文章编号: 1001-0920(2017)03-0443-08 DOI: 10.13195/j.kzyjc.2016.0010

一种彩色图像的量子描述方法及应用

李盼池†, 曹梓崎

(东北石油大学 计算机与信息技术学院，黑龙江 大庆 163318)

摘 要: 为了提高量子彩色图像的存储效率,提出一种新的量子彩色图像描述方法. 在该方法中,像素的位置信息采用多比特量子系统的基态描述,像素的三基色灰度值信息只采用一个量子比特描述,具体描述为该量子比特的相位. 利用这种描述方法,给出量子彩色图像的几种简单操作方法,包括像素三基色灰度值的改变、互换,图像位置翻转、置换,设计一种新的量子图像水印的实现方法. 所提出的方法可在将来的量子计算机上执行. 经典计算机上的仿真结果验证了该方法的有效性.

关键词: 图像处理；量子图像描述；量子图像处理；量子图像水印

中图分类号: TP391 **文献标志码:** A

Quantum description method of color image and its application

LI Pan-chi†, CAO Zi-qi

(School of Computer and Information Technology，Northeast Petroleum University，Daqing 163318，China)

Abstract: In order to improve the storage efficiency of the quantum color image, a new method of describing quantum color image is proposed. In the proposed method, the positions of the pixels are described by the basis states of a multi-qubits system, while the grey value of three primary colors of the pixels are described by the phase of only one qubit. By using this method, several simple operations of the quantum color image are firstly presented, including the change and swap of grey values of three primary colors, and the flip and swap of the positions of the pixels. Then a new method of implementing quantum image watermarking is introduced. The proposed method can run on quantum computers in the future. The simulation results on the classic computer show the effectiveness of the proposed method.

Keywords: image processing；quantum image representing；quantum image processing；quantum image watermarking

0 引 言

数字图像处理是信息科学领域的重要分支. 近几年,量子计算和图像处理的结合已被广泛研究. 为了采用量子机制存储和处理数字图像,目前已提出的量子图像描述模型主要有:灵活的量子比特描述(FRQI)[1]、八粒子量子态描述[2]、规范任意叠加态描述(NASS)[3]、规范任意量子叠加态描述(NAQSS)[4]、相关相位的规范任意叠加态描述(NASSRP)[5]. 其中,FRQI采用一个叠加态存储图像的像素信息,就设计量子图像处理算法而言,在所有现存的模型中,它是最灵活且最适合的. 在FRQI模型的基础上,学者已经进行了很多量子图像处理的相关研究. 文献[6-7]讨论了像素位置的几何变换和颜色操作,并且证明了这些方法较传统方法有较大改进;文献[8]从图像描述、图像置乱、几何操作等多个侧面全面阐述了量子图像处理的若干关键问题;鉴于FRQI仅能描述黑白图像,文献[9]对其进行了扩展,采用3个量子比特存储RGB三基色的灰度值信息,提高了原模型的适应性. 然而,扩展的模型增加了两个量子比特,从而降低了存储效率. 如何提高彩色图像量子描述方法的存储效率是本文研究的主要目的之一.

在量子图像水印方面:文献[10]提出了在图像预定区域执行严格几何变换的水印嵌入策略;随后,文献[11-14]相继提出了基于WaQI(watermark and authenticate FRQI images)协议的量子水印策略;文献[15]提出了基于量子傅里叶变换(QFT)的水印策略,将水印图像嵌入载体图像的QFT系数中;文献[16]提出了基于量子小波变换和量子Hadamard变换的水印

收稿日期: 2016-01-04；**修回日期:** 2016-06-23.

基金项目: 国家自然科学基金项目(61170132)；黑龙江省自然科学基金项目(F2015021)；黑龙江省教育厅科学技术研究项目(12541059, 12541078).

作者简介: 李盼池(1969−), 男, 教授, 博士生导师, 从事量子智能优化和量子神经网络等研究；曹梓崎(1993−), 女, 硕士生, 从事量子图像处理的研究.

†通讯作者. E-mail: lipanchi@vip.sina.com

策略. 然而,在这些水印策略中,水印的嵌入必然会影响载体图像的视觉效果. 为此,本文将研究一种新的彩色图像的量子水印嵌入和抽取策略.

本文提出一种改进的FRQI描述方法,该方法使用的量子比特数与普通FRQI描述相同,但能描述彩色图像,既能扩展FRQI的适用范围,又能提高其存储效率. 作为改进模型的应用,基于量子比特的Bloch球面描述和绕轴旋转研究几种量子图像的处理方法,提出一种量子水印图像的嵌入和抽取方法.

1 量子比特的球面描述和绕轴旋转

在量子计算中,量子比特有两个基态$|0\rangle$和$|1\rangle$,根据叠加原理,量子比特可写为这两个基态的线性组合,即

$$|\boldsymbol{\varphi}\rangle=\cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{1}$$

其中:$0\leqslant\theta\leqslant\pi,0\leqslant\phi\leqslant2\pi$.

由于θ和ϕ连续,一个量子比特可以描述无穷多个不同的状态. 量子比特可以用三维Bloch球面上的一个点描述,此时,在Bloch球面上的任意一点$P(x,y,z)$都与一个量子比特$|\boldsymbol{\varphi}\rangle$对应,其中$x=\cos\phi\times\sin\theta,y=\sin\phi\times\sin\theta,z=\cos\theta$.

量子比特在Bloch球面上的移动可以通过绕着固定旋转轴旋转实现,旋转算子为一个二维酉矩阵. 根据量子计算原理,使量子比特在Bloch球面上绕Z轴逆时针转动δ弧度的旋转矩阵为

$$\boldsymbol{R_z}(\delta)=\begin{bmatrix}1&0\\0&\mathrm{e}^{i\delta}\end{bmatrix}. \tag{2}$$

绕一个沿单位矢量$\boldsymbol{n}=[n_x,n_y,n_z]$的轴逆时针转动$\delta$弧度的旋转矩阵为

$$\boldsymbol{R_n}(\delta)=\cos\frac{\delta}{2}\boldsymbol{I}-i\sin\frac{\delta}{2}(\boldsymbol{n}\times\boldsymbol{\sigma}). \tag{3}$$

其中:$\boldsymbol{I}$为单位矩阵;$\boldsymbol{\sigma}=[\boldsymbol{\sigma}_x,\boldsymbol{\sigma}_y,\boldsymbol{\sigma}_z]$,泡利矩阵[17]$\boldsymbol{\sigma}_x$,$\boldsymbol{\sigma}_y,\boldsymbol{\sigma}_z$表示如下:

$$\boldsymbol{\sigma}_x=\begin{bmatrix}0&1\\1&0\end{bmatrix},\boldsymbol{\sigma}_y=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\boldsymbol{\sigma}_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}. \tag{4}$$

