文章编号: 1001-0920 (2016) 08-1363-09 **DOI:** 10.13195/j.kzyjc.2015.0782

基于量子比特绕轴旋转的彩色图像加密方法

李盼池, 卢爱平

(东北石油大学 计算机与信息技术学院，黑龙江 大庆 163318)

摘 要: 提出一种基于量子计算的彩色图像加密方法. 首先, 将彩色图像转换为量子叠加态 $|\text{Image}\rangle$, 每个像素用 3 个量子比特 $|r\rangle, |g\rangle, |b\rangle$ 描述, 分别表示红绿蓝三基色; 然后, 对所有像素的 $|r\rangle, |g\rangle, |b\rangle$ 在 Bloch 球面上实施随机旋转, 对旋转后的 $|\text{Image}\rangle$ 实施量子傅里叶变换; 对所有像素的 $|r\rangle, |g\rangle, |b\rangle$ 实施随机旋转, 对旋转后的 $|\text{Image}\rangle$ 实施量子傅里叶反变换, 即可完成加密操作. 经典计算机上的仿真结果表明, 所提出的方法具有较好的安全性, 可在将来的量子计算机上执行.

关键词: 图像处理；加密算法；量子比特旋转；量子傅里叶变换

中图分类号: TP183 **文献标志码:** A

Color image encryption method based on qubits rotation about axis

LI Pan-chi, LU Ai-ping

(School of Computer and Information Technology, Northeast Petroleum University, Daqing 163318, China. Correspondent: LI Pan-chi, E-mail: lipanchi@vip.sina.com)

Abstract: A color image encryption method based on quantum computing is proposed. Firstly, the color image is encoded in quantum superposition $|\text{Image}\rangle$. Each pixel is described by three quantum bits $|r\rangle, |g\rangle, |b\rangle$ which represent the red, green and blue colors. And then, all qubits are randomly rotated on the Bloch sphere. The quantum fourier transform(QFT) is performed on the $|\text{Image}\rangle$. Once again, all qubits are randomly rotated on the Bloch sphere and the inverse QFT is performed on the $|\text{Image}\rangle$, and the encryption process is implemented. The simulation results on the classic computer show that the method has better security, and can be run on quantum computers in the future.

Keywords: image processing; encryption algorithm; qubits rotating; quantum fourier transform

0 引 言

随着多媒体网络的快速发展, 信息安全吸引了很多研究者的注意. 图像作为最重要的信息载体之一, 在多媒体通讯中已获得广泛应用. 为实现图像的安全传输, 人们提出了多种不同的加密方案[1-14]. 然而, 绝大多数传统的加密算法最初是针对文本加密提出的, 其加密过程过于复杂而不适合图像加密. 混沌系统具有对初值敏感、遍历性、容易实现等特点, 受这些特点的启发, 人们也研究了一些基于混沌系统的图像加密技术[1, 6-7, 11, 14], 但大多数混沌加密方法都存在弱点, 从而限制了这些方法的应用.

随着量子计算的发展, 经典的图像处理方法必将自然地扩展到量子计算领域. 利用量子态的相干、纠缠、叠加等特性, 一些量子算法 (如 Shor 的大数质因子分解算法[15]、Grover 的无序数据库搜索算法[16]、量子傅里叶变换[17]、量子小波变换[18])获得了超越任何经典算法的性能. 作为量子计算和图像处理的融合, 量子图像加密正在逐渐引起研究者的注意, 目前在这一方向的研究成果还相对较少. 尽管文献 [19] 提出了基于量子图像几何变换的图像加密算法, 但其加密操作不符合量子计算原理, 该方案在量子计算机上是不能实现的. 真正能在量子计算机上执行的量子图像加密算法是由北京工业大学的杨宇光教授首次提出的[20]. 该算法首次采用量子旋转门和量子傅里叶变换实现了对彩色图像加密. 根据量子计算的可逆性, 对密文图像实施加密的逆操作, 即可获得明文图像. 然而, 该方法中的量子比特只有一个相位参数, 且概率幅为实数, 而真实的量子系统量子比特有两个

收稿日期: 2015-06-18；**修回日期:** 2015-08-31.

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).

作者简介: 李盼池(1969−), 男, 教授, 博士生导师, 从事量子智能优化、量子神经网络等研究；卢爱平(1977−), 女, 博士生, 从事智能优化算法的研究.

相位参数, 且概率幅为复数. 鉴于此, 本文沿用文献[20]的思路, 提出一种改进的彩色图像加密方法. 该方法与文献[20]的区别是: 在编码和加密方面, 采用基于Bloch球面描述的量子比特实现图像编码, 采用量子比特绕着随机生成的旋转轴旋转的方法实现图像加密. 除此之外, 在实现方面, 采用单比特量子门和二比特受控门给出了实现加密和解密过程的量子线路. 经典计算机上的实验结果表明, 该方法具有较好的安全性.

1 相关工作概述

1.1 双随机相位编码方法

1995年, 文献[21]提出了一种适合于图像加密的双随机相位编码方法(DRPE), 该方法通过两次统计独立的随机相位扰动和两次傅里叶变换实施加密. 令明文图像为$f(x,y)$, 加密图像为$\varphi(x,y)$, 解密图像为$f'(x,y)$, 加密和解密过程可表述为

$$\varphi(x,y)=\mathrm{FT}^{-1}[\mathrm{FT}[f(x,y)\mathrm{e}^{j2\pi n(x,y)}]\mathrm{e}^{j2\pi b(\xi,\eta)}], \quad (1)$$

$$f'(x,y)=\mathrm{FT}^{-1}[\mathrm{FT}[\varphi(x,y)\mathrm{e}^{-j2\pi b(\xi,\eta)}]\mathrm{e}^{-j2\pi n(x,y)}]. \quad (2)$$

其中: $n(x,y)$和$b(\xi,\eta)$为两个统计独立且在(0,1)均匀分布的随机函数, FT和FT^{-1}分别为傅里叶变换和傅里叶逆变换.

DRPE方法的一个重要步骤是将图像转换为一个稳定的白噪声, 但人们已经发现DRPE的一些弱点, 且已提出一些相应的攻击策略[22-25].

1.2 基于量子傅里叶变换和DRPE的彩色图像加密算法

在彩色图像加密与量子计算的融合方面, 文献[20]做了开创性的工作. 其核心思想是: 首先, 将彩色图像每个像素三基色的灰度值用量子比特描述, 将整幅彩色图形转换成量子叠加态; 然后, 与DRPE类似, 在量子傅里叶变换前后采用量子旋转门对量子比特的相位实施随机扰动, 其中转角为在$(0,2\pi)$均匀分布的随机数. 实验结果表明, 该方法明显优于DRPE.

