基于量子舒尔变换和图像的信息隐藏

胡万斌，廖　伟，刘志鑫，董玉民*

(重庆师范大学计算机与信息科学学院　重庆 沙坪坝区　401331)

【摘要】如何在载体 (文本、图像、音频) 中巧妙地嵌入秘密信息及扩大传输信息的容量一直是研究人员面临的挑战。从量子信息的角度提出了一种新的信息隐藏思想，在不破坏载体数据的情况下构造量子纠缠态实现了秘密信息的隐藏和传输。为了提高秘密信息的传输容量，将经过 Schur 变换压缩的量子秘密信息编码到纠缠态的相位中进行传输。在比特传输过程中，新协议能够安全隐蔽地发送秘密量子比特信息。接收方可以通过量子傅里叶变换和已接收量子态的测量结果来提取秘密信息并得到无损的量子图像。此外，还给出了提取秘密量子态信息的具体方法，将量子比特转换为经典比特信息，有效地提升了秘密信息传输容量。该方案在不牺牲载体图像质量的前提下，保证了秘密信息传输的安全性。

关　键　词　量子图像；　量子信息隐藏；　量子隐写；　量子舒尔变换

中图分类号　TP309.2　　**文献标志码**　A　　doi:10.12178/1001-0548.2022270

Information Hiding Based on Quantum Schur Transformation and Images

HU Wanbin, LIAO Wei, LIU Zhixin, and DONG Yumin*

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

Abstract　How to subtly embed secret information in carriers (text, image, audio) has been a challenge for researchers. From the perspective of quantum information, a new idea of information hiding is proposed to construct quantum entangled states to realize the hiding and transmission of secret information without destroying the carrier data in this paper. In order to increase the transmission capacity of secret information, the quantum secret information compressed by Schur transform is encoded into the phase of the entangled state for transmission. During the bit transmission, the new protocol can securely and covertly send secret quantum bit information. The receiver can extract the secret information and obtain a lossless quantum image by using the quantum Fourier transform (QFT) and the measurement results of the received quantum state. In addition, a specific method is given to extract the secret quantum state information and then convert the quantum bits to classical bits, which can effectively increase the capacity of secret information transmission. This scheme ensures the security of the secret information transmission without sacrificing the carrier image quality.

Key words　quantum image;　quantum information hiding;　quantum schur transform;　quantum steganography

信息隐藏是将秘密信息通过某些巧妙的方式嵌入一个无需公开保密的载体中，并且要保证秘密信息的隐蔽性。目前的信息隐藏技术主要分为信息隐写技术[1-2] 和水印技术[3]。隐写技术是指秘密信息嵌入某个无需保密的载体中实现秘密通信。而水印技术一般用作数字版权保护，在数据中嵌入特殊标识保护作者权益。但随着量子并行技术的兴起[4]，传统的信息隐藏技术受到冲击。量子力学中的不确定性原理、量子测量坍塌原理和量子态不可克隆原理使得量子信息隐藏技术在安全性和隐蔽性上比经典信息隐藏更具优势。于是，研究者们将目光从经典信息隐藏转向量子信息隐藏[5-7]。

图像是通信过程中最常用的多媒体信息之一，近年来量子图像的研究成果颇丰[8-10]。文献 [11] 在 FRQI(flexible representation of quantum images) 的基础上提出了一种新的量子图像模型 NEQR(novel

收稿日期：2022－08－14；修回日期：2022－11－11

基金项目：国家自然科学基金 (61772295, 61572270)；重庆市教委科学技术研究项目 (KJZD-M202000501)；重庆市技术创新与应用发展项目 (cstc2020jscxlyjsAX0002)；重庆市技术预见与制度创新项目 (cstc2021jsyj-yzysbAX0011)

作者简介：胡万斌 (1997－)，男，主要从事量子信息及信息安全方面的研究.

*通信作者：董玉民，E-mail：dym@cqnu.edu.cn

enhanced quantum representation)。与 FRQI 相比，NEQR 模型的制备复杂度实现了二次加速，许多复杂的图像处理操作都可以基于 NEQR 来设计。得益于量子图像的发展，量子信息隐藏技术也发展迅速。相比于水印技术的单一场景，基于图像的信息隐藏技术凭借其嵌入容量大、隐蔽性高的优点在实际生活中获得了更广泛的应用。因此，结合量子信息的优势和图像信息隐藏的特点来研究基于量子图像的信息隐藏技术具有重要意义。与经典图像信息隐藏一样，量子图像信息隐藏主要分为量子图像水印[12-14] 和量子图像隐写[15-17]。量子图像水印技术以量子图像为载体，同样具有嵌入容量大、易实现的特点。

