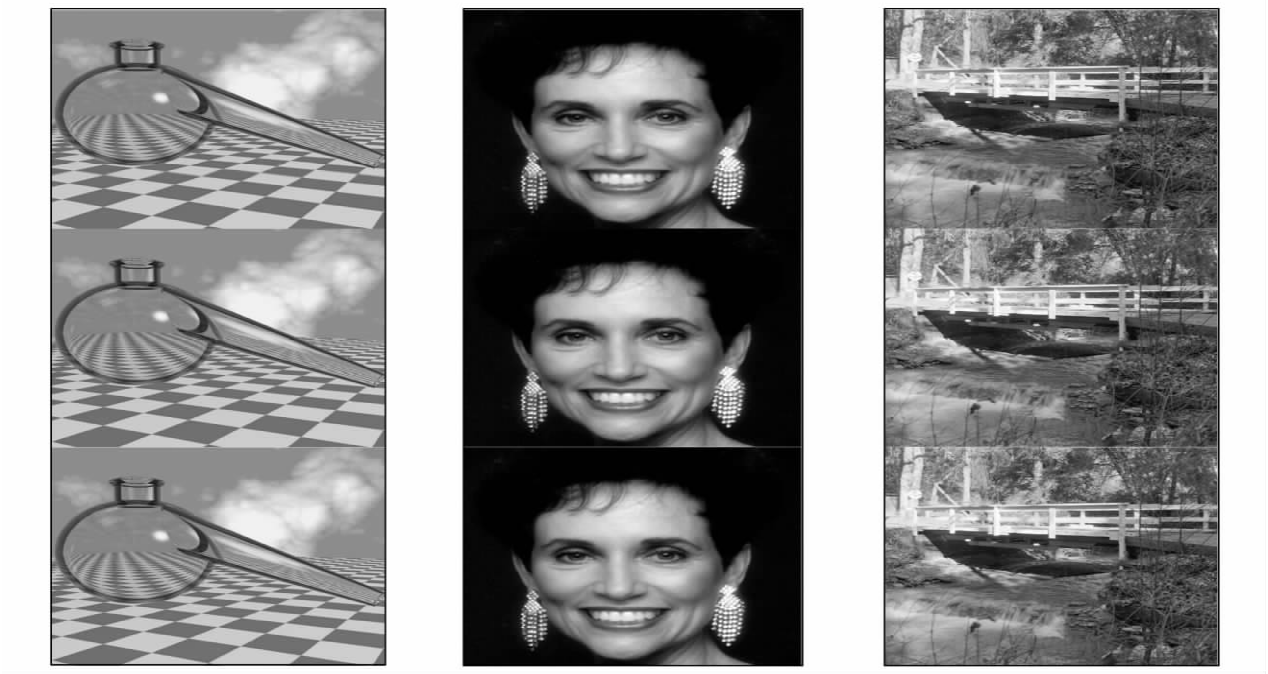


图14 笔者方案使用的3幅秘密图像

Fig. 14 Three secret images are used in the proposed scheme

3.1　4 种隐写方案的 PSNR 比较

不可见性是隐写性能的基本要求，通常使用峰值信噪比(PSNR：Peak Signal-to-Noise Ratio)衡量[28]。设 C 为大小为 $2^n \times 2^n$ 像素的彩色载体图像，S 为嵌入秘密信息后的隐写图像，PSNR 可以定义为

$$P = 20\log_{10}\left(\frac{255\sqrt{3\times 2^{2n}}}{\sqrt{\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}\sum_{k=0}^{3}[C(i,j,k)-S(i,j,k)]^2}}\right) \tag{7}$$

笔者方案和其他 3 种方案 PSNR 对比如表 1 所示。

表 1　4 种隐写方案在不同秘密/载体图像下的 PSNR 对比

Tab. 1　The PSNR of the four steganographic schemes for the various combinations of coverimages and secret images　(dB)