2 彩色图像的量子描述方法

为了提高量子图像描述方法的存储效率,本文提出一种彩色图像量子描述方法(FRQCI). 对于一幅$2^n\times2^n$的彩色图像,设每个像素RGB三基色的灰度值范围均为$\{0,1,\cdots,255\}$,第k个像素的三基色灰度值分别为c_k^R,c_k^G,c_k^B,在FRQCI中,该图像可描述为

$$|I(\theta,\phi)\rangle=\frac{1}{2^n}\sum_{k=0}^{2^{2n}-1}|k\rangle|c_k\rangle, \tag{5}$$

$$|c_k\rangle=\cos\frac{\theta_k}{2}|0\rangle+\mathrm{e}^{i\phi_k}\sin\frac{\theta_k}{2}|1\rangle, \tag{6}$$

$$\theta_k=\frac{(c_k^R\times2^{16}+c_k^G\times2^8+c_k^B)\pi}{2^{24}-1}, \tag{7}$$

$$\phi_k=2\pi\times\mathrm{rand}_k. \tag{8}$$

其中:$|k\rangle$描述第k个像素的位置,$|c_k\rangle$描述第k个像素的三基色灰度值. 容易看出,式(5)所示的量子态满足如下归一化条件:

$$|||I(\theta,\phi)\rangle||=\frac{1}{2^n}\sqrt{\sum_{k=0}^{2^{2n}-1}\Big(\cos^2\frac{\theta_k}{2}+|\mathrm{e}^{i\phi_k}|^2\sin^2\frac{\theta_k}{2}\Big)}=1. \tag{9}$$

为了便于描述式(5)的实现方法,首先给出二维单位矩阵$\boldsymbol{I}$和二维Hadamard矩阵$\boldsymbol{H}$的定义如下:

$$\boldsymbol{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix},\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}. \tag{10}$$

量子旋转门$\boldsymbol{R}_k(\theta_k,\phi_k)$和受控旋转门$\mathbf{CR}_k(\theta_k,\phi_k)$的定义如下:

$$\boldsymbol{R}_k(\theta_k,\phi_k)=\begin{bmatrix}\cos\dfrac{\theta_k}{2}&-\sin\dfrac{\theta_k}{2}\\ \mathrm{e}^{i\phi_k}\sin\dfrac{\theta_k}{2}&\mathrm{e}^{i\phi_k}\cos\dfrac{\theta_k}{2}\end{bmatrix}, \tag{11}$$

$$\mathbf{CR}_k(\theta_k,\phi_k)=\Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\langle j|\Big)\otimes\boldsymbol{I}+|k\rangle\langle k|\otimes\boldsymbol{R}_k(\theta_k,\phi_k). \tag{12}$$

首先制备量子比特初态$|0\rangle^{\otimes2n+1}$,在该初态上执行$\boldsymbol{H}^{\otimes2n}\otimes\boldsymbol{I}$可得中间态$|H\rangle$,即

$$|H\rangle=(\boldsymbol{H}^{\otimes2n}\otimes\boldsymbol{I})|0\rangle^{\otimes2n+1}=\frac{1}{2^n}\Big(\sum_{k=0}^{2^{2n}-1}|k\rangle\Big)\otimes|0\rangle. \tag{13}$$

在$|H\rangle$上执行$\mathbf{CR}_k(\theta_k,\phi_k)$,可得

$$\mathbf{CR}_k(\theta_k,\phi_k)|H\rangle=\frac{1}{2^n}\Big[\Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\Big)\otimes|0\rangle+|k\rangle\otimes\Big(\cos\frac{\theta_k}{2}|0\rangle+\mathrm{e}^{i\phi_k}\sin\frac{\theta_k}{2}|1\rangle\Big)\Big]. \tag{14}$$

由式(14)可知,为了获得式(5)所示的$|I(\theta,\phi)\rangle$,只需在$|H\rangle$上连续执行$\mathbf{CR}_k(\theta_k,\phi_k)(k=0,1,\cdots,2^{2n}-1)$即可,具体如下式所示:

$$|I(\theta,\phi)\rangle=\Big(\prod_{k=0}^{2^{2n}-1}\mathbf{CR}_k(\theta_k,\phi_k)\Big)|H\rangle. \tag{15}$$

对于一幅$2^n\times2^n$的彩色图像,具体实现FRQCI描述的量子线路如图1所示. 由于FRQCI描述采用的量子比特数与FRQI相同,仅就彩色图像的量子描述而言,它所使用的量子门数与FRQI相同,即两者的计算复杂度是相同的.

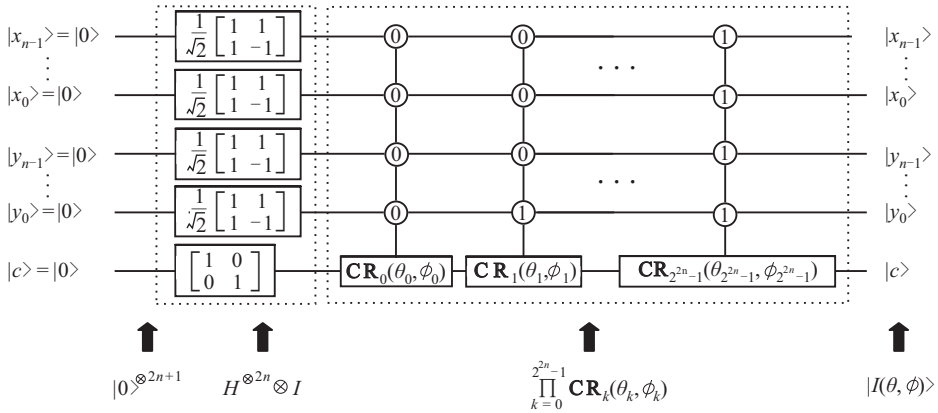


图 1　实现FRQCI描述的量子线路

3　量子彩色图像的几种处理方法

本节基于提出的FRQCI,给出量子彩色图像的几种处理方法:只改变GRB一种基色的灰度值;两基色灰度值互换;图像的上下翻转、左右翻转、上下置换、左右置换.