在这个方法中, 编码采用的是基于平面单位圆描述的量子比特, 只有一个相位参数. 加密采用的量子旋转门使量子比特绕着单位圆的圆心随机旋转, 也只改变量子比特的一个参数. 在真实的量子系统中, 量子比特是基于Bloch球面描述的, 具有两个相位参数, 量子比特在Bloch球面上的绕轴旋转可同时改变量子比特的这两个参数. 因此, 本文的目的是将文献[20]中的方法加以推广, 即采用具有两个相位参数的量子比特实现对彩色图像的编码, 采用量子比特在Bloch球面上的绕轴旋转实现对彩色图像的加密, 同时也将给出具体实现彩色图像的编码、加密、解密过程的量子线路设计方案.

2 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

$$|\boldsymbol{\varphi}\rangle=\cos\frac{\theta}{2}|0\rangle+e^{\mathrm{i}\phi}\sin\frac{\theta}{2}|1\rangle. \quad (3)$$

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3维Bloch球面上的一个点来描述, 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$x=\cos\phi\sin\theta$, $y=\sin\phi\sin\theta$, $z=\cos\theta$.

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球面上绕一个沿单位矢量$\boldsymbol{n}=[n_x,n_y,n_z]$的轴转动$\delta$弧度的旋转矩阵为

$$\boldsymbol{R}_{\boldsymbol{n}}(\delta)=\cos\frac{\delta}{2}\boldsymbol{I}-\mathrm{i}\sin\frac{\delta}{2}(\boldsymbol{n}\times\boldsymbol{\sigma}). \quad (4)$$

其中: $\boldsymbol{I}$为单位矩阵; $\boldsymbol{\sigma}=[\boldsymbol{\sigma}_x,\boldsymbol{\sigma}_y,\boldsymbol{\sigma}_z]$, $\boldsymbol{\sigma}_x,\boldsymbol{\sigma}_y,\boldsymbol{\sigma}_z$为按下式定义的泡利矩阵[26]:

$$\boldsymbol{\sigma}_x=\begin{bmatrix}0&1\\1&0\end{bmatrix},\boldsymbol{\sigma}_y=\begin{bmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{bmatrix},\boldsymbol{\sigma}_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}. \quad (5)$$

3 彩色图像的量子加密方法

令彩色图像有2^n个像素. 本文提出的彩色图像加密方法包括: 1) 量子编码; 2) 时域加密; 3) 量子傅里叶变换; 4) 频域加密; 5) 量子傅里叶反变换.

3.1 彩色图像的量子编码

彩色图像的3种基色分别用$|r\rangle,|g\rangle,|b\rangle$编码. 令第$j$个像素的三基色灰度值分别为$c_r^j,c_g^j,c_b^j$. 记

$$\theta_r^j=\frac{c_r^j}{255}\times\frac{\pi}{2},\ \theta_g^j=\frac{c_g^j}{255}\times\frac{\pi}{2},\ \theta_b^j=\frac{c_b^j}{255}\times\frac{\pi}{2},$$

$\phi_r^j,\phi_g^j,\phi_b^j$为区间$(0,2\pi)$内均匀分布的随机数, 则该像素的三基色可用量子比特编码为

$$\begin{cases}|r_j\rangle=\cos\dfrac{\theta_r^j}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\phi_r^j}\sin\dfrac{\theta_r^j}{2}|1\rangle,\\ |g_j\rangle=\cos\dfrac{\theta_g^j}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\phi_g^j}\sin\dfrac{\theta_g^j}{2}|1\rangle,\\ |b_j\rangle=\cos\dfrac{\theta_b^j}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\phi_b^j}\sin\dfrac{\theta_b^j}{2}|1\rangle.\end{cases} \quad (6)$$

设图像有2^n个像素, 利用式(6), 该图像可编码为如下的量子叠加态:

$$|\mathrm{Image}\rangle=\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle|r_j\rangle|g_j\rangle|b_j\rangle. \quad (7)$$

由式(7)可知, 该图像的编码可用$n+3$个量子比特实现, 其中前n个对像素坐标编码, 后3个对像素颜色编码. 为了用量子线路实现该图像的编码, 按如下两式

定义量子旋转门和受控旋转门:

$$\boldsymbol{R}(\theta,\phi)=\begin{bmatrix}\cos\dfrac{\theta}{2} & -\sin\dfrac{\theta}{2}\\ \mathrm{e}^{\mathrm{i}\phi}\sin\dfrac{\theta}{2} & \mathrm{e}^{\mathrm{i}\phi}\cos\dfrac{\theta}{2}\end{bmatrix},\tag{8}$$

$$\boldsymbol{CR}(p,m)=\Big(\sum_{k=0,k\neq m}^{2^{p-1}-1}|k\rangle\langle k|\Big)\otimes\boldsymbol{I}+|m\rangle\langle m|\otimes\boldsymbol{R}(\theta,\phi).\tag{9}$$

其中: $p=2,3;\ 0\leqslant m\leqslant 2^{p-1}-1$; $\boldsymbol{I}$ 为单位矩阵.

令 $\boldsymbol{R}^{+}(\theta,\phi)$ 为 $\boldsymbol{R}(\theta,\phi)$ 的共轭转置矩阵, 容易证明 $\boldsymbol{R}(\theta,\phi)\boldsymbol{R}^{+}(\theta,\phi)=\boldsymbol{R}^{+}(\theta,\phi)\boldsymbol{R}(\theta,\phi)=\boldsymbol{I}$, 所以 $\boldsymbol{R}(\theta,\phi)$ 和 $\boldsymbol{CR}(p,m)$ 都是酉算子.

根据式 (8) 和 (9), 式 (7) 中的像素比特 $|r_j\rangle$, $|g_j\rangle$, $|b_j\rangle$ 可用图 1 所示的量子线实现. 对于编码后的量子图像 $|\mathrm{Image}\rangle$, 可用图 2 所示的量子线实现. 图 2 中, $\boldsymbol{H}$ 为 Hadamard 门, 定义式为

$$\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ \boldsymbol{H}^{\otimes n}=\overbrace{\boldsymbol{H}\otimes\boldsymbol{H}\otimes\cdots\otimes\boldsymbol{H}}^{n}.$$

其在初态 $|0_1 0_2\cdots 0_n\rangle$ 上的作用为

$$\boldsymbol{H}^{\otimes n}|0_1 0_2\cdots 0_n\rangle=\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle,$$

即将初态变换为均衡的量子叠加态.