目前主流的量子图像隐写方案主要分为两个方向。1) 一种是受经典图像隐写算法启发，将经典最低有效位 (least significant bit, LSB) 算法拓展到量子图像中并进行创新。如 2016 年，文献 [18] 在 NEQR 的基础上直接将秘密信息的量子位与图像像素的最低有效量子位交换实现了与经典最低有效位算法相对应的量子隐写算法，但该方法安全性较差且易受外界因素影响。因此，作者又提出先将载体图像分块再进行秘密信息嵌入的方案，该方案在一定程度上提升了算法的安全性和隐蔽性。文献 [19] 同样在量子 LSB 算法的基础上提出了 3 种改进算法，并在彩色量子图像上实现了信息隐藏。2019 年，文献 [20] 使用最优最低有效位法研究了用于信息隐藏两级嵌入的量子隐写算法，双重嵌入使嵌入的位置具有一定的随机性，从而增强了算法的安全性。文献 [21] 提出了一种基于龟壳和 LSB 算法的量子图像隐写算法，同时在方案中引入了人类视觉系统 (human visual system, HVS)模型和校验码，提升了算法的隐蔽性。2) 另一方向则通过编码的方式实现量子信息隐藏。文献 [22]实现了基于 Gray 码的量子图像信息隐藏，该方案与 LSB 算法相比，有效地增大了秘密信息的嵌入容量。文献 [23] 提出了基于 ASCII 码的盲量子隐写协议，该方案相较于其他隐写算法具有更低的复杂度。文献 [24] 利用矩阵编码良好的不可感知性和高嵌入效率提出了一种新的基于矩阵编码的量子彩色图像隐写术算法。2022 年，文献 [25] 提出了两种基于双层矩阵编码的协议，在 IBM 的量子平台上成功运行了协议的核心电路并给出了相应结果。

在经典信息隐藏技术和量子信息隐藏技术中，无论是哪一种基于图像的信息隐藏技术通常都需要破坏载体图像的数据。本文提出了一种基于舒尔变换和图像的量子信息隐写方案，在不破坏量子图像质量的前提下，利用量子态的物理特性实现秘密信息的隐藏，通过一定的操作实现秘密消息的恢复。首先，制备了 $4n+2q$ 量子纠缠态，利用舒尔变换压缩秘密信息以扩大传输秘密数据的容量，再将秘密信息编码到纠缠态中。使用量子图像作为数据载体，在量子图像上应用量子傅里叶逆变换 (IQFT)，然后将量子图像与秘密信息纠缠在一起，无需破坏量子图像。再将载体信息和秘密信息编码到发送方和接收方共享的纠缠态相位中。在这个纠缠态中，载体信息和秘密信息都不会被泄露。最后，接收方通过应用 QFT 和手中量子态的测量结果来恢复秘密消息和量子图像。

1 量子预备知识

1.1 NEQR 量子图像

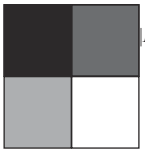
越来越多的研究人员致力于量子图像处理，各种量子图像表示法相继提出，如 FRQI、NEQR、MCQI[26] 和 QUALPI[27] 等。其中，FRQI 是一种经典的量子图像表示方案。该方案利用量子叠加，仅使用$2n+1$个量子比特存储$2^n\times 2^n$的量子灰度图像。然而，这种量子图像表示限制了量子变换的多样性和复杂性。NEQR 则克服了这些缺陷，对于$2^n\times 2^n$的量子图像，NEQR 的表达式为：

$$|I\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=0}^{q-1}|C_{YX}^{i}\rangle|YX\rangle \tag{1}$$

式中，$|f(Y,X)\rangle$表示颜色；$|YX\rangle$表示位置信息；$|f(Y,X)\rangle$用二进制编码表示为：

$$f(Y,X)=C_{YX}^{0}C_{YX}^{1}\cdots C_{YX}^{q-2}C_{YX}^{q-1} \tag{2}$$

式中，$C_{YX}^{i}\in[0,1]$; $f(Y,X)\in[0,2^q-1]$。图 1 是一个2×2大小的 NEQR 量子图像。



$|I\rangle=\frac{1}{2}(|0\rangle\otimes|00\rangle+|100\rangle\otimes|01\rangle+|200\rangle\otimes|10\rangle+|255\rangle\otimes|11\rangle)=$
$\frac{1}{2}(|00000000\rangle\otimes|00\rangle+|01100100\rangle\otimes|01\rangle+$
$|11001000\rangle\otimes|10\rangle+|11111111\rangle\otimes|11\rangle)$

