基于交替量子随机行走的高维量子图像加密模型

柯祉衡[1]，宋佳宝[1]，王一诺[2]，王浩文[1]，王淑梅[2]，马鸿洋[2*]

(1. 青岛理工大学信息与控制工程学院 山东 青岛 266520；2. 青岛理工大学理学院 山东 青岛 266520)

【摘要】图像加密是保证数字图像在互联网上进行安全传输的关键环节。文中提出了一种基于交替量子随机行走（AQW）与异或操作的彩色量子图像加密算法。首先，对原始彩色图像进行彩色量子图像表示法（NCQI）表示，构建量子线路，利用受控 AQW 生成的二进制概率矩阵构建量子异或矩阵，完成对原始量子图像的加密操作，解密过程是加密过程的逆过程。AQW 的初始条件是保证量子图像加密算法安全性的关键。通过对提出的加密模型进行经典计算机上的仿真实验，验证了该量子图像加密模型的安全性。

关 键 词 AQW； NCQI； 量子异或操作； 量子图像加密； 量子线路

中图分类号 TP391.9 **文献标志码** A doi:10.12178/1001-0548.2022303

High Dimensional Quantum Image Encryption Model Based on Alternating Quantum Random Walk

KE Zhiheng[1], SONG Jiabao[1], WANG Yinuo[2], WANG Haowen[1], WANG Shumei[2], and MA Hongyang[2*]

(1. School of Information and Control Engineering, Qingdao University of Technology Qingdao Shandong 266520;

2. College of Science, Qingdao University of Technology Qingdao Shandong 266520)

Abstract Image encryption is a key link to ensure the secure transmission of digital images over the Internet. In this paper, a color quantum image encryption algorithm based on alternating quantum random walk (AQW) and XOR operation is proposed. Firstly, the original color image is represented by color quantum image representation (NCQI), the quantum circuit is constructed, and the quantum XOR matrix is constructed by using the binary probability matrix generated by the controlled AQW to complete the encryption operation of the original quantum image, and the decryption process is the reverse process of the encryption process. The initial condition of AQW is the key to guaranteeing the security of quantum image encryption algorithms. The security of the proposed quantum image encryption model is verified through the simulation experiment of on classical computer.

Key words AQW; NCQI; quantum XOR; quantum image encryption; quantum circuit

随着互联网与通信技术的发展，图像作为最广泛应用的信息传输媒介，相较于文字信息，其包含的信息量更加巨大，每年由于信息泄漏而造成的损失十分巨大，图像传输过程中的安全问题成为一个重要的研究课题[1]，提出更加安全高效的加密算法就显得尤其重要。数字图像在计算机中的存储可以视为一个二维像素矩阵，以二进制方式存在硬盘中，具有数据量大、相邻像素点间关联度高等特点，故而传统的流数据加密算法如 DES、IDEA、AES 等对数字图像进行处理时，加密后的图像容易被攻击和破解。

目前，主流的数字图像加密思路分为像素点位置制乱与像素值制乱，前者有 Arnold 变换[2]，Fibonacci 变换与魔方置换[3] 等，前面两种方法在对图像进行加密时，均表现出周期性，这增大了图像被破译的风险；像素值制乱主要有混沌映射法[4]，利用混沌系统的初值敏感性生成加密矩阵，并通过对像素值处理完成加密。文献 [5] 提出了结合多种

收稿日期：2022－09－05；修回日期：2022－12－04

基金项目：国家自然科学基金 (11975132)；山东省自然基金面上项目 (ZR2021MF049)；山东省自然科学基金 (ZR2019YQ01)；山东省自然科学基金联合基金 (ZR202108020011)

作者简介：柯祉衡 (1996－)，男，主要从事软件工程、图像加密等方面的研究.

*通信作者：马鸿洋，E-mail：hongyang_ma@aliyun.com

混沌系统的图像加密算法，进一步提高了加密效率与安全性。

量子计算[6]是以量子力学基本原理为基础对数据进行计算的一种模型，用来研究量子计算机上的计算问题，包含叠加、纠缠等特性，拥有了传统计算机不具有的强大并行运算能力。1994 年，文献 [7] 提出了大数质因子分解量子算法，1996 年，文献 [8] 提出量子快速搜索算法，前者将复杂度从经典算法的O(N)减小到O($N^{1/2}$)；后者将复杂度从指数级降低到多项式级。2022 年，文献 [9] 提出了一种基于置换群的量子行走反馈搜索算法，提高了搜索速度，近些年，将量子特性与其他领域相融合成为一种研究趋势[10-12]。