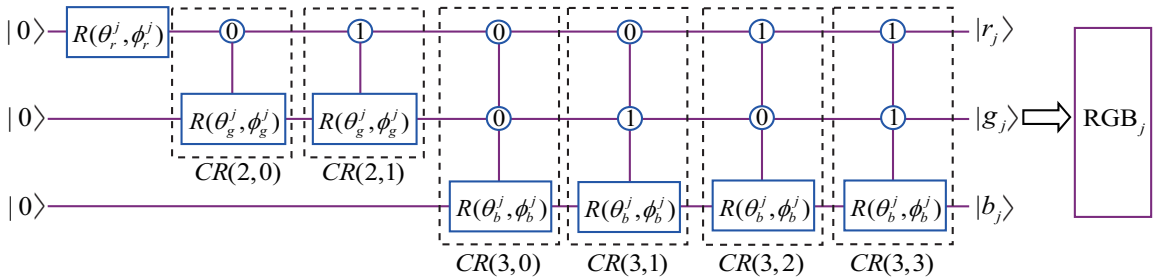


图 1　实现 $|r_j\rangle, |g_j\rangle, |b_j\rangle$ 编码的量子线路

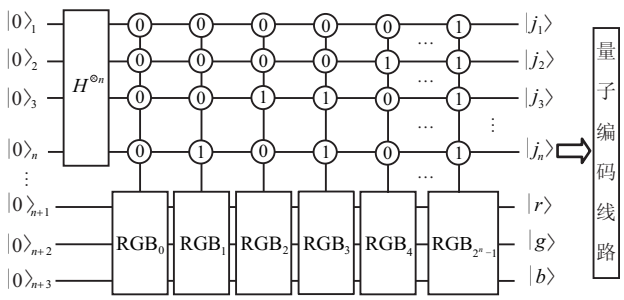


图 2　实现彩色图像编码的量子线路

值得指出, 若彩色图像的像素总数 $M\neq 2^n$, 此时取 $n=\lceil\log(M)\rceil$, 该图像的编码仍可用 $n+3$ 个量子比特实现, 只不过此时在图 2 中, 子模块 RGB_i 的个数为 M, 且 $i=0,1,\cdots,M-1$.

3.2　彩色图像的时域加密

时域加密 (TDE) 通过将每个像素的 $|r_j\rangle, |g_j\rangle, |b_j\rangle$ 在 Bloch 球面绕轴旋转实现. 秘钥为每个像素随机产生的旋转矩阵, 该矩阵由旋转轴和旋转角度确定. 令 $\boldsymbol{sn}_r^j=[x_r^j,y_r^j,z_r^j]$, $\boldsymbol{sn}_g^j=[x_g^j,y_g^j,z_g^j]$, $\boldsymbol{sn}_b^j=[x_b^j,y_b^j,z_b^j]$ 为取值 $(0,1)$ 区间的随机数向量, $\delta_r^j,\delta_g^j,\delta_b^j\in(0,2\pi)$ 为随机产生的旋转角度. 则 $|r_j\rangle, |g_j\rangle, |b_j\rangle$ 的旋转矩阵分别为

$$\boldsymbol{SR}_r^j=\cos\frac{\delta_r^j}{2}\boldsymbol{I}-\mathrm{i}\sin\frac{\delta_r^j}{2}\Big(\frac{\boldsymbol{sn}_r^j\times\sigma}{||\boldsymbol{sn}_r^j||}\Big),\tag{10}$$

$$\boldsymbol{SR}_g^j=\cos\frac{\delta_g^j}{2}\boldsymbol{I}-\mathrm{i}\sin\frac{\delta_g^j}{2}\Big(\frac{\boldsymbol{sn}_g^j\times\sigma}{||\boldsymbol{sn}_g^j||}\Big),\tag{11}$$

$$\boldsymbol{SR}_b^j=\cos\frac{\delta_b^j}{2}\boldsymbol{I}-\mathrm{i}\sin\frac{\delta_b^j}{2}\Big(\frac{\boldsymbol{sn}_b^j\times\sigma}{||\boldsymbol{sn}_b^j||}\Big).\tag{12}$$

旋转操作分别为

$$|r_j'\rangle=\boldsymbol{SR}_r^j|r_j\rangle,\ |g_j'\rangle=\boldsymbol{SR}_g^j|g_j\rangle,\ |b_j'\rangle=\boldsymbol{SR}_b^j|b_j\rangle.$$

定义受控运算

$$\boldsymbol{CSR}_\chi^j(p,m)=\Big(\sum_{k=0,k\neq m}^{2^{p-1}-1}|k\rangle\langle k|\Big)\otimes\boldsymbol{I}+|m\rangle\langle m|\otimes\boldsymbol{SR}\chi^j,$$

其中 $\chi=g,b$. 容易证明, $\boldsymbol{SR}_\chi^j$ 和 $\boldsymbol{CSR}_\chi^j(p,m)$ 都是酉算子. 实现时域加密的量子线路如图 3 和图 4 所示.

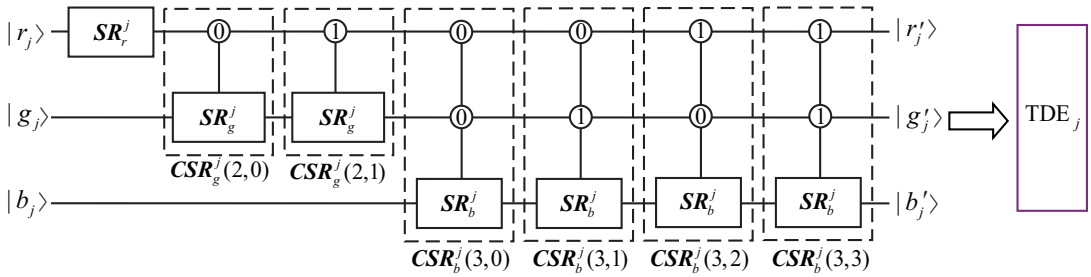


图 3　实现 $|r\rangle, |g\rangle, |b\rangle$ 随机旋转的量子线路

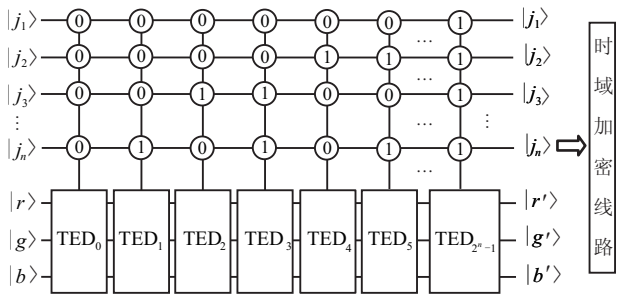


图 4 实现彩色图像时域加密的量子线路

3.3 彩色图像的量子傅里叶变换

量子傅里叶变换 (QFT) 是一个定义在标准正交基 $|0\rangle, |1\rangle, \cdots, |N-1\rangle$ 上的线性算子. 该算子在基态上的作用为[27]

$$\mathrm{QFT}(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{e}^{2\pi ijk/N} |k\rangle, \tag{13}$$

在任意叠加态上的作用为

$$\mathrm{QFT}\Big(\sum_{j=0}^{N-1} x_j |j\rangle \Big) = \sum_{k=0}^{N-1} y_k |k\rangle, \tag{14}$$

其中 $y_k = \dfrac{1}{\sqrt{N}} \displaystyle\sum_{j=0}^{N-1} x_j \mathrm{e}^{2\pi ijk/N}$.