图 1 NEQR 量子图像表示方式

1.2 量子傅里叶变换

在数学上，离散傅里叶变换是一种重要变换，是把一个离散函数映射为另一个离散函数。而在量子计算中，将作用于空间C^{2n}离散傅里叶变换称为量子傅里叶变换：

$$\mathrm{QFT}: U_{\mathrm{QFT}}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{t=0}^{2^n-1} \mathrm{e}^{2\pi\, itx/2^n}|t\rangle \tag{3}$$

式中，输入量子态为$|x\rangle, x = 0, 1, \cdots 2^n - 1$，二进制表示为$j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$，所以量子傅里叶变换的形式变为$|j_1, j_2, \cdots, j_n\rangle \to \left(|0\rangle + \mathrm{e}^{2\pi\, i0.j_n}|1\rangle\right)(|0\rangle + \mathrm{e}^{2\pi\, i0.j_{n-1}j_n}|1\rangle)\cdots\left(|0\rangle + \mathrm{e}^{2\pi\, i0.j_1 j_2\cdots j_n}|1\rangle\right)/2^{\frac{n}{2}}$。

具体的量子傅里叶变换电路如图 2 所示。

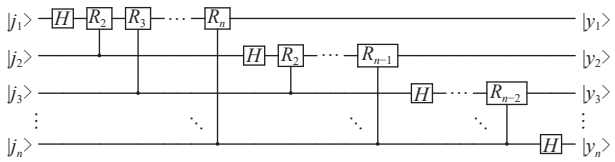


图 2　量子傅里叶变换电路图

图中，H 是 Hadamard 门；R 是受控旋转门。类似地，可以将量子傅里叶逆变换 (IQFT) 定义为：

$$\mathrm{IQFT}|k\rangle = \frac{1}{\sqrt{d}}\sum_{x=0}^{d-1} \mathrm{e}^{-i\frac{2\pi xk}{d}}|x\rangle \tag{4}$$

1.3　量子加法器

量子 Shor 算法和 Grover 搜索的效率激发了研究人员对量子算术运算的兴趣。研究人员对量子算术运算的研究也取得了一些成果。文献 [28] 提出了一种 QFT 加法器，验证了如何用量子加法操作实现相位编码操作。在变换域中，需要量子算符来作用于量子态的分布相位。这些运算符的基本单位是受控相位门 CZ。对于输入 N 维系统的$|x\rangle$、$|y\rangle$，量子态可以进行 QFT 变换，将$|y\rangle$编码到相位中：

$$|x\rangle|y\rangle \xrightarrow{\mathrm{QFT}} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \mathrm{e}^{i\frac{2\pi yk}{N}}|x\rangle|k\rangle \tag{5}$$

再对$|x\rangle$施加受控相位门 CZ：

$$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \mathrm{e}^{i\frac{2\pi yk}{N}}|x\rangle|k\rangle \xrightarrow{\mathrm{CZ}} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \mathrm{e}^{i\frac{2\pi yk}{N}}\mathrm{e}^{i\frac{2\pi xk}{N}}|x\rangle|k\rangle \tag{6}$$

最后通过 IQFT 得到计算结果：

$$\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \mathrm{e}^{i\frac{2\pi(x+y)k}{N}}|x\rangle|k\rangle \xrightarrow{\mathrm{IQFT}} \frac{1}{N}\sum_{k,l=0}^{N-1} \mathrm{e}^{i\frac{2\pi(x+y)k}{N}}\mathrm{e}^{-i\frac{2\pi kl}{N}}|x\rangle|l\rangle = |x\rangle|x+y(\mathrm{mod}N)\rangle \tag{7}$$

1.4　基于量子舒尔变换的信息压缩

量子舒尔变换是量子信息论中的一个基本协议。虽然 Schur-Weyl 对偶允许同时进行不可约表示，将 d 维复杂空间的 n 次张量积分解为酉群和对称群，但 Schur 变换将标准基础更改为全局基础。2005 年，Dave Bacon 等人实现了量子 Schur 变换，这使得许多量子信息协议在实验上可行。之后，文献 [29] 在此基础上提出了基于量子舒尔变换的量子压缩协议，具体过程如下。