3.1　只改变一种基色的灰度值

对于一幅$2^n\times 2^n$的彩色图像,令第k个像素的三基色灰度值分别为c_k^{R}、c_k^{G}、c_k^{B},根据FRQCI描述,该图像可描述为式(5). 令改变后的三基色灰度值分别为$\hat{c}_k^{\mathrm{R}}$、$\hat{c}_k^{\mathrm{G}}$、$\hat{c}_k^{\mathrm{B}}$,则三基色灰度值的变化量对应的相位变化量分别为

$$\Delta\theta_k^{\mathrm{R}}=(\hat{c}_k^{\mathrm{R}}-c_k^{\mathrm{R}})\times 2^{16}\pi/(2^{24}-1), \tag{16}$$

$$\Delta\theta_k^{\mathrm{G}}=(\hat{c}_k^{\mathrm{G}}-c_k^{\mathrm{G}})\times 2^{8}\pi/(2^{24}-1), \tag{17}$$

$$\Delta\theta_k^{\mathrm{B}}=(\hat{c}_k^{\mathrm{B}}-c_k^{\mathrm{B}})\times \pi/(2^{24}-1). \tag{18}$$

三基色灰度值的具体改变可以通过量子比特的绕轴旋转实现. 由于在FRQCI中,只有相位θ_k携带像素灰度值信息,实施旋转时可使相位ϕ_k保持不变. 显然,使$|c_k\rangle$向着Bloch球面上的点$(0,0,-1)$旋转$\Delta\theta_k$即可达到此目的.

令$|c_k\rangle$的Bloch坐标为(x_k,y_k,z_k),为使$|c_k\rangle$向着Bloch球面上的点$(0,0,-1)$旋转,旋转轴应为

$$\boldsymbol{R}_k=\frac{(x_k,y_k,z_k)\times(0,0,-1)}{||(x_k,y_k,z_k)\times(0,0,-1)||}=\frac{(-y_k,x_k,0)}{x_k^2+y_k^2}, \tag{19}$$

旋转矩阵为

$$\boldsymbol{M}_k^{\Theta}=\cos\frac{\Delta\theta_k^{\Theta}}{2}\boldsymbol{I}-i\sin\frac{\Delta\theta_k^{\Theta}}{2}(\boldsymbol{R}_k\times\boldsymbol{\sigma}), \tag{20}$$

其中Θ为R,G,B三者之一.

定义受控旋转门

$$\mathbf{CM}_k^{\Theta}=\Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\langle j|\Big)\otimes\boldsymbol{I}+|k\rangle\langle k|\otimes\boldsymbol{M}_k^{\Theta}, \tag{21}$$

旋转操作可表述为

$$|I(\theta,\phi)^{\Theta}\rangle=\Big(\prod_{k=0}^{2^{2n}-1}\mathbf{CM}_k^{\Theta}\Big)|I(\theta,\phi)\rangle. \tag{22}$$

至此,完成了只改变一种基色灰度值的量子图像处理操作.

3.2　两种基色灰度值互换

任意两种基色灰度值的互换也采用量子比特绕轴旋转的方法实现. 令第k个像素的三基色灰度值分别为c_k^{R}、c_k^{G}、c_k^{B},则R、G互换,G、B互换,R、B互换后,对应于$|c_k\rangle$相位θ_k的旋转角度分别为

$$\Delta\theta_k^{\mathrm{RG}}=\frac{((c_k^{\mathrm{G}}-c_k^{\mathrm{R}})\times 2^{16}+(c_k^{\mathrm{R}}-c_k^{\mathrm{G}})\times 2^{8})\pi}{2^{24}-1}, \tag{23}$$

$$\Delta\theta_k^{\mathrm{GB}}=\frac{((c_k^{\mathrm{B}}-c_k^{\mathrm{G}})\times 2^{8}+(c_k^{\mathrm{G}}-c_k^{\mathrm{B}}))\pi}{2^{24}-1}, \tag{24}$$

$$\Delta\theta_k^{\mathrm{RB}}=\frac{((c_k^{\mathrm{B}}-c_k^{\mathrm{R}})\times 2^{16}+(c_k^{\mathrm{R}}-c_k^{\mathrm{B}}))\pi}{2^{24}-1}. \tag{25}$$

互换操作的具体实施与上节类似,只需要在式(20) ~ (22)中将$\Delta\theta_k^{\Theta}$替换为$\Delta\theta_k^{\mathrm{RG}}$,$\Delta\theta_k^{\mathrm{GB}}$,$\Delta\theta_k^{\mathrm{RB}}$中的一个即可.

3.3　图像的翻转和置换

关于图像的翻转和置换,同样可以采用量子比特的绕轴旋转实现. 令第i行第j个像素的量子比特相位为$\theta_{(i-1)2^n+j-1}$.

上下翻转之后的相位为$\theta_{(2^n-i)2^n+j-1}$,对应的旋转角度为$\Delta\theta_k^{\mathrm{UD1}}=\theta_{(2^n-i)2^n+j-1}-\theta_{(i-1)2^n+j-1}$.

左右翻转之后的相位为$\theta_{(i-1)2^n+2^n-j}$,对应的旋转角度为$\Delta\theta_k^{\mathrm{LR1}}=\theta_{(i-1)2^n+2^n-j}-\theta_{(i-1)2^n+j-1}$.

关于上下置换,如果$i\leqslant 2^{n-1}$,则对应的旋转角度为$\Delta\theta_k^{\mathrm{UD2}}=\theta_{(2^{n-1}+i-1)2^n+j-1}-\theta_{(i-1)2^n+j-1}$,否则对应的旋转角度为$\Delta\theta_k^{\mathrm{UD2}}=\theta_{(i-2^{n-1}-1)2^n+j-1}-\theta_{(i-1)2^n+j-1}$.

关于左右置换,如果$j\leqslant 2^{n-1}$,则对应的旋转角度为$\Delta\theta_k^{\mathrm{LR2}}=\theta_{(i-1)2^n+2^{n-1}+j-1}-\theta_{(i-1)2^n+j-1}$,否

则对应的旋转角度为$\Delta\theta_k^{\mathrm{LR2}} = \theta_{(i-1)2^n+j-2^{n-1}-1} - \theta_{(i-1)2^n+j-1}$.

以上4种操作的具体实现只需在式(20)～(22)中将$\Delta\theta_k^{\Theta}$分别替换为$\Delta\theta_k^{\mathrm{UD1}}$、$\Delta\theta_k^{\mathrm{LR1}}$、$\Delta\theta_k^{\mathrm{UD2}}$、$\Delta\theta_k^{\mathrm{LR2}}$即可,具体的量子线路如图2所示.