定义酉算子 $\boldsymbol{R}_k = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{2\pi \mathrm{i}/2^k} \end{bmatrix}$ 及受控运算 $\boldsymbol{CR}_k |j_s\rangle|j_t\rangle = \boldsymbol{R}_k^{j_t} |j_s\rangle|j_t\rangle$, 即若 $j_t = 1$, 则酉算子 $\boldsymbol{R}_k$ 作用于 $|j_s\rangle$, 否则 $\boldsymbol{R}_k$ 不起作用. 彩色图像的量子傅里叶变换可用图 5 所示的量子线路实现.

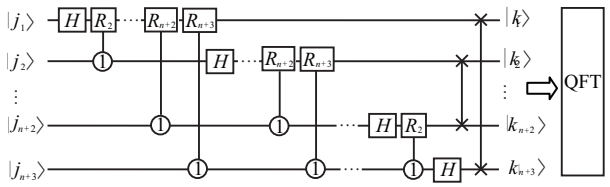


图 5 实现量子傅里叶变换的量子线路

3.4 彩色图像的频域加密

与时域加密类似, 频域加密 (FDE) 也采用对 3 个像素比特 $|j_{n+1}\rangle, |j_{n+2}\rangle, |j_{n+3}\rangle$ 实施绕轴旋转实现, 秘钥为每个像素随机产生的旋转矩阵. 令 $\boldsymbol{fn}_r^j = [u_r^j, v_r^j, w_r^j]$, $\boldsymbol{fn}_g^j = [u_g^j, v_g^j, w_g^j]$, $\boldsymbol{fn}_b^j = [u_b^j, v_b^j, w_b^j]$ 为取值 $(0,1)$ 区间的随机数向量, $\xi_r^j, \xi_g^j, \xi_b^j \in (0, 2\pi)$ 为随机产生的旋转角度. $|r_j\rangle, |g_j\rangle, |b_j\rangle$ 的旋转矩阵为

$$\boldsymbol{FR}_\chi^j = \cos\frac{\xi_\chi^j}{2}\boldsymbol{I} - \mathrm{i}\sin\frac{\xi_\chi^j}{2}\Big(\frac{\boldsymbol{fn}_\chi^j \times \sigma}{||\boldsymbol{fn}_\chi^j||}\Big), \tag{15}$$

其中 $\chi = r, g, b$.

实现频域加密的量子线路结构与图 4 相同, 仅是旋转轴和旋转角度不同, 即频域秘钥和时域秘钥是相互独立的.

3.5 彩色图像的量子傅里叶逆变换

量子傅里叶逆变换 (IQFT) 也是一个定义在标准正交基 $|0\rangle, |1\rangle, \cdots, |N-1\rangle$ 上的线性算子. 在任意叠加态上的作用为

$$\mathrm{IQFT}\Big(\sum_{j=0}^{N-1} x_j |j\rangle \Big) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} x_j \mathrm{e}^{-2\pi ijk/N} |k\rangle. \tag{16}$$

定义酉算子 $\boldsymbol{R}_k = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{-2\pi \mathrm{i}/2^k} \end{bmatrix}$ 及受控运算 $\boldsymbol{CR}_k |j_s\rangle|j_t\rangle = \boldsymbol{R}_k^{j_t} |j_s\rangle|j_t\rangle$, 彩色图像的量子傅里叶反变换也可用图 5 的量子线路实现. 至此完成了彩色图像的量子加密过程.

4 量子图像的解密方法

解密是加密的逆运算, 与加密方法类似, 解密方法也包括: 1) 量子傅里叶变换; 2) 频域解密; 3) 量子傅里叶反变换; 4) 时域解密; 5) 投影测量. 各步采用的解密秘钥与加密秘钥严格相同. 由于加密阶段采用的算子都是酉算子, 对于解密过程的前 4 步, 可采用与加密过程第 2) ~ 第 5) 步相同的量子线路, 只需将所有算子改为其共轭转置即可. 为实现投影测量, 首先按酉矩阵谱分解的形式定义测量算子

$$\boldsymbol{M} = \sum_{k=0}^{2^3-1} (m_k^{(1)} \boldsymbol{p}_k^{(1)} + \cdots + m_k^{(2^n-1)} \boldsymbol{p}_k^{(2^n-1)}), \tag{17}$$

其中 $\boldsymbol{p}_k^{(j)} = |j\rangle|k\rangle\langle j|\langle k|$ 为 $\boldsymbol{M}$ 的本征值 $m_k^{(j)}$ 对应的一组正交投影矩阵.

经过解密操作 1) ~ 4), 彩色图像可恢复为式 (7) 描述的量子叠加态 $|\mathrm{Image}\rangle$. 在 $|\mathrm{Image}\rangle$ 上应用测量算子 $\boldsymbol{M}$, 可以概率 $P(m_k^{(j)}) = \langle \mathrm{Image}|\boldsymbol{p}_k^{(j)}|\mathrm{Image}\rangle = |\boldsymbol{\zeta}_j(k)|^2$ 获得 $m_k^{(j)}$, 即

$$|\boldsymbol{\zeta}_j(k)| = \sqrt{P(m_k^j)}. \tag{18}$$

与量子图像 $|\mathrm{Image}\rangle$ 作比较, 并注意到 $|\mathrm{e}^{\mathrm{i}\phi_r^j}| = |\mathrm{e}^{i\phi_g^j}| = |\mathrm{e}^{\mathrm{i}\phi_b^j}| = 1$, $\boldsymbol{\zeta}_j$ 可简写为

$$\boldsymbol{\zeta}_j = \begin{bmatrix} \cos\dfrac{\theta_r^j}{2}\cos\dfrac{\theta_g^j}{2}\cos\dfrac{\theta_b^j}{2} \\ \cos\dfrac{\theta_r^j}{2}\cos\dfrac{\theta_g^j}{2}\sin\dfrac{\theta_b^j}{2} \\ \cos\dfrac{\theta_r^j}{2}\sin\dfrac{\theta_g^j}{2}\cos\dfrac{\theta_b^j}{2} \\ \cos\dfrac{\theta_r^j}{2}\sin\dfrac{\theta_g^j}{2}\sin\dfrac{\theta_b^j}{2} \\ \sin\dfrac{\theta_r^j}{2}\cos\dfrac{\theta_g^j}{2}\cos\dfrac{\theta_b^j}{2} \\ \sin\dfrac{\theta_r^j}{2}\cos\dfrac{\theta_g^j}{2}\sin\dfrac{\theta_b^j}{2} \\ \sin\dfrac{\theta_r^j}{2}\sin\dfrac{\theta_g^j}{2}\cos\dfrac{\theta_b^j}{2} \\ \sin\dfrac{\theta_r^j}{2}\sin\dfrac{\theta_g^j}{2}\sin\dfrac{\theta_b^j}{2} \end{bmatrix}. \tag{19}$$

由式(19)可得

$$\begin{cases}\theta_r^j=\arctan\dfrac{\zeta_j(5)}{\zeta_j(1)},\\ \theta_g^j=\arctan\dfrac{\zeta_j(3)}{\zeta_j(1)},\\ \theta_b^j=\arctan\dfrac{\zeta_j(2)}{\zeta_j(1)};\end{cases}\tag{20}$$

$$\begin{cases}c_r^j=\dfrac{510\theta_r^j}{\pi},\\ c_g^j=\dfrac{510\theta_g^j}{\pi},\\ c_b^j=\dfrac{510\theta_b^j}{\pi}.\end{cases}\tag{21}$$

至此, 彩色图像得以完全恢复.