方案	秘密图像	载体图像					
		图 12a	图 12b	图 12c	图 12d	图 12e	图 12f
文献[16]	图 13a	52.888 0	52.897 5	52.893 5	52.901 7	52.893 5	52.901 7
	图 13b	52.891 3	52.891 7	52.913 3	52.899 8	52.913 3	52.899 8
	图 13c	52.903 6	52.895 1	52.914 8	52.900 6	52.898 3	52.893 7
文献[17]	图 13a	50.092 9	50.067 2	50.040 9	50.078 6	50.040 9	50.078 6
	图 13b	50.936 4	50.804 9	50.851 1	50.878 2	50.851 1	50.878 2
	图 13c	50.166 7	50.122 9	50.125 7	50.166 7	50.114 4	50.169 8
文献[15]	图 13a	52.896 8	52.908 1	52.902 9	52.908 9	52.902 9	52.908 9
	图 13b	52.912 4	52.890 8	52.914 5	52.916 8	52.914 5	52.916 8
	图 13c	52.908 4	52.905 4	52.898 4	52.903 2	52.903 2	52.895 9
	图 14a	51.144 1	51.133 4	51.140 0	51.148 9	51.140 0	51.148 9
	图 14b	51.152 3	51.128 6	51.148 4	51.144 9	51.148 4	51.144 9
	图 14c	51.143 6	51.136 8	51.141 0	51.148 0	51.138 2	51.136 2
笔者	图 13a	48.900 1	48.896 4	48.916 4	48.898 0	48.901 4	48.934 6
	图 13b	48.912 2	48.879 4	48.924 5	48.881 6	48.899 0	48.942 6
	图 13c	48.911 2	48.911 7	48.911 3	48.908 9	48.904 9	48.928 6
	图 15a	44.138 0	44.137 4	44.141 5	44.132 4	44.145 3	44.157 2
	图 15b	44.134 9	44.148 5	44.145 1	44.145 0	44.142 4	44.163 6
	图 15c	44.144 7	44.139 5	44.141 9	44.137 6	44.146 7	44.158 4

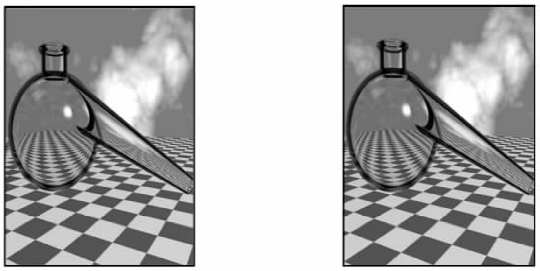
从表 1 可以看出，当嵌入相同大小的秘密图像后，与其他方案相比，笔者方案的 PSNR 仅降低了 2 ~ 4 dB。当达到最大嵌入容量时，与文献[16]和文献[17]的方案相比，虽然 PSNR 降低了 6 ~ 8 dB，但嵌入容量增加了两倍；与文献[15]中的方案相比，虽然 PSNR 降低了约 7 dB，但嵌入容量增加了 1 倍。此外，本方案在达到最大嵌入容量后，PSNR 值还是大于 44 dB，这在一般情况下是可以接受的。

将图 12a 中的秘密图像嵌入到所述载体图像中，笔者方案的视觉效果如图 15 所示。从图 15 可以看出，原始的载体图像和对应的隐写图像仅用肉眼是无法区分的，从而验证了笔者方案的安全性。

原始的秘密图像和从载体图像中提取的秘密图像用肉眼看也是没有任何差异的，从而保证了笔者方案的正确性。

a 原始载体图像

b 嵌入图12a中的秘密图像后的隐写图像



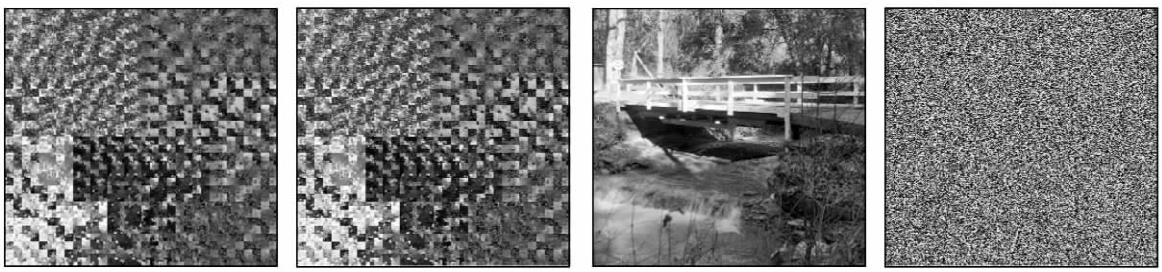
c 从所述载体图像中提取出来的秘密图像和原始秘密图像

图15 秘密信息嵌入载体图像前后的视觉效果

Fig. 15 The visual effect before and after the secret information is embedded in the carrier image