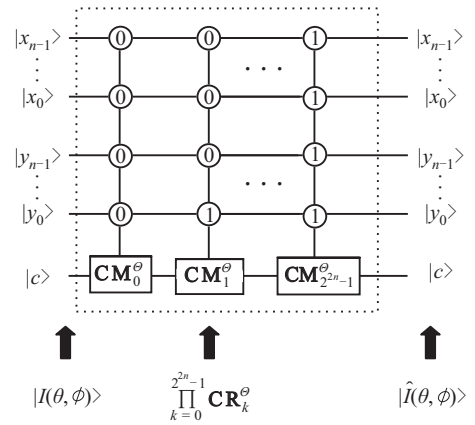


图 2 实现4种基本操作的量子线路

关于图2中量子线路的复杂性,该线路共使用2^{2n}个$2n-$受控旋转门,根据文献[18]可知,每个$k-$受控门能分解为$(4k-8)$个$2-$受控门,即$k-$受控门的计算复杂度不超过$O(k)$. 因此,就图2量子线路而言,其复杂度不超过$O(n2^{2n+1})$.

4 量子水印图像的嵌入和抽取

本节提出一种基于FRQCI的水印嵌入和抽取方法. 该方法的优点是:可使水印图像的幅度最大化到等于载体图像的幅度;由于水印图像和载体图像分别存储在不同的相位,水印图像的嵌入对载体图像不会造成任何影响;采用的嵌入方法可使水印图像具有很高的安全性.

4.1 水印图像的嵌入

水印嵌入的基本思路是:首先,将水印图像的幅度调整为与载体图像相同,具体方法是先将两图像重叠并使左上角对齐,再将水印图像的多余像素删除,不足像素的RGB均采用$[0,255]$的随机灰度值补足,利用FRQCI方案,将水印图像量子化,其中RGB灰度值信息存储在θ_k中;然后,对水印图像进行时域和频域加密;最后,将载体图像量子化,并将RGB灰度值信息存储在ϕ_k中. 其中两次加密均采用$|c_k\rangle$绕着随机选择的旋转轴旋转实现.

1) $|I(\theta,\phi)\rangle$的时域加密.

根据量子比特的球面描述,任何量子比特都与Bloch球面上的一点对应. 令$|c_k\rangle$的Bloch球面坐标为$(\hat{x}_k,\hat{y}_k,\hat{z}_k)$,根据量子计算原理,该坐标可以通过泡利矩阵按下式获得:

$$\begin{cases}\hat{x}_k = \langle c_k|\boldsymbol{\sigma}_x|c_k\rangle = \Big\langle c_k\Big|\Big(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\Big)\Big|c_k\Big\rangle,\\ \hat{y}_k = \langle c_k|\boldsymbol{\sigma}_y|c_k\rangle = \Big\langle c_k\Big|\Big(\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\Big)\Big|c_k\Big\rangle,\\ \hat{z}_k = \langle c_k|\boldsymbol{\sigma}_z|c_k\rangle = \Big\langle c_k\Big|\Big(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\Big)\Big|c_k\Big\rangle.\end{cases} \tag{26}$$

令x_k,y_k,z_k为在区间$(-1,1)$内均匀分布的随机数,$|c_k\rangle$的旋转轴可按下式计算:

$$\mathbf{sn}_k = [\hat{x}_k,\hat{y}_k,\hat{z}_k]\times[x_k,y_k,z_k] = [\hat{y}_kz_k-\hat{z}_ky_k,\hat{z}_kx_k-\hat{x}_kz_k,\hat{x}_ky_k-\hat{y}_kx_k]. \tag{27}$$

令δ_k表示在区间$(0,2\pi)$内均匀分布的随机数,则$|c_k\rangle$的旋转矩阵和相应的受控矩阵分别为

$$\mathbf{SR}_k(\delta_k,\mathbf{sn}_k) = \cos\frac{\delta_k}{2}\boldsymbol{I} - i\sin\frac{\delta_k}{2}\Big(\frac{\mathbf{sn}_k\times\boldsymbol{\sigma}}{\|\,\mathbf{sn}_k\,\|}\Big), \tag{28}$$

$$\mathbf{CSR}_k(\delta_k,\mathbf{sn}_k) = \Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\langle j|\Big)\otimes\boldsymbol{I} + |k\rangle\langle k|\otimes\mathbf{SR}_k(\delta_k,\mathbf{sn}_k). \tag{29}$$

通过对$|I(\theta,\phi)\rangle$连续执行$\mathbf{CSR}_k(\delta_k,\mathbf{sn}_k)$即可完成时域加密,如下式所示:

$$|I_1(\theta,\phi)\rangle = \Big(\prod_{k=0}^{2^{2n}-1}\mathbf{CSR}_k(\delta_k,\mathbf{sn}_k)\Big)|I(\theta,\phi)\rangle, \tag{30}$$

其中秘钥为像素灰度值比特$|c_k\rangle$的旋转轴和旋转角度.

2) $|I_1(\theta,\phi)\rangle$的量子傅里叶变换.

量子傅里叶变换是一种定义在标准正交基$|0\rangle$,$|1\rangle,\cdots,|2^{2n+1}-1\rangle$上的线性算子. 该算子在基态上的作用效果可表述为

$$\mathrm{QFT}(|k\rangle) = \frac{1}{\sqrt{2^{2n+1}}}\sum_{j=0}^{2^{2n+1}-1}\mathrm{e}^{2\pi ijk/N}|j\rangle. \tag{31}$$

在任意迭代态上的作用效果为

$$\mathrm{QFT}\Big(\sum_{k=0}^{2^{2n+1}-1}x_k|k\rangle\Big) = \sum_{j=0}^{2^{2n+1}-1}y_j|j\rangle, \tag{32}$$

其中$y_j = \dfrac{1}{\sqrt{2^{2n+1}}}\displaystyle\sum_{k=0}^{2^{2n+1}-1}x_k\mathrm{e}^{2\pi ijk/N}$.

$|I_1(\theta,\phi)\rangle$的量子傅里叶变换可以简单地表述为$|I_2(\theta,\phi)\rangle = \mathrm{QFT}(|I_1(\theta,\rangle)$.

3) $|I_2(\theta,\phi)\rangle$的频域加密.