5　普通计算机上的实现方法

本文提出的基于量子比特绕轴旋转的彩色图像加密方法, 是直接基于量子线路设计的, 是可以在将来的量子计算机上执行的. 量子计算机目前还没有普及, 因此有必要给出在普通计算机上的仿真方法.

设明文图像有 $3MN$ 个像素, 存储为 $M\times N\times 3$ 的矩阵, 因为三基色采用 $|r\rangle,|g\rangle,|b\rangle$ 编码, 编码后每个像素有 8 个概率幅, 因此量子图像可用 $8MN$ 维列向量 Image 存储.

对于时域加密和频域加密, 本质上是对每个像素施加旋转操作. 令第 j 个像素的 8 个概率幅为 $\boldsymbol{\zeta}_j=[\zeta_1^j,\cdots,\zeta_8^j]^{\mathrm{T}}$, 三基色的旋转矩阵分别为 $\boldsymbol{R}_r^j,\boldsymbol{R}_g^j,\boldsymbol{R}_b^j$, 该像素的旋转操作为 $\boldsymbol{\zeta}_j'=(\boldsymbol{R}_r^j\otimes\boldsymbol{R}_g^j\otimes\boldsymbol{R}_b^j)\boldsymbol{\zeta}_j$.

对于傅里叶变换, 可采用下式实现:

$$\mathrm{Image}'(j)=\frac{1}{\sqrt{8MN}}\sum_{k=0}^{8MN-1}\mathrm{Image}(j)\mathrm{e}^{\frac{i2\pi jk}{8MN}};$$

对于傅里叶逆变换, 可采用下式实现:

$$\mathrm{Image}(j)=\frac{1}{\sqrt{8MN}}\sum_{k=0}^{8MN-1}\mathrm{Image}'(j)\mathrm{e}^{-\frac{i2\pi jk}{8MN}}.$$

对于时域解密和频域解密, 与加密操作类似, 只需采用加密时相应旋转矩阵的共轭转置即可. 对于量子叠加态的测量, 只需将式(20)修改为

$$\begin{cases}\theta_r^j=\arctan\dfrac{\mathrm{e}^{-i\phi_r^j}\zeta_j(5)}{\zeta_j(1)},\\ \theta_g^j=\arctan\dfrac{\mathrm{e}^{-i\phi_g^j}\zeta_j(3)}{\zeta_j(1)},\\ \theta_b^j=\arctan\dfrac{\mathrm{e}^{-i\phi_b^j}\zeta_j(2)}{\zeta_j(1)},\end{cases}\tag{22}$$

然后应用式(21)即可.

6　对比实验

目前, 还没有量子计算机, 所以本实验在普通计算机上进行仿真.

为验证本文所提出方法的优势, 与文献 [20] 提出的方法作对比. 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. 采用的彩图来源于网站 http://sipi.usc.edu/database/database.php, 共 15 幅, 其中前 8 幅每行每列均为 256 个像素, 后 7 幅每行每列均为 512 个像素. 15 幅原始图像如图 6 所示, 加密图像如图 7 所示.

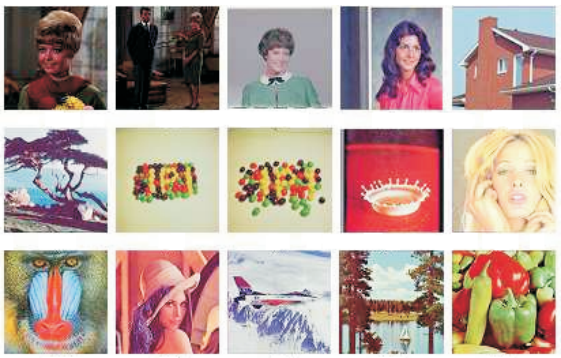


图 6　15 幅原始图像

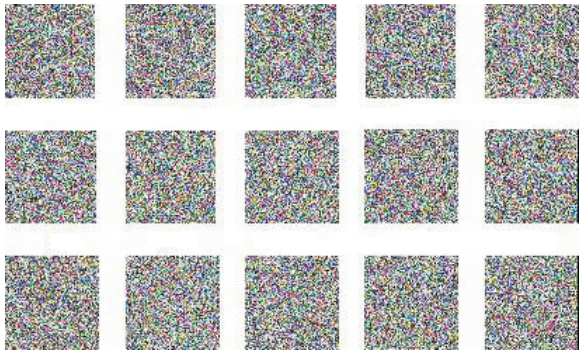


图 7　15 幅加密图像

6.1　密钥空间分析

为抵御蛮力攻击, 密钥空间必须足够大, 本文所提出算法的密钥可描述为

$$\mathrm{Key}_s=\boldsymbol{SR}_r^j\otimes\boldsymbol{SR}_g^j\otimes\boldsymbol{SR}_b^j,\tag{23}$$

$$\mathrm{Key}_f=\boldsymbol{FR}_r^j\otimes\boldsymbol{FR}_g^j\otimes\boldsymbol{FR}_b^j.\tag{24}$$

其中: Key_s 包含随机数 $x_r^j,y_r^j,z_r^j,x_g^j,y_g^j,z_g^j,x_b^j,y_b^j,z_b^j$; Key_f 包含随机数 $u_r^j,v_r^j,w_r^j,u_g^j,v_g^j,w_g^j,u_b^j,v_b^j,w_b^j$; $j=1,2,\cdots,2^n$, 2^n 为彩色图像的像素数. 这些随机数或者在区间 $(0,1)$ 均匀分布, 或者在区间 $(0,2\pi)$ 均匀分布. 这表明本文算法有足够大的密钥空间, 可以抵御蛮力攻击.

6.2　密钥敏感性分析

一个理想的加密方案, 其解密效果应该对秘钥高度敏感. 为检验解密效果对秘钥的敏感性, 采用文献 [20] 中的方法, 即分别采用正确的 Key_s 和正确的 Key_f、正确的 Key_s 和随机的 Key_f、随机的 Key_s 和正确的 Key_f 恢复加密图像. 其中采用正确 Key_s 和正确 Key_f 的恢复效果与原始图像完全相同, 不再重列, 其他两种的恢复效果分别如图 8 和图 9 所示.