$\mathcal{E}: \mathcal{H}^{\otimes N} \to \mathcal{H}_{\mathrm{enc}}$表示编码过程；$\mathcal{D}: \mathcal{H}_{\mathrm{enc}} \to \mathcal{H}^{\otimes N}$表示解码过程；$\rho\otimes N$表示量子态集。根据 Schur-Weyl 对偶的基本理论，N 个量子比特的 Hilbert 空间可以分解为：

$$\mathcal{H}^{\otimes N} \simeq \oplus_{j=0}^{N/2}\left(\mathcal{R}_j \otimes \mathcal{M}_j\right) \tag{8}$$

式中，j是总角动量的量子数；$\mathcal{R}_j$是表示张量空间；$\mathcal{M}_j$是复数空间。现在，由于状态$\rho\otimes N$在N量子位的置换下是不变的，有：

$$\rho_{\boldsymbol{n}}^{\otimes N} = \oplus_{j=0}^{N/2} q_{j,N}\left(\rho_{\boldsymbol{n},j} \otimes \frac{I_{m_j}}{m_j}\right) \tag{9}$$

式中，$q_{j,N}$是j中合适的概率分布；$\rho_{\boldsymbol{n},j}$是$\mathcal{R}_j$上的量子态；I_{m_j}是$\mathcal{M}_j$上的恒等式；m_j是$\mathcal{M}_j$的维数。因此，$\rho\otimes N$可以被编码为量子态$\mathcal{E}\left(\rho_{\boldsymbol{n}}^{\otimes N}\right) = \bigoplus_j q_{j,N}\rho_{\boldsymbol{n},j}$，初始状态可以被编码为$\lg N$，解码过程是：

$$\mathcal{D}(\rho) := \bigoplus_j \left(P_j \rho P_j \otimes \frac{I_{m_j}}{m_j}\right) \tag{10}$$

2　量子信息隐藏方案

数字图像的每个像素值要么表示为单个灰度值，要么表示为 RGB 像素值。因此经典的 LSB 算法的思路就是牺牲分配给灰度值的最低有效位来编码秘密信息，隐藏数据是通过将载体数据的部分数据替换为秘密信息而实现的。为了清楚地说明 LSB 技术的原理，可以用一个简单的例子来描述它。假设需要在 3×3 图像中隐藏二进制秘密消息 11001001，图像像素值也用 8 位二进制表示，嵌入和提取过程如图 3 所示。载体图像的每个像素的最低有效位被标记为红色，最低有效位为 110111100，秘密消息被替换为最低有效位，替换位被标记为蓝色。只提取每个像素位置的最低有效位来恢复秘密信息。这种方法也经常用于量子图像信息隐藏，但这种技术不可避免地会导致载体图像质量下降。相比之下，本文方案中的信息隐藏是通过将一些量子态与对应于载体数据信息的秘密消息相结合来实现的，这使得信息隐藏不会影响量子图像的视觉质量。

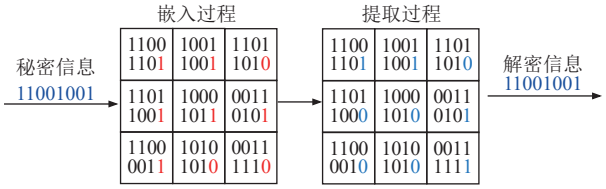


图 3 LSB 算法原理图

本节将展示如何将秘密消息 m 隐藏在 NEQR 量子图像$\boldsymbol{I}$中，其中$\boldsymbol{I}$包含 $2n+q$ 量子位，并发送到接收器。图 4 是整个信息隐藏过程的流程图。

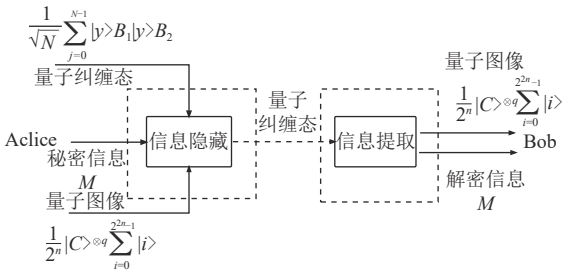


图 4 量子图像信息隐藏流程图

1) 首先需要安全可信的第三方来准备 $4n+2q$ 量子纠缠态：

$$\sum_{y=0}^{N-1}|y\rangle_{B_1}|y\rangle_{B_2} \tag{11}$$

式中，B_1、B_2是两个长度为$2n+q$的量子寄存器。其中 Alice 有第一个寄存器B_1，Bob 有第二个寄存器B_2。这种状态必须在双方之间安全共享。

2) 假设要隐藏的信息是$|K\rangle=|K_0K_1\cdots K_N\rangle$。为了增加可隐藏信息的容量，可以使用压缩协议[29]压缩$|K\rangle$以获得$|m\rangle$。如图 5 所示，首先使用一个类量子 Schur 变换操作，它将初始的N量子位与$O(\lg(N))$辅助量子位一起转换为 3 个寄存器 J、R 和 M。J 是索引寄存器用于存储$\lg(N/2+1)$量子位的状态；R 寄存器对表示空间进行编码；M 则是一个多重性寄存器，其中多重性空间被编码为$\lg(N)$量子位。该压缩电路的效率为$N/\lg(N)$，即 N 个比特的信息可以压缩为$\lg(N)$比特信息，能够有效提升秘密信息传输容量。