3.2 安全性比较

通过直接提取隐写图像的LSB检验隐写方案的安全性。具体提取方法如下。对文献[16-17]，首先提取R信道的LSB作为2比特段的第1位比特，然后随机提取G或B信道的LSB作为2比特段的第2位比特。对文献[15]，由于嵌入容量为每像素3 bit/pixel，因此直接提取RGB 3通道的LSB作为3比特段。对笔者提出的方案，首先提取RGB 3通道的第2个LSB作为6比特段的前3位比特，然后再提取LSB 3通道的第1个LSB为6比特段的最后3位比特。图16显示了通过直接提取隐写图像的LSB而得到的4种隐写结果。



a 文献[16]方案 b 文献[17]方案 c 文献[15]方案 d 笔者方案

图16 4种方案直接提取隐写图像中RGB 3通道的LSB得到的秘密图像

Fig. 16 The secret image obtained by directly extracting the LSB of the RGB threechannels in the stego-image for four schemes

从图16中可以看出，笔者提出的方案和文献[17]中的方案更加安全，文献[16]中的方案安全性较低，而文献[15]中的方案基本没有任何安全性。与文献[15]中的方案不同，在笔者提出的方案中，秘密比特并没有直接嵌入到载体图像中。根据格雷码嵌入规则，大约50%嵌入后的秘密比特在隐写图像中翻转。以图15中的3个秘密图像为例，具体的数值结果如表2所示。

表 2　隐藏秘密比特与载体图像 LSBs 的数量比较

Tab. 2　Quantity comparison of hiding secret bits and LSBs of cover image

载体图像	图 15 的秘密图像 a				图 15 的秘密图像 b			
	秘密比特 0(750 945)		秘密比特 1(821 919)		秘密比特 0(1 092 363)		秘密比特 1(480 501)	
	翻转为 0	翻转为 1	翻转为 0	翻转为 1	翻转为 0	翻转为 1	翻转为 0	翻转为 1
图 12a	369 050	381 895	416 111	405 808	545 338	547 025	242 122	238 379
图 12b	369 408	381 537	417 180	404 739	545 015	547 348	243 318	237 183
图 12c	374 048	376 897	412 226	409 693	543 666	548 697	241 891	238 610
图 12d	379 261	371 684	409 155	412 764	543 759	548 604	238 188	242 313
图 12e	372 616	378 329	412 076	409 843	551 324	541 039	240 069	240 432
图 12f	374 792	376 153	410 928	410 991	554 193	538 170	237 990	242 511

载体图像	图 15 的秘密图像 c			
	秘密比特 0(800 664)		秘密比特 1(772 200)	
	翻转为 0	翻转为 1	翻转为 0	翻转为 1
图 12a	395 364	405 300	389 663	382 537
图 12b	395 501	405 163	389 383	382 817
图 12c	398 116	402 548	388 396	383 804
图 12d	403 475	397 189	383 593	388 607
图 12e	399 302	401 362	385 032	387 168
图 12f	400 330	400 334	385 872	386 328

3.3　嵌入容量

关于隐写方案的嵌入容量，文献 [8] 将其定义为秘密图像量子比特数与载体图像像素数的比值，即

$$C = \frac{\text{秘密图像量子比特数}}{\text{载体图像像素数}} \tag{8}$$

根据式(8)，笔者方案的嵌入容量 $C = (6 \times 2^n \times 2^n) / (2^n \times 2^n) = 6(\text{bit/pixel})$。而文献 [15] 中方案的嵌入容量为 3 bit/pixel，文献 [16] 和文献 [17] 中方案的嵌入容量仅为 2 bit/pixel。

4　结　语

笔者研究了基于量子计算机上 LSB 替换思想的彩色图像隐写的实现方法。该方案没有采用秘密比特直接取代载体图像的 LSB，而是通过格雷码规则将秘密信息间接嵌入到 LSB 中，提高了隐写的安全性。与现有的几种彩色图像的量子隐写方案相比，该方案具有可接受的 PSNR，最显著的优点是具有较大的嵌入容量和较高的安全性。此外如何提高在噪声下的鲁棒性能是下一步要进行的工作。

参考文献:

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

[2] MASTRIANI M. Quantum Image Processing: the Pros and Cons of the Techniques for the Internal Representation of the Image. A Reply to: A Comment on "Quantum Image Processing?" [J]. Quantum Information Processing, 2020, 19(5): 1-17.

[3] VENEGAS-ANDRACA S E, BOSE S. Storing, Processing, and Retrieving an Image Using Quantum Mechanics [C] // Proceedings of SPIE-The International Society for Optical Engineering. [S.l.]: SPIE, 2003: 137-147.

[4] LATORRE J I. Image Compression and Entanglement [J/OL]. (2005-10-04) [2021-04-06]. https://arxiv.org/pdf/quant-ph/0510031.pdf.

[5] LE P Q, DONG F, HIROTA K. A Flexible Representation of Quantum Images for Polynomial Preparation, Image Compression, and Processing Operations [J]. Quantum Information Processing, 2011, 10(1): 63-84.