与时域加密类似,令$|c_k\rangle$的Bloch球面坐标为$(\tilde{x}_k,\tilde{y}_k,\tilde{z}_k)$,$u_k,v_k,w_k$为在区间$(-1,1)$内均匀分布的随机数,$|c_k\rangle$的旋转轴按下式计算:

$$\mathbf{fn}_k=[\tilde{x}_k,\tilde{y}_k,\tilde{z}_k]\times[u_k,v_k,w_k]=$$
$$[\tilde{y}_kw_k-\tilde{z}_kv_k,\tilde{z}_ku_k-\tilde{x}_kw_k,\tilde{x}_kv_k-\tilde{y}_ku_k]. \quad (33)$$

令ξ_k表示在区间$(0,2\pi)$内均匀分布的随机数,则$|c_k\rangle$的旋转矩阵和相应的受控矩阵分别为

$$\mathbf{FR}_k(\xi_k,\mathbf{fn}_k)=\cos\frac{\xi_k}{2}\boldsymbol{I}-i\sin\frac{\xi_k}{2}\Big(\frac{\mathbf{fn}_k\times\boldsymbol{\sigma}}{\parallel\mathbf{fn}_k\parallel}\Big), \quad (34)$$

$$\mathbf{CFR}_k(\xi_k,\mathbf{fn}_k)=$$
$$\Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\langle j|\Big)\otimes\boldsymbol{I}+|k\rangle\langle k|\otimes\mathbf{FR}_k(\xi_k,\ \mathbf{fn}_k). \quad (35)$$

通过对$|I_2(\theta,\phi)\rangle$连续执行$\mathbf{CFR}_k(\xi_k,\mathbf{fn}_k)$即可完成频域加密,如下式所示:

$$|I_3(\theta,\phi)\rangle=\Big(\prod_{k=0}^{2^{2n}-1}\mathbf{CFR}_k(\xi_k,\mathbf{fn}_k)\Big)|I_2(\theta,\phi)\rangle. \quad (36)$$

其中秘钥为像素灰度值比特$|c_k\rangle$的旋转轴和旋转角度.

4) $|I_3(\theta,\phi)\rangle$的量子傅里叶反变换.

量子傅里叶反变换也是一种定义在标准正交基$|0\rangle,|1\rangle,\cdots,|2^{2n+1}-1\rangle$上的线性算子,该算子在任意叠加态上的作用效果为

$$\mathrm{IQFT}\Big(\sum_{j=0}^{2^{2n+1}-1}x_j|j\rangle\Big)=$$
$$\frac{1}{\sqrt{2^{2n+1}}}\sum_{k=0}^{2^{2n+1}-1}\Big(\sum_{j=0}^{2^{2n+1}-1}x_j\mathrm{e}^{-2\pi ijk/N}|k\rangle\Big). \quad (37)$$

由上式可知,$|I_3(\theta,\phi)\rangle$的量子傅里叶反变换可简单表述为$|I_4(\theta,\phi)\rangle=\mathrm{IQFT}(|I_3(\theta,\phi)\rangle)$.

5)载体图像量子化.

由于$|c_k\rangle$的相位θ_k承载着水印图像信息,为了使载体图像与水印图形相互独立,载体图像的量子化过程采用使$|c_k\rangle$绕着Z轴旋转(这种旋转可以使θ_k保持不变)的方法,并将载体图像的像素信息存储到ϕ_k中. 令第k个像素的三基色灰度值分别为$c_k^{\mathrm{R}},c_k^{\mathrm{G}},c_k^{\mathrm{B}}$,则有

$$\phi_k=\frac{(c_k^{\mathrm{R}}\times2^{16}+c_k^{\mathrm{G}}\times2^8+c_k^{\mathrm{B}})2\pi}{2^{24}-1}. \quad (38)$$

令水印图像中$|c_k\rangle$的当前相位为$\hat{\phi}_k$,只需使$|c_k\rangle$绕着Z轴逆时针旋转$\Delta\phi_k=\phi_k-\hat{\phi}_k$弧度即可. 旋转矩阵和受控矩阵分别为

$$\boldsymbol{R}_{zk}(\Delta\phi_k)=\begin{bmatrix}1&0\\0&\mathrm{e}^{i\Delta\phi_k}\end{bmatrix}, \quad (39)$$

$$\mathbf{CR}_{zk}(\Delta\phi_k)=$$
$$\Big(\sum_{j=0,j\neq k}^{2^{2n}-1}|j\rangle\langle j|\Big)\otimes\boldsymbol{I}+|k\rangle\langle k|\otimes\boldsymbol{R}_{\boldsymbol{z}k}(\Delta\phi_k). \quad (40)$$

通过对$|I_4(\theta,\phi)\rangle$连续执行$\mathbf{CR}_{\boldsymbol{z}k}(\Delta\phi_k)$即可完成载体图像的量子化载入,如下式所示:

$$|I_5(\theta,\phi)\rangle=\Big(\prod_{k=0}^{2^{2n}-1}\mathbf{CR}_{zk}(\Delta\phi_k)\Big)|I_4(\theta,\phi)\rangle. \quad (41)$$

至此,完成了量子水印图像的嵌入过程. 由嵌入过程可知,嵌入算法的密钥可描述为如下两式:

$$\mathrm{Key}_s=[\mathbf{sn}_0,\delta_0,\mathbf{sn}_1,\delta_1,\cdots,\mathbf{sn}_{2^{2n}-1},\delta_{2^{2n}-1}], \quad (42)$$

$$\mathrm{Key}_f=[\mathbf{fn}_0,\xi_0,\mathbf{fn}_1,\xi_1,\cdots,\mathbf{fn}_{2^{2n}-1},\xi_{2^{2n}-1}]. \quad (43)$$

其中: Key_s包含4×2^{2n}个随机数$x_k,y_k,z_k,\delta_k(k=0,1,\cdots,2^{2n}-1)$, Key_f也包含4×2^{2n}个随机数$u_k,v_k,w_k,\xi_k(k=0,1,\cdots,2^{2n}-1)$. 这些随机数或者在$(-1,1)$上或者在$(0,2\pi)$上均匀分布,这表明所提出的算法有足够大的密钥空间,足以抵御蛮力攻击.

4.2　水印图像的抽取

水印抽取的基本思路是: 去除载体图像,执行量子傅里叶变换,频域解密及量子傅里叶反变换,执行时域解密,即可抽取出嵌入的水印图像. 由于量子计算具有可逆性,以上各步骤中的算子只需采用嵌入过程相应算子的共轭转置即可.

关于实现彩色图像水印的量子线路,嵌入和抽取的量子线路可参考图1,加密和解密的量子线路可参考图2,只需使旋转角度取反即可,量子傅里叶变换和反变换的量子线路可参见文献[19].