3) 将秘密信息编码到量子纠缠态中：

$$\frac{1}{\sqrt{2^{2n+q}}}\sum_{y=0}^{2^{2n+q}-1}\mathrm{e}^{-2i\pi my/2^{2n+q}}|y\rangle_{B_1}|y\rangle_{B_2} \tag{12}$$

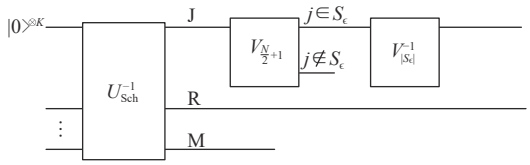


图 5 量子压缩编码

4) Alice 创建 NEQR 量子态：

$$|I_1\rangle=\frac{1}{\sqrt{2^{2n+q}}}|0\rangle^{\otimes q}|0\rangle^{\otimes 2n} \tag{13}$$

然后通过在像素寄存器和位置寄存器中应用 $2n$个 Hadamard 门和 $\boldsymbol{U}_{YX}$ 门，获得$2^n\times 2^n$NEQR 量子图像：

$$|I_2\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y,X)\rangle|YX\rangle=$$
$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=0}^{q-1}|C_{YX}^i\rangle\otimes_{j=0}^{n-1}|y_Y^j\rangle\otimes_{j=0}^{n-1}|x_X^j\rangle=$$
$$\frac{1}{2^n}|c\rangle^{\otimes q}\otimes\sum_{i=0}^{2^{2n}-1}|i\rangle \tag{14}$$

5) 对 NEQR 量子图像执行 IQFT，使量子图像的形式与秘密消息的形式一致：

$$|I_3\rangle=\mathrm{IQFT}(|I_2\rangle)=$$
$$\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\mathrm{IQFT}\left(|c_{YX}^0\ldots c_{YX}^{q-1}y_{YX}^0\ldots y_{YX}^{n-1}x_{YX}^0\ldots x_{YX}^{n-1}\rangle\right)\right)=$$
$$\frac{1}{2^n}\frac{1}{\sqrt{2^n}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(|0\rangle+\mathrm{e}^{-2i\pi\,0.x_{YX}^{n-1}}|1\rangle\right)\otimes$$
$$\left(|0\rangle+\mathrm{e}^{-2i\pi\,0.x_{YX}^{n-2}x_{YX}^{n-1}}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle+\mathrm{e}^{-2i\pi\,0.c_{YX}^0c_{YX}^1\cdots x_{YX}^{n-1}}|1\rangle\right) \tag{15}$$

令$\left|c_{YX}^0\cdots c_{YX}^{q-1}y_{YX}^0\cdots y_{YX}^{n-1}x_{YX}^0\cdots x_{YX}^{n-1}\right\rangle=|I_{YX}\rangle$，得到：

$$|I_3\rangle=\frac{1}{2^n}\frac{1}{\sqrt{2^n}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(\sum_{k=0}^{N}\mathrm{e}^{-2i\pi\,l_{YX}k/N}|k\rangle\right) \tag{16}$$

6) 与步骤 3) 中量子态合并，形成一个新的纠缠态：

$$|I_4\rangle=\frac{1}{2^n}\frac{1}{\sqrt{2^{2n+q}}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(\sum_{k=0}^{N}\mathrm{e}^{-2i\pi\,l_{YX}k/N}|k\rangle\right)\frac{1}{\sqrt{2^{2n+q}}}\sum_{y=0}^{2^{2n+q}-1}\mathrm{e}^{-i2\pi\,my/2^{2n+q}}|y\rangle_{B_1}|y\rangle_{B_2}\rightarrow$$
$$\frac{1}{2^n}\frac{1}{\sqrt{N^2}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{k=0}^{N-1}\sum_{y=0}^{N-1}\mathrm{e}^{-i2\pi\,l_{YX}k/N}\mathrm{e}^{-i2\pi\,my/N}|k\rangle|k+y\rangle_{B_1}|y\rangle_{B_2}=$$
$$\frac{1}{2^n}\frac{1}{\sqrt{N}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{y=0}^{N-1}\mathrm{e}^{-i2\pi\,my/N}\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{-i2\pi\,l_{YX}k/N}|k\rangle|k+y\rangle_{B_1}|y\rangle_{B_2}\right) \tag{17}$$