[6] LE P Q, ILIYASU A M, DONG F, et al. A Flexible Representation and Invertible Transformations for Images on Quantum Computers [C] // New Advances in Intelligent Signal Processing. Berlin, Heidelberg: Springer, 2011: 179-202.

[7] YAN F, ILIYASU A M, VENEGAS-ANDRACA S E. A Survey of Quantum Image Representations [J]. Quantum Information

Processing, 2016, 15(1): 1-35.
[8] EVSUTIN O O, MELMAN A S, MESHCHERYAKOV R V. Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions [J]. IEEE Access, 2020, 8: 166589-166611.
[9] QU Z, LI Z, XU G, et al. Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm [J]. IEEE Access, 2019, 7: 50849-50857.
[10] JIANG N, WANG L. A Novel Strategy for Quantum Image Steganography Based on Moiré Pattern [J]. International Journal of Theoretical Physics, 2015, 54(3): 1021-1032.
[11] WANG S, SANG J, SONG X, et al. Least Significant Qubit (LSQb) Information Hiding Algorithm for Quantum Image [J]. Measurement, 2015, 73: 352-359.
[12] JIANG N, ZHAO N, WANG L. LSB Based Quantum Image Steganography Algorithm [J]. International Journal of Theoretical Physics, 2016, 55(1): 107-123.
[13] NASERI M, HEIDARI S, BAGHFALAKI M, et al. A New Secure Quantum Watermarking Scheme [J]. Optik, 2017, 139: 77-86.
[14] ZHOU R G, HU W, FAN P. Quantum Watermarking Scheme through Arnold Scrambling and LSB Steganography [J]. Quantum Information Processing, 2017, 16(9): 1-21.
[15] SANG J, WANG S, LI Q. Least Significant Qubit Algorithm for Quantum Images [J]. Quantum Information Processing, 2016, 15(11): 4441-4460.
[16] HEIDARI S, POURARIAN M R, GHEIBI R, et al. Quantum Red-Green-Blue Image Steganography [J]. International Journal of Quantum Information, 2017, 15(5): 336-360.
[17] HEIDARI S, FARZADNIA E. A Novel Quantum LSB-Based Steganography Method Using the Gray Code for Colored Quantum Images [J]. Quantum Information Processing, 2017, 16(10): 1-28.
[18] HEIDARI S, GHEIBI R, HOUSHMAND M, et al. A Robust Blind Quantum Copyright Protection Method for Colored Images Based on Owner's Signature [J]. International Journal of Theoretical Physics, 2017, 56(8): 2562-2578.
[19] AHIN E, YILMAZ I. QRMW: Quantum Representation of Multi Wavelength Images [J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2018, 26(2): 768-779.
[20] WANG X, GAO S. A Chaotic Image Encryption Algorithm Based on a Counting System and the Semi-Tensor Product [J]. Multimedia Tools and Applications, 2021, 80(7): 10301-10322.
[21] FRANK G. Pulse Code Communication: US, 2632058 [P]. 1953-03-17.
[22] WU Z, GUO W, LI Y, et al. High-Speed and High-Efficiency Three-Dimensional Shape Measurement Based on Gray-Coded Light [J]. Photonics Research, 2020, 8(6): 819-829.
[23] CHEN C C, CHANG C C. LSB-Based Steganography Using Reflected Gray Code [J]. IEICE Transactions on Information and Systems, 2008, 91(4): 1110-1116.
[24] JIANG N, WANG J, MU Y. Quantum Image Scaling up Based on Nearest-Neighbor Interpolation with Integer Scaling Ratio [J]. Quantum Information Processing, 2015, 14(11): 4001-4026.
[25] JIANG N. Quantum Image Processing [M]. Beijing: Tsinghua University Press, 2016.
[26] ZAINI H G. Image Segmentation to Secure LSB2 Data Steganography [J]. Engineering, Technology & Applied Science Research, 2021, 11(1): 6632-6636.
[27] QUAN D X, NIU L, ZHU L L, et al. Efficient Fault-Tolerant Logical Hadamard Gates Implementation in Reed-Muller Quantum Codes [J/OL]. Concurrency and Computation: Practice and Experience. (2020-11-20) [2021-04-05]. https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.6079.
[28] HASAN A M, MOHEBBIAN M R, WAHID K A, et al. Hybrid-Collaborative Noise2Noise Denoiser for Low-Dose CT Images [J]. IEEE Transactions on Radiation and Plasma Medical Sciences, 2020, 5(2): 235-244.

(责任编辑: 刘俏亮)