图 8 正确 Key_s 和随机 Key_f 的解密效果

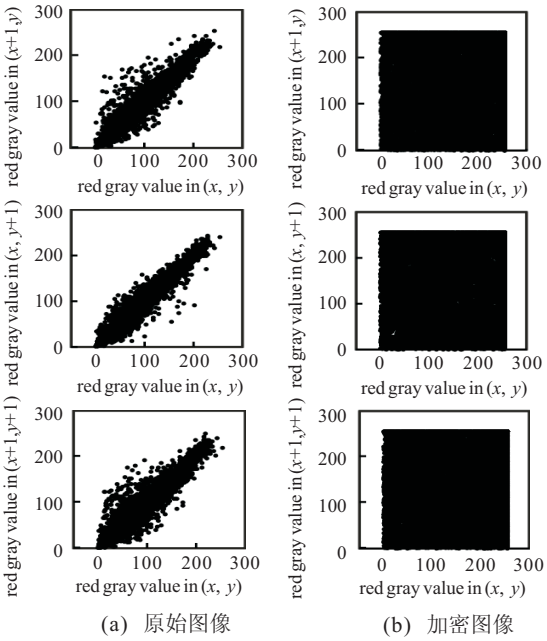
图 9 随机 Key_s 和正确 Key_f 的解密效果

由图 8 和图 9 可知, 当 Key_s 正确、Key_f 随机时, 解密图像呈现为不能获取任何信息的随机噪声. 当 Key_s 随机、Key_f 正确时, 解密图像仅呈现出相当模糊的原始图像的轮廓. 实验结果表明, 只有当 Key_s、Key_f 都正确时才能无失真地恢复原来的彩色图像. 由于该方法的密钥空间很大, 除非事先获得正确的 Key_s、Key_f, 否则要精确地恢复原始图像几乎是不可能的.

6.3 相邻像素的相关性分析

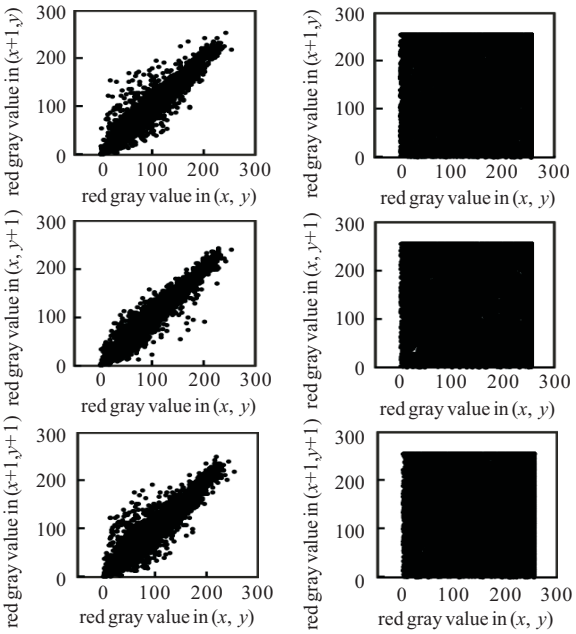
在原始图像中, 相邻像素的三基色灰度值是高度相关的. 然而一个好的加密方案, 其加密图像应使水平、竖直、对角 3 个方向上相邻像素灰度值的相关性尽量小. 为检验本文所提出的加密方案的性能, 分别针对 15 幅原始图像和加密图像考察相邻像素的相关性. 具体方法为: 分别在水平、竖直、对角 3 个方向上随机选取 10 000 对相邻像素, 根据像素三基色的灰度值绘制这些相邻像素的分布.

以第 1 幅图像为例, 原始图像和加密图像中 10 000 对相邻像素的相关性如图 10 ～图 12 所示, 其中子图 (a) 是针对原始图像的, 子图 (b) 是针对加密图像的.