这意味着已经成功地将秘密消息$|m\rangle$嵌入到载体数据中且没有破坏载体数据。秘密信息独立于量子图像信息，实现了在不修改载体数据的情况下隐藏数据的目的。

7) Alice 将量子图像I_4和寄存器B_1发送给 Bob。

8) Bob 接收量子图像和B_1，并通过 QFT 恢复秘密信息和量子图像信息：

$$\frac{1}{2^n}\frac{1}{\sqrt{N}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{y=0}^{N-1}\mathrm{e}^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{-i2\pi\, l_{YX}k/N}|k\rangle|k+y\rangle_{B_1}|y\rangle_{B_2}\right)=$$

$$\frac{1}{2^n}\frac{1}{\sqrt{N^5}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{y=0}^{N-1}\sum_{k=0}^{N-1}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_1=0}^{N-1}\mathrm{e}^{-i2\pi my/N}\mathrm{e}^{-i2\pi l_{YX}k/N}\mathrm{e}^{i2\pi\pi kx_1/N}\times\mathrm{e}^{i2\pi(k+y)x_2/N}\mathrm{e}^{i2\pi yy_1/N}|k\rangle|k+y\rangle_{B_1}|y\rangle_{B_2}=$$

$$\frac{1}{2^n}\frac{1}{\sqrt{N^5}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_1=0}^{N-1}\left(\sum_{k=0}^{N-1}\mathrm{e}^{i2\pi\,(x_1+x_2-l_{YX})k/N}\right)\times\left(\sum_{y=0}^{N-1}\mathrm{e}^{i2\pi(y_1+x_2-m)y/N}\right)|x_1\rangle|x_2\rangle_{B_1}|y_1\rangle_{B_2}\tag{18}$$

9) 将量子傅里叶加法器应用于寄存器中的$|x_1\rangle,|y_1\rangle$：

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|x_1\rangle\mathrm{IQFT}\cdot\mathrm{CZ}\cdot\mathrm{QFT}|x_2\rangle_{B_1}|y_1\rangle_{B_2}=$$

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|x_1\rangle|x_2\rangle|x_2+y_1(\bmod N)\rangle\tag{19}$$

10) 将量子傅里叶加法器应用于$|x_1\rangle$和$|x_2\rangle$：

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\mathrm{IQFT}\cdot\mathrm{CZ}\cdot\mathrm{QFT}|x_1\rangle|x_2\rangle|x_2+y_1\,(\mathrm{mod}N)\rangle=$$

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|x_1\rangle|x_1+x_2\,(\mathrm{mod}N)\rangle|x_2+y_1\,(\mathrm{mod}N)\rangle=$$

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|x_1\rangle|l_{YX}\rangle|m\rangle\tag{20}$$

然后解码$|m\rangle$，具体电路如图 6 所示。

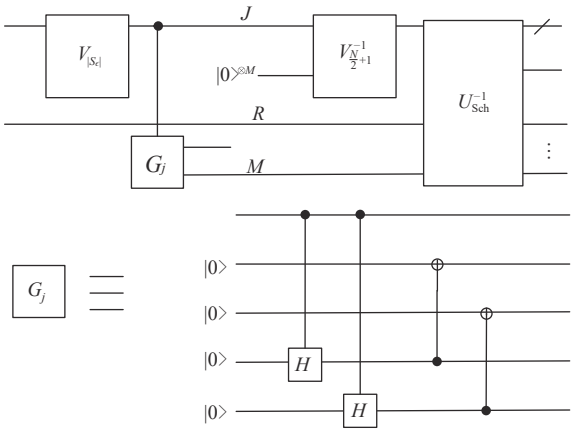


图 6　量子压缩解码电路

最终，得到量子图像$|l_{YX}\rangle$和秘密信息$|K\rangle$。

3　分　析

3.1　安全性分析

为了保障传输过程的安全性，可以在该方案传输前发送一个验证信息来确保传输过程不被窃听。首先，Alice 从选择的正交基底中随机挑选值组成一组验证序列 $\boldsymbol{V}_1$，接着将 $\boldsymbol{V}_1$ 和量子纠缠态混合成新的粒子序列 $\boldsymbol{V}_2$，并将 $\boldsymbol{V}_2$ 发送给 Bob。Bob 通过被告知的验证序列基底和位置进行测量，再将初始态信息和测量结果进行比较计算出错误率，若错误率大于给定的阈值则终止发送信息，反之信道是安全的，可以采用本文的方案传输秘密信息。