对比本文水印方案和文献[15]中的方案可知,两种方案都使用了量子傅里叶变换,本文方案中的时域加密,相当于文献[15]方案中的置乱,但本文增加了频域加密,因此本文方案的复杂度略高于文献[15]中的方案. 但增加了频域加密后有助于提高水印图像的抗攻击能力,本文方案正是以牺牲线路复杂度为代价换取水印图像安全性的提高的,这与无免费午餐定理的结论是一致的. 另外,值得指出的是,本文方案是针对将来的量子计算机设计的,在经典计算机上执行仅是为了检验方案的执行效果,由于本文方案在经典计算机上无法实现量子并行性,对于经典图像处理算法而言,尽管执行效果相同,但执行效率相当低.

5　量子图像的测量

在所有的量子计算中,最后一步均为测量. 只有对量子图像测量才能真正显示出量子图像的内容.

5.1　基于θ_k的量子图像测量

为了实现量子图像的测量,首先按酉矩阵谱分解的形式定义测量算子$\boldsymbol{M}$,即

$$\boldsymbol{M}=\sum_{k=0}^{2^{2n}-1}(m_0^{(k)}\boldsymbol{p}_0^{(k)}+m_1^{(k)}\boldsymbol{p}_1^{(k)}), \quad (44)$$

其中$\boldsymbol{p}_0^{(k)}=|k\rangle|0\rangle\langle k|\langle 0|$和$\boldsymbol{p}_1^{(k)}=|k\rangle|1\rangle\langle k|\langle 1|$是与$\boldsymbol{M}$的本征值$m_0^{(k)}$和$m_1^{(k)}$对应的一组正交投影矩阵.

对于式(5)描述的量子彩色图像$|I(\theta,\phi)\rangle$,应用测量算子$\boldsymbol{M}$获得$m_0^{(k)}$和$m_1^{(k)}$的概率可分别计算如下:

$$\begin{cases}P(m_0^{(k)})=\langle I(\theta,\phi)|\boldsymbol{p}_0^{(k)}|I(\theta,\phi)\rangle=\dfrac{1}{2^{2n}}\cos^2\dfrac{\theta_k}{2},\\ P(m_1^{(k)})=\\ \langle I(\theta,\phi)|\boldsymbol{p}_1^{(k)}|I(\theta,\phi)\rangle=\dfrac{1}{2^{2n}}|\mathrm{e}^{i\phi_k}|^2\sin^2\dfrac{\theta_k}{2}.\end{cases}\tag{45}$$

根据上式可以导出如下θ_k的计算式:

$$\theta_k=2\arcsin(\sqrt{2^{2n}P(m_1^{(k)})}.\tag{46}$$

根据式(7),第k个像素的RBG灰度值可分别计算如下:

$$c_{\mathrm{R}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\theta_k}{\pi\times2^8\times2^8}\right\rfloor,\tag{47}$$

$$c_{\mathrm{G}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\theta_k-(c_R\times2^8\times2^8)\times\pi}{\pi\times2^8}\right\rfloor,\tag{48}$$

$$c_{\mathrm{B}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\theta_k}{\pi}-c_{\mathrm{R}}\times2^8\times2^8-c_{\mathrm{G}}\times2^8\right\rfloor.\tag{49}$$

5.2 基于ϕ_k的量子图像测量

令$|c_k\rangle=\cos\dfrac{\theta_k}{2}|0\rangle+\mathrm{e}^{i\phi_k}\sin\dfrac{\theta_k}{2}|1\rangle$,在$|c_k\rangle$上应用算子$\boldsymbol{U}_1=\dfrac{1}{\sqrt{2}}\begin{bmatrix}1&1\\-1&1\end{bmatrix}$可得

$$|c_k^{(1)}\rangle=U_1|c_k\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}\cos\dfrac{\theta_k}{2}+\mathrm{e}^{i\phi_k}\sin\dfrac{\theta_k}{2}\\-\cos\dfrac{\theta_k}{2}+\mathrm{e}^{i\phi_k}\sin\dfrac{\theta_k}{2}\end{bmatrix}.\tag{50}$$

在计算基矢上的投影测量得到输出为$|0\rangle$和$|1\rangle$的概率分别为

$$P_0^{(1)}=|\langle 0|c_k^{(1)}\rangle|^2=\frac{1}{2}(1+\cos\phi_k\sin\theta_k),\tag{51}$$

$$P_1^{(1)}=|\langle 1|c_k^{(1)}\rangle|^2=\frac{1}{2}(1-\cos\phi_k\sin\theta_k).\tag{52}$$

因此有

$$P_0^{(1)}-P_1^{(1)}=\cos\phi_k\sin\theta_k=x_k.\tag{53}$$

同样,在$|c_k\rangle$上应用算子$\boldsymbol{U}_2=\dfrac{1}{\sqrt{2}}\begin{bmatrix}1&-i\\-i&1\end{bmatrix}$可得

$$|c_k^{(2)}\rangle=U_2|c_k\rangle=\frac{1}{\sqrt{2}}\begin{bmatrix}\cos\dfrac{\theta_k}{2}+\mathrm{e}^{i\left(\phi_k-\frac{\pi}{2}\right)}\sin\dfrac{\theta_k}{2}\\ \mathrm{e}^{i\left(-\frac{\pi}{2}\right)}\cos\dfrac{\theta_k}{2}+\mathrm{e}^{i\phi_k}\sin\dfrac{\theta_k}{2}\end{bmatrix}.\tag{54}$$

在计算基矢上的投影测量得到输出为$|0\rangle$和$|1\rangle$的概率分别为

$$P_0^{(2)}=|\langle 0|c_k^{(2)}\rangle|^2=\frac{1}{2}(1+\sin\phi_k\sin\theta_k),\tag{55}$$

$$P_1^{(2)}=|\langle 1|c_k^{(2)}\rangle|^2=\frac{1}{2}(1-\sin\phi_k\sin\theta_k).\tag{56}$$

因此有

$$P_0^{(2)}-P_1^{(2)}=\sin\phi_k\sin\theta_k=y_k.\tag{57}$$

由以上推导可知,制备N个相同的量子态$|c_k^{(1)}\rangle$,实施计算基上的测量,令得到$|0\rangle$和$|1\rangle$的数目分别为$N_0^{(1)}$和$N_1^{(1)}$,则$x_k\approx\dfrac{N_0^{(1)}-N_1^{(1)}}{N}$;同理,通过制备$N$个相同的量子态$|c_k^{(2)}\rangle$,令得到$|0\rangle$和$|1\rangle$的数目分别为$N_0^{(2)}$和$N_1^{(2)}$,则$y_k\approx\dfrac{N_0^{(2)}-N_1^{(2)}}{N}$.