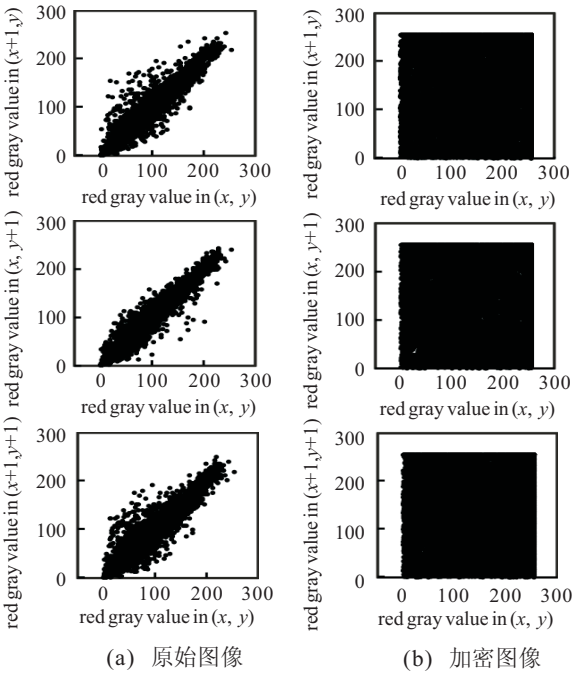
(a) 原始图像 (b) 加密图像

图 10 原始图像与加密图像的绿色相关性对比



(a) 原始图像 (b) 加密图像

图 11 原始图像与加密图像的红色相关性对比



(a) 原始图像 (b) 加密图像

图 12 原始图像与加密图像的蓝色相关性对比

表 1　原始图像和加密图像的相关系数对比

序号		水平相关		竖直相关		对角相关	
		原始图像	加密图像	原始图像	加密图像	原始图像	加密图像
1	R	0.961 5	0.001 2	0.972 7	−0.011 0	0.948 8	−0.005 6
	G	0.969 6	−0.019 4	0.972 2	−0.000 6	0.954 1	0.002 4
	B	0.957 3	−0.002 1	0.961 1	0.007 7	0.940 9	0.006 6
2	R	0.957 4	0.006 4	0.952 6	0.000 8	0.921 3	−0.005 3
	G	0.949 0	−0.003 9	0.930 8	0.011 0	0.897 4	0.011 8
	B	0.938 7	0.002 0	0.913 5	0.001 1	0.881 6	−0.002 2
3	R	0.948 6	0.008 0	0.976 5	−0.008 9	0.932 3	0.011 2
	G	0.939 8	−0.000 1	0.974 4	−0.018 1	0.923 1	−0.004 7
	B	0.943 7	−0.006 1	0.972 3	−0.003 4	0.926 1	0.008 3
4	R	0.994 3	0.001 0	0.979 0	−0.004 2	0.975 6	0.000 7
	G	0.989 5	0.016 1	0.961 2	−0.010 2	0.954 3	0.013 4
	B	0.982 5	0.013 9	0.943 0	−0.004 5	0.935 3	0.004 1
5	R	0.935 5	0.033 6	0.969 8	−0.003 8	0.916 7	−0.004 1
	G	0.973 2	0.000 3	0.981 1	0.011 5	0.958 8	−0.017 2
	B	0.975 9	−0.006 8	0.983 1	−0.006 3	0.964 3	−0.002 7
6	R	0.915 9	0.006 9	0.959 5	0.001 5	0.898 8	0.003 1
	G	0.934 6	0.014 4	0.968 0	0.010 3	0.921 8	0.000 8
	B	0.926 1	0.007 8	0.963 0	−0.001 2	0.916 5	0.006 8
7	R	0.977 8	0.008 6	0.975 8	−0.005 6	0.955 7	0.006 9
	G	0.980 8	−0.010 6	0.976 9	−0.002 0	0.962 5	0.016 8
	B	0.989 6	−0.025 7	0.990 2	0.010 8	0.981 2	0.008 4
8	R	0.976 2	−0.008 4	0.973 6	0.011 7	0.950 5	−0.002 4
	G	0.977 3	0.000 8	0.971 7	−0.000 7	0.951 1	−0.001 9
	B	0.981 0	0.002 2	0.976 0	−0.006 1	0.958 8	0.004 7
9	R	0.998 3	−0.002 0	0.997 0	0.001 0	0.996 2	0.013 9
	G	0.989 2	0.004 7	0.988 1	−0.001 8	0.981 7	−0.001 6
	B	0.985 4	0.003 4	0.984 7	−0.011 7	0.975 3	−0.004 0
10	R	0.851 0	0.000 3	0.960 5	−0.005 1	0.828 4	−0.012 2
	G	0.857 9	−0.004 5	0.918 3	−0.003 2	0.814 6	−0.001 7
	B	0.844 4	0.007 3	0.920 8	0.009 7	0.797 3	−0.006 8
11	R	0.862 5	−0.001 6	0.916 2	−0.006 4	0.849 8	−0.017 8
	G	0.764 5	0.011 2	0.859 3	−0.008 7	0.737 0	0.009 0
	B	0.869 4	−0.005 9	0.895 6	0.000 9	0.824 8	−0.005 2
12	R	0.989 4	−0.020 2	0.977 8	−0.001 2	0.968 3	−0.000 6
	G	0.981 9	0.005 8	0.966 1	−0.010 8	0.953 3	0.011 9
	B	0.955 5	−0.001 3	0.925 3	0.000 3	0.907 8	0.008 9
13	R	0.972 2	0.007 0	0.966 0	−0.005 6	0.945 3	−0.025 2
	G	0.973 7	0.003 9	0.905 4	−0.001 9	0.888 1	−0.011 0
	B	0.958 4	0.002 5	0.955 2	−0.014 4	0.933 6	−0.000 0
14	R	0.959 5	0.006 7	0.950 7	0.014 8	0.942 7	0.016 8
	G	0.970 5	0.008 9	0.962 6	−0.000 7	0.949 6	0.020 9
	B	0.970 1	−0.003 0	0.960 9	−0.014 5	0.944 8	0.002 6
15	R	0.967 5	0.018 0	0.952 1	−0.008 2	0.945 8	0.012 7
	G	0.987 3	0.001 8	0.970 2	−0.005 4	0.963 3	0.008 7
	B	0.973 8	0.007 4	0.962 7	−0.011 4	0.948 4	−0.002 3

为定量分析原始图像和加密图像中相邻像素的相关性, 首先定义相关系数

$$R_{xy}=\frac{\mathrm{E}(x-\mathrm{E}(x)\mathrm{E}(y-\mathrm{E}(y)))}{\sqrt{D(x)D(y)}}, \tag{25}$$

其中 $\mathrm{E}(x)$ 和 $D(y)$ 分别为灰度值 x 的数学期望和方差.

对于 15 幅彩色图像及对应加密图像, 水平、竖直、对角 3 个方向相邻像素的相关系数见表 1. 由

图 10～图 12 和表 1 可知, 原始图像中相邻像素之间的相关性很强, 而加密图像中的相邻像素几乎是不相关的. 因此, 本文提出的加密方案具有很好的安全性.

6.4 直方图分析

直方图可以反映图像中像素灰度值的分布, 显然, 均匀分布的直方图能够有效抵御各种蛮力攻击. 以第 12 幅图像为例, 加密前后像素灰度值的直方图如图 13 所示, 其中上面 3 幅为原始图像的直方图, 下面 3 幅为加密图像的直方图. 由图 13 可知, 加密前后的直方图显著不同, 且加密后的直方图比较均匀, 几乎不能给蛮力攻击者提供任何解密线索.

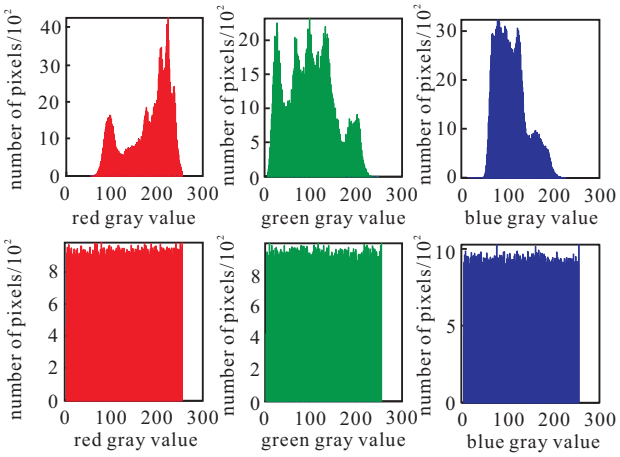


图 13 原始图像和加密图像中像素的直方图分布

6.5 与文献 [20] 方法的比较

本文方法与文献 [20] 方法的加密思想基本相同, 但在图像编码及量子比特旋转方面明显不同. 由于文献 [20] 已验证其方法优于文献 [21] 中的 DRPE 方法, 所以仅与文献 [20] 提出的方法作比较.

首先考虑密钥空间. 文献 [20] 中的密钥参数为 $\Psi_{1j}, \upsilon_{1j}, \tau_{1j} \in (0, 2\pi)$, $\Psi_{2j}, \upsilon_{2j}, \tau_{2j} \in (0, 2\pi)$, 密钥空间为 $(0, 2\pi)^{6\times 2^n}$; 本文方法的秘钥参数为 $x_r^j, y_r^j, z_r^j \in (0,1)$, $x_g^j, y_g^j, z_g^j \in (0,1)$, $x_b^j, y_b^j, z_b^j \in (0,1)$, $\delta_r^j, \delta_g^j, \delta_b^j \in (0, 2\pi)$, $u_r^j, v_r^j, w_r^j \in (0,1)$, $u_g^j, v_g^j, w_g^j \in (0,1)$, $u_b^j, v_b^j, w_b^j \in (0,1)$, $\xi_r^j, \xi_g^j, \xi_b^j \in (0, 2\pi)$, 密钥空间为 $(0,1)^{18\times 2^n} \times (0, 2\pi)^{6\times 2^n}$. 所以, 本文方法的密钥空间比文献 [20] 中的方法大得多.