在传输秘密信息的过程中，传输的量子态$\frac{1}{2^n}\frac{1}{\sqrt{N}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{y=0}^{N-1}\mathrm{e}^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{-i2\pi lk/N}|k\rangle|k+y\rangle|y\rangle\right)$是量子图像和秘密信息的叠加态，其中每一个粒子都能够以相同的概率取任意值，这意味着即使传输信息被窃听截取也无法直接获取信息。此外，Alice 作为信息的发送方存在数据泄露的风险。当数据发生泄漏时，任何人都可能对量子态$\frac{1}{2^n}\frac{1}{\sqrt{N}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\sum_{y=0}^{N-1}\mathrm{e}^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\mathrm{e}^{-i2\pi lk/N}|k\rangle|k+y\rangle|y\rangle\right)$中的部分态进行逆操作，再通过测量两个寄存器得到测量结果。但是，从步骤 8) 可以看出，即使任何逆操作都可以运用到寄存器上，想要提取秘密信息 m 必须知道寄存器 B_2 中每一个$|y\rangle$。而只有 Bob 才有纠缠态的寄存器 B_2，所以只有 Bob 可以提取出秘密信息 m。

3.2　复杂度和嵌入容量分析

本文方案先使用量子 Schur 变换将秘密信息进行压缩，文献 [29] 给出了信息压缩的复杂度$O(n)$。步骤 3) 运用 $2n+q$ 个相位门将秘密信息嵌入纠缠态中。接着构建一个 $2^n\times2^n$ 的 NEQR 量子图像，在步骤 4) 中需要$2n$个 $\boldsymbol{H}$ 门和 $\boldsymbol{U}_{YX}$操作，而一个 $\boldsymbol{U}_{YX}$ 操作的复杂度为$O(qn)$[11]，因此构建一个 $2^n\times2^n$ 的 NEQR 量子图像，其总复杂度为$O(qn2^{2n})$。步骤 5) 使用了

量子傅里叶逆变换，复杂度为$O(n^2)$。而在提取隐秘信息m的过程中，需要对3个寄存器执行QFT，在文献[4]中可以知道QFT的复杂度为$O(n^2)$。步骤9)和10)用到了量子加法器，QFT加法器主要依靠QFT和受控相移门实现，文献[28]给出了量子加法器的复杂度$O(n^2)$。因此，整个协议的复杂度为$O(qn2^{2n}+6n^2+2n)$。

LSB方案中，信息嵌入容量取决于量子图像大小。对于一幅$N\times N$的量子灰度图像，理论上可以嵌入N^2比特信息，为了考虑视觉效果，可以嵌入的秘密信息比特非常有限。而本文方案中秘密信息并没有嵌入量子图像的颜色信息中，而是构建了一种新的量子纠缠态，因此不受量子图像大小的限制。传输的秘密信息$m>N^2$，能够有效增大秘密信息的传输容量。

4 结束语

本文利用量子传输协议，提出了一种基于量子舒尔变换和图像的信息隐藏方案。该方案可以将秘密信息和量子图像编码到高维量子纠缠态的相位之中实现信息隐藏，并通过测量结果和执行一些逆操作解密传输的秘密信息和量子图像。与其他采用LSB算法的方案相比，本文方案采用量子Schur变换实现信息压缩，打破了传统方案中传输容量的限制，有效地提升了传输秘密信息的容量。此外，由于本文方案并没有像LSB算法那样对图像的像素进行替换，而是利用量子态的物理特性实现秘密信息的隐藏，因此不会造成量子图像的质量损失。通过分析表明，本文所提出的方案在保障信息安全隐蔽传输的同时能够有效提升秘密信息的嵌入容量。

参考文献

[1] ARTZ D. Digital steganography: Hiding data within data[J]. IEEE Internet Computing, 2001, 5(3): 75-80.

[2] GE H, HUANG M, QIAN W. Steganography and steganalysis based on digital image[C]// 2011 4th International Congress on Image and Signal Processing. NJ: IEEE, 2011: 252-255.

[3] SAIKIA M, HUSSAIN M A. Robust watermarking using extended anti-collusion codes[C]// 2011 International Conference on Image Information Processing. NJ: IEEE, 2011: 1-6.

[4] NIELSEN M A, CHUANG I L. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000.