由式(53)和(57)可知,$\phi_k=\arctan\left(\dfrac{y_k}{x_k}\right)$,考虑到此时$\phi_k\in\left[-\dfrac{\pi}{2},\dfrac{\pi}{2}\right]$,需要作如下变换:

$$\phi_k=\begin{cases}\arctan\left(\dfrac{y_k}{x_k}\right),\ x_k\geqslant 0,\ y_k\geqslant 0;\\ 2\pi+\arctan\left(\dfrac{y_k}{x_k}\right),\ x_k\geqslant 0,\ y_k<0;\\ \pi+\arctan\left(\dfrac{y_k}{x_k}\right),\ x_k<0.\end{cases}\tag{58}$$

再由式(38)可得

$$c_{\mathrm{R}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\phi_k}{2\pi\times2^8\times2^8}\right\rfloor,\tag{59}$$

$$c_{\mathrm{G}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\phi_k-(c_R\times2^8\times2^8)\times\pi}{2\pi\times2^8}\right\rfloor,\tag{60}$$

$$c_{\mathrm{B}}^k=\left\lfloor\frac{(2^8\times2^8\times2^8-1)\phi_k}{2\pi}-c_{\mathrm{R}}\times2^8\times2^8-c_{\mathrm{G}}\times2^8\right\rfloor,\tag{61}$$

其中$\lfloor\cdot\rfloor$为向下取整算符.

图像的存储与检索是不可分割的两个部分,量子图像的测量本质上就是量子图像的检索. 对于存储线路,FRQCI所用的比特数与FRQI相同,然而FRQCI存储的是彩色图像,因此提高了存储效率,对于检索(即测量),FRQCI也是基于量子叠加态坍缩到基态的概率进行的,本质上与FRQI是没有区别的,但本方案检索出的是彩色图像,因此检索效率也比FRQI有所提高.

6 经典计算机上的仿真

由于目前还没有量子计算机,本文提出的所有算法都在普通计算机上采用Matlab的向量、矩阵操作进行仿真. 由于采用经典计算方式不能仿真量子计算的并行性,但能仿真量子算法的执行步骤及执行量子测量后的视觉效果,故能够验证算法的有效性. 实验环境为配置Window 7系统,主频3.2 GHz,内存4.0 GB,Matlab(R2009a)软件的微机.

6.1　像素值及像素位置的改变

采用512 × 512的Lena图像进行仿真,载体图像如图3(a)所示,只改变R、G、B,以及R、G互换、G、B互换、R、B互换的结果如图3(b)～图3(g)所示. 上下左右翻转,上下左右置换的结果如图3(h)～图3(k)所示. 其中图3(b)～图3(d)中改变后的R、G、B均为[0, 255]内的随机整数.

(a) 原始图像　(b) 只改 R　(c) 只改 G　(d) 只改 B　(e) R、G 互换　(f) G、B 互换　(g) R、B 互换　(h) 上下翻转　(i) 左右翻转　(j) 上下置换　(k) 左右置换

图 3　像素值及像素位置的改变效果

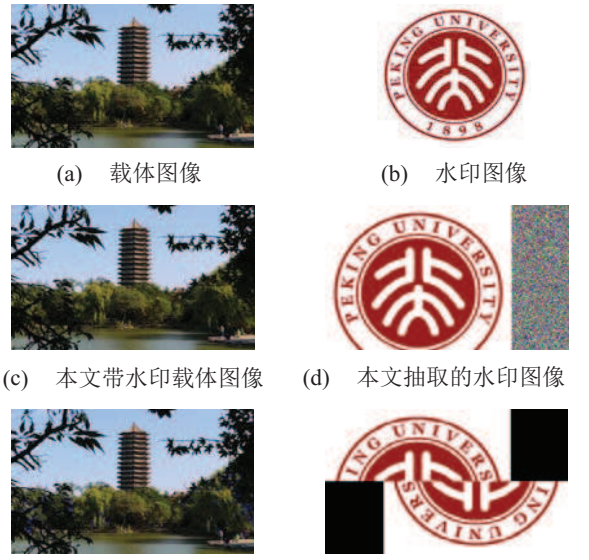
6.2　量子水印的嵌入和抽取

采用北大和清华的校园图片作为载体图像,采用两校的校徽作为水印图像,其中北大校园图片幅度为352 × 220,校徽图片幅度为268 × 268,清华校园图片幅度为770 × 460,校徽图片幅度为1 600 × 505.

为了验证本文水印方案的优越性,将与文献[15]中的水印策略对比. 文献[15]中策略仅适用于单色图像,水印的嵌入和抽取违背量子力学原理,且水印大小仅为载体图像的一半. 本文在仿真文献[15]中的策略时,采用FRQCI描述彩色图像,采用量子比特旋转的方法实现水印图像的嵌入和抽取. 实验发现,文献[15]中方案的嵌入比例因子α的取值对嵌入效果十分敏感,当$\alpha > 10^{-7}$时,嵌入效果明显失真,因此,本文取$\alpha = 3.0^{-8}$. 两校载体图像、水印图像、带水印载体图像、抽取出的水印图像如图4和图5所示.

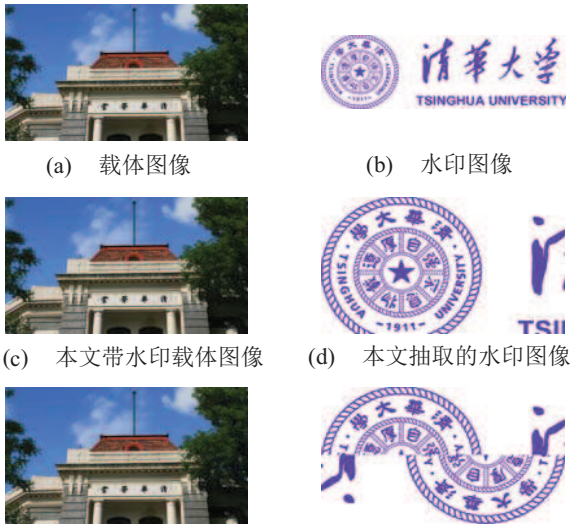
为了定量描述水印图像的嵌入对载体图像的影响,首先给出两图像之间的均方误差及带噪声图像峰值信噪比的定义.