其次考虑加密图像的相关系数. 为简便, 采用 3 种基色相关系数的平均值作为对比指标. 分别采用两种方法加密后, 15 幅彩色图像中相邻像素的相关系数如表 2 所示.

表 2 本文方法与文献[20]方法的加密效果对比

序号	水平相关		竖直相关		对角相关	
	本文方法	文献 [20]	本文方法	文献 [20]	本文方法	文献 [20]
1	−0.006 8	−0.003 4	−0.001 3	0.005 1	0.001 1	0.009 5
2	0.001 5	0.008 5	0.004 3	−0.006 0	0.001 4	−0.005 9
3	0.000 6	−0.007 3	−0.010 1	0.004 0	0.004 9	0.003 6
4	0.010 3	0.002 9	−0.006 3	−0.008 2	0.006 1	−0.016 8
5	0.009 0	−0.002 1	0.000 5	0.005 8	−0.008 0	0.009 7
6	0.009 7	0.005 2	0.003 5	−0.008 3	0.003 6	0.005 1
7	−0.009 2	0.009 6	0.001 1	0.002 1	0.010 7	−0.004 9
8	−0.001 8	0.009 5	0.001 6	0.004 5	0.000 1	−0.000 5
9	0.002 0	0.003 0	−0.004 2	−0.006 9	0.002 8	−0.003 4
10	0.001 0	−0.005 0	0.000 5	−0.003 4	−0.006 9	−0.002 1
11	0.001 2	0.008 8	−0.004 7	−0.009 7	−0.004 7	0.007 3
12	−0.005 2	0.006 7	−0.003 9	0.004 6	0.006 7	−0.003 9
13	0.004 5	0.002 9	−0.007 3	−0.008 2	−0.012 1	−0.017 6
14	0.004 2	0.005 6	−0.000 1	−0.002 2	0.013 4	−0.014 2
15	0.009 1	−0.007 9	−0.008 3	−0.009 1	0.006 4	0.002 0
平均	0.002 0	0.002 5	−0.002 3	−0.002 4	0.001 7	−0.002 1

由表 2 可知, 本文方法使加密图像在水平、竖直、对角 3 个方向的相关性均略弱于文献 [20] 中的方法. 所以, 本文方法略优于文献 [20] 的方法. 然而, 从密钥空间考虑, 本文算法的密钥空间远大于文献 [20] 中的方法, 从而使对密码的破解更为困难, 进一步提高了图像传输的安全性.

7 结 论

本文提出了一种基于量子计算的彩色图像加密解密方法. 加密操作包括: 量子编码、时域加密、量子傅里叶变换、频域加密、量子傅里叶反变换. 时域加密和频域加密采用量子比特绕轴旋转实现, 秘钥为旋转矩阵. 解密操作为加密操作的逆运算. 针对方法的每一步, 给出了具体实现的量子线路. 该方法的优势在于能够在量子计算机上实现且具有很大的密钥空间. 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] Akhshani A, Akhavan A, Lim S C. An image encryption scheme based on quantum logistic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(12): 4653-4661.

[2] Chen L F, Zhao D M, Ge F. Image encryption based on singular value decomposition and Arnold transform in fractional domain[J]. Optics Communications, 2013, 291(3): 98-103.

[3] Chen T H, Wu C S. Compression-unimpaired batch-image encryption combining vector quantization and index compression[J]. Information Science, 2010, 180(9): 1690-1701.

[4] Chen T H, Li K C. Multi-image encryption by circular random grids[J]. Information Science, 2012, 189(15): 255-265.

[5] Lu D J, He W Q, Peng X. Optical image encryption based on a radial shearing interferometer[J]. J of Optics, 2013, 15(10): 105405.

[6] Mandal M K B, Gourab D, Chattopadhyay D. An image encryption process based on chaotic logistic map[J]. IETE Technical Review, 2012, 29(5): 395-404.

[7] Ozkaynak F, Ozer A B, Yavuz S. Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences[J]. Optics Communications, 2012, 285(24): 4946-4948.

[8] Shi Y S, Li T, Wang Y L. Optical image encryption via ptychography[J]. Optics Letters, 2013, 38(9): 1425-1427.

[9] Sun M J, Shi J H, Li H. A simple optical encryption based on shape merging technique in periodic diffraction correlation imaging[J]. Optics Express, 2013, 21(16): 19395-19400.

[10] Wang X G, Zhao D M. Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle[J]. Applied Optics, 2013, 52(25): 21-29.

[11] Wang X Y, Liu L T. Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos[J]. Nonlinear Dynamics, 2013, 73(1/2): 795-800.

[12] Ye G D, Wong K W. An efficient chaotic image encryption algorithm based on a generalized Arnold map[J]. Nonlinear Dynamics, 2012, 69(4): 2079-2087.

[13] Zang J L, Xie Z W, Zhang Y. Optical image encryption with spatially incoherent illumination[J]. Optics Letters, 2013, 38(8): 1289-1291.

[14] Zhu Z L, Zhang W, Wong K W. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Science, 2011, 181(6): 1171-1186.

[15] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]. Proc of the 35th Annual IEEE Symposium on Foundations of Computer Science. New York: IEEE Press, 1994: 124-134.

[16] Grover L K. A fast quantum mechanical algorithm for database search[C]. Proc of the 28th Annual ACM Symposium on Theory of Computing. New York: IEEE Press, 1996: 212-219.

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

[18] Phuc Q L, Fangyan D, Kaoru H. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations[J]. Quantum Information Processing, 2011, 10(1): 63-84.

[19] Zhou R G, Wu Q, Zhang M Q, et al. Quantum image encryption and decryption algorithms based on quantum image geometric transformations[J]. Int J of Theoretical Physics, 2013, 52(6): 1802-1817.

[20] Yang Y G, Jia X, Sun S J, et al. Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding[J]. Information Sciences, 2014, 277(9): 445-457.

[21] Refregier R, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics Letters, 1995, 20(7): 767-769.

[22] Carnicer A, Montes U, Arcos S. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys[J]. Optics Letters, 2005, 30(13): 1644-1646.

[23] Frauel Y, Castro A, Naughton T. Resistance of the double random phase encryption against various attacks[J]. Optics Express, 2007, 15(16): 10253-10265.

[24] Peng X, Zhang P, Wei H. Known-plaintext attack on optical encryption scheme based on double random phase keys[J]. Optics Letters, 2006, 31(8): 1044-1046.

[25] Peng X, Wei H, Zhang P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain[J]. Optics Letters, 2006, 31(22): 3261-3263.

[26] Giuliano B, Giulio C, Giuliano S. Principles of quantum computation and information[M]. Singapore: World Scientific, 2004: 103-105.

(责任编辑：孙艺红)