[5] LUO G, ZHOU R G, MAO Y. Two-Level information hiding for quantum images using optimal LSB[J]. Quantum Information Processing, 2019, 18(10): 297-297.

[6] SHEN W, SONG X. Quantum video information hiding based on improved LSQb and motion vector[J]. Journal of Internet Technology, 2017, 18(6): 1361-1368.

[7] WANG S, SANG J, SONG X, et al. Least significant qubit (LSQb) information hiding algorithm for quantum image[J]. Measurement, 2015, 73: 352-359.

[8] VENEGAS-ANDRACA S E , BOSE S. Storing, processing and retrieving an image using quantum mechanics[C]//Conference on Quantum Information and Computation. Bellingham,WA: SPIE, 2003: 137-147.

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

[10] LE P Q, ILIYASU A M, DONG F, et al. A flexible representation of quantum images for polynomial preparation, image compression and processing operations[J]. Quantum Information Processing, 2011, 10(1): 63-84.

[11] ZHANG Y, KAI L, GAO Y, et al. NEQR: A novel enhanced quantum representation of digital images[J]. Quantum Information Processing, 2013, 12(8): 2833-2860.

[12] QU Z, CHENG Z, WANG M. A robust quantum watermark algorithm based on quantum log-polar images[J]. Interndtional Journal of Theoretical Physics, 2017, 56: 3460-3476.

[13] YAN F, ILIYASU A, SUN B, et al. A duple watermarking strategy for multi-channel quantum images[J]. Quantum Information Processing, 2015, 14(5): 1675-1692.

[14] HU W W, ZHOU R G, EL-RAFEI A, et al. Quantum image watermarking algorithm based on haar wavelet transform[J]. IEEE Access, 2019, 7: 121303-121320.

[15] LUO J, ZHOU R, LI Y, et al. Information hiding scheme based on quantum generative adversarial network[J]. Journal of Computer-Aided Design & Computer Graphics, 2021, 33(7): 983-990.

[16] MOGOS G. Stego quantum algorithm[C]//International Symposium on Cowputer Science and Its Application. NJ: IEEE, 2008:187-190.

[17] DIVINCENZO P D, LEUNG D W. Quantum data hiding[J]. IEEE Transactions on Information Theory, 2002, 48(3): 580-598.

[18] JIANG N, ZHAO N, WANG L, et al. LSB based quantum image steganography algorithm[J]. International Journal of Theoretical Physics, 2016, 55(1): 107-123.

[19] HEIDARI S, POURARIAN M R, GHEIBI R, et al. Quantum red-green-blue image steganography[J]. International Journal of Quantum Information, 2017, 15(5): 1750039.

[20] LUO G, ZHOU R G, MAO Y. Two-Level information hiding for quantum images using optimal LSB[J]. Quantum Information Processing, 2019, 18(10): 1-19.

[21] WANG M X, YANG H M, JIANG D H, et al. A novel quantum color image steganography algorithm based on turtle shell and LSB[J]. Quantum Information Processing, 2022, 21(4): 1-32.

[22] LI P, LU A. LSB-Based steganography using reflected gray code for color quantum images[J]. International

Journal of Theoretical Physics, 2018, 57(5): 1516-1548.

[23] LUO J, ZHOU R G, LIU X A, et al. A novel quantum steganography scheme based on ASCII[J]. International Journal of Quantum Information, 2019, 17(4): 1950033.

[24] QU Z, CHENG Z, WANG X. Matrix coding-based quantum image steganography algorithm[J]. IEEE Access, 2019, 7: 35684-35698.

[25] SUN H, QU Z, SUN L, et al. High-Efficiency quantum image steganography protocol based on double-layer matrix coding[J]. Quantum Information Processing, 2022, 21(5): 1-27.

[26] BO S, ILIYASU A M, FEI Y, et al. An RGB multi-channel representation for images on quantum computers[J]. Journal of Advanced Computational Intelligence & Intelligent Informatics, 2013, 17(3): 404-417.

[27] YI Z, KAI L, GAO Y, et al. A novel quantum representation for log-polar images[J]. Quantum Information Processing, 2013, 12(9): 3103-3126.

[28] RUIZ-PEREZ L, GARCIA-ESCARTIN J. C. Quantum arithmetic with the quantum fourier transform[J]. Quantum Information Processing, 2017, 16(6): 152.

[29] YANG Y, CHIRIBELLA G, EBLER D. Efficient quantum compression for ensembles of identically prepared mixed states[J]. Physical Review Letters, 2016, 116(8): 080501.

编　辑　蒋　晓