令I'为嵌入水印后的载体图像,I为最初的载体图像,m, n分别为图像中的行列像素数. I'与I之间RGB灰度值的均方误差定义为



(a) 载体图像　(b) 水印图像　(c) 本文带水印载体图像　(d) 本文抽取的水印图像　(e) 文献[15]带水印载体图像　(f) 文献[15]抽取的水印图像

图 4　北大校园水印效果



(a) 载体图像　(b) 水印图像　(c) 本文带水印载体图像　(d) 本文抽取的水印图像　(e) 文献[15]带水印载体图像　(f) 文献[15]抽取的水印图像

图 5　清华校园水印效果

$$\mathrm{MSE_R} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I'(i,j,1) - I(i,j,1)]^2,$$

$$\mathrm{MSE_G} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I'(i,j,2) - I(i,j,2)]^2,$$

$$\mathrm{MSE_B} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I'(i,j,3) - I(i,j,3)]^2.$$

嵌入水印后载体图像的峰值信噪比定义为

$$\mathrm{PSNR_R} = 20\log_{10}\frac{255}{\sqrt{\mathrm{MSE_R}}},$$

$$\mathrm{PSNR_G} = 20\log_{10}\frac{255}{\sqrt{\mathrm{MSE_G}}},$$

$$\mathrm{PSNR_B} = 20\log_{10}\frac{255}{\sqrt{\mathrm{MSE_B}}}.$$

两种方案带水印图像的峰值信噪比对比如表1所示.

表1 两种方案带水印图像的三基色峰值信噪比

图像	方案	$PSNR_R$	$PSNR_G$	$PSNR_B$
北大校园	本文	∞	∞	∞
	文献[15]	90.9999	42.8585	20.8457
清华校园	本文	∞	∞	∞
	文献[15]	89.1517	41.0182	24.8168

如前所述,在嵌入水印之前,对水印图像进行幅度调整. 对于本文方案,水印图像可以最大化到与载体图像相同,由于北大校徽的高度大于校园图片的高度,而宽度小于校园图片的宽度,抽取出的水印图像下部具有截断痕迹,而右侧具有随机添加的像素信息,清华校徽图像也应有类似的情况. 对于文献[15]中的方案,水印图像仅能最大化到载体图像的一半. 图4和图5给出的仿真结果验证了上述情况. 另外,对于本文方案,由于载体图像和水印图像分别存储在不同的相位,水印的嵌入对于载体图像的可视化效果没有任何影响,而对于文献[15]中的方案,水印的嵌入必然影响载体图像的可视化效果,而且只有当$\alpha < 10^{-7}$时才能使带水印的载体图像具有较高的峰值信噪比. 表1给出的仿真结果验证了上述情况.

7 结 论

本文提出了一种彩色图像的量子描述新方法. 对于$M \times N$的彩色图像,只需$\log_2(MN)+1$个量子比特即可同时存储像素的位置和颜色信息. 应用所提出的新方法设计了几种基本的量子图像处理操作,提出了一种新的量子水印策略. 该策略将水印图像和载体图像分别存储在量子比特的两个相位参数中,同时采用量子比特绕轴旋转的方法对水印图像进行两次加密处理,有效提高了水印图像的安全性. 经典计算机上的仿真结果验证了所提出方法的有效性.

参考文献(References)

[1] 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.

[2] Su D, He W, Wu J W, et al. The storage scheme of eight particle quantum states to color iamge[J]. J of Yunnan Normal University: Natural Science Edition, 2014, 34(3): 56-60.

[3] Li Haisheng, Zhu Qingxin, Zhou Rigui, et al. Multidimensional color image storage, retrieval, and compression based on quantum amplitudes and phases[J]. Information Sciences, 2014, 273(3): 212-232.

[4] Li Haisheng, Zhu Qingxin, Zhou Rigui, et al. Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state[J]. Quantum Information Processing, 2014, 13(4): 991-1011.

[5] Li H S. Key techniques research of quantum image processing[D]. Chengdu: School of Computer Science and Engineering, University of Electronic Science and Technology of China, 2014: 57-60.

[6] Le P Q, Iliyasu A M, Dong F, et al. Strategies for designing geometric transformations on quantum images[J]. Theory Computer Science, 2011, 412(15): 1406-1418.

[7] Le P Q, Iliyasu A M, Dong F, et al. Efficient color transformations on quantum images[J]. J of Advanced Computational Intelligence and Intelligent Informatics, 2011, 15(6): 698-706.

[8] Zhou Rigui, Sun Yajuan, Fan Ping. Quantum image Gray-code and bit-plane scrambling[J]. Quantum Information Processing, 2015, 14(5): 1717-1734.

[9] Jiang N. quantum image Process[M]. Beijing: Tsinghua University Press, 2016: 39-93.

[10] Iliyasu A, Le P, Dong F, et al. Watermarking and authentication of quantum images based on restricted geometric transformations[J]. Information Science, 2012, 186(1): 126-149.

[11] Iliyasu A, Le P, Yan F, et al. A two-tier scheme for greyscale quantum image watermarking and recovery[J]. Int J of Innovative Computing and Applications, 2013, 5(2): 85-101.

[12] Song X, Wang S, Niu X. Dynamic watermarking scheme for quantum images based on Hadamard transform[J]. Multimedia Systems, 2014, 20(4): 379-388.

[13] Song X, Wang S, Liu S, et al. A dynamic watermarking scheme for quantum images using quantum wavelet transform[J]. Quantum Information Processing, 2013, 12(2): 3689-3706.

[14] Zhang W, Gao F, Liu B, et al. A quantum watermark protocol[J]. Int J of Theory Physics, 2013, 52(2): 504-513.

[15] Zhang W, Gao F, Liu B, et al. A watermark strategy for quantum images based on quantum fourier transform[J]. Quantum Information Processing, 2013, 12(2): 793–803.

[16] Song X H. Research of key technologies of quantum image security[D]. Harbin: School of Computer Science and Technology, Harbin Institute of Techno-logy, 2015: 25-34.

[17] Giuliano B, Giulio C, Giuliano S. Principles of Quantum Computation and Information(Volume I: Basic Concepts)[M]. Singapore: World Scientific, 2004: 103-105.

[18] Yang G W, Song X Y, Hung W N, et al. Group theory based synthesis of binary reversible circuits[J]. Lecture Notes in Computer Science, 2006, 3959: 365-374.

[19] Michael A Nielsen, Isaac L Chuang. Quantum computation and quantum information[M]. Cambridge: Cambridge University Press, 2000: 217-221.

（责任编辑：闫 妍）