量子随机行走（alternating quantum random walk, AQW）是一种量子计算模型，1993 年由文献 [13] 首次提出，但在这个实验中，研究人员需要对其中的每一步进行一次测量，而测量将导致量子态的坍缩，故而与经典行走相比并未表现出量子优越性，直到文献 [14] 提出连续量子随机行走，文献 [15] 提出离散量子随机行走，其量子特性才得以显现。随后，研究人员开始致力于探索量子随机行走的应用领域。文献 [16-19] 针对不同场景对量子行走的性质作了进一步的研究，2012 年，文献 [20] 将连续时间量子随机行走运用于图同构和聚类算法中，拓展了量子随机行走的应用范围，近年来，一些学者尝试将 AQW 作用到图像的加密中，并得到了良好的加密效果[21-23]。

量子图像处理作为量子计算的分支，集图像处理、量子信息学等学科于一体，由文献 [24] 在 1997 年首次提出。2003 年，文献 [25] 尝试将已有的量子算法应用于图像处理上，并逐渐形成两个分支：量子图像表示和量子图像处理。2005 年，文献 [26] 提出一种量子图像表示方法，将二维图像中的像素值转换为了 Hilbert 空间中的量子态，目前已经有多种量子图像表示方法被提出，如 Entangled Image[27], FRQI[28], NEQI[29]。本文使用的 NCQI[30] 是 NEQI 模型的扩展，解决了 NEQI 只能表示灰度图像的缺陷，将量子图像表示运用到了彩色图像中。在量子图像处理方面，也有很多成果问世，如量子几何变换[31]、量子缩放[32]、量子平移[33]。2020 年，文献 [34] 提出了一种新型的基于 Kirsch 算子边缘提取的量子图像处理算法，2021 年，文献 [35] 提出了一种新的量子彩色图像加密算法，验证了对量子图像进行加密传输的安全性与可行性。

为解决目前图像传输过程易受攻击与泄密的难题，本文提出了一种基于 AQW 与量子异或操作的量子图像加密算法，首先为一幅经典的彩色图像构建量子线路，并以 NCQI 模型存入量子计算机中，得到$|I\rangle$，接着按照通信双方事先约定好的密钥进行一定步数的 AQW 并生成概率矩阵，并以此生成量子异或操作矩阵，将其作用到$|I\rangle$上，得到加密后的量子图像$|M\rangle$；解密过程是加密过程的逆过程，由于接收方拥有相同的 AQW 参数，将生成一个相同的量子异或操作矩阵。基于 AQW 的安全性与量子图像的量子性，可以提高图像在传输过程中的安全性。

1 相关工作

1.1 交替量子随机行走

交替量子随机行走作为经典漫步的推广，具有密钥敏感性与非周期性等特点，可抵抗各种攻击。一维量子漫步的演化算符U作用在希尔伯特空间$H_p \times H_c$上，其中H_p为行走空间，由位置态$|x\rangle$，$x \in X$张量而成，X是一维直线上所有点的集合，H_c为硬币空间，由$|0\rangle$和$|1\rangle$张量而成。演化算符$U = S(I \times C)$，其中 $\boldsymbol{C}$ 为硬币抛掷算符，其矩阵形式如下所示：

$$\boldsymbol{C} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \tag{1}$$

将 $\boldsymbol{C}$ 作用于H_c，移位算符 S 根据硬币的投掷结果作用于H_p，S 的作用效果描述为当硬币态为$|0\rangle$时，粒子向右移动，当硬币态为$|1\rangle$时，粒子向左移动。本文使用的 AQW 如图 1 所示，将位置态拓展为 x、y 两个方向的二维平面，并依次在这两个方向上交替行走。

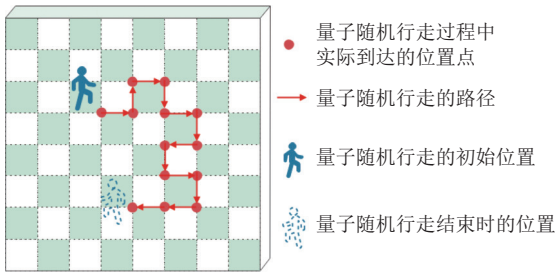

图 1 量子随机行走示意图

此时的演化算符$U=S_y(I\times C)S_x(I\times C)$，其中$S_y$为：

$$S_y=\sum_{x,y}^{N}|x,(y+1)\ \bmod\ N,0\rangle\langle x,y,0|+$$

$$|x,(y-1)\ \bmod\ N,1\rangle\langle x,y,1| \tag{2}$$

S_x表示 x 轴方向上的移位算符，与上式同理，设行走粒子的初始状态为$|\Psi_0\rangle$，则经过 t 步随机行走后，整个系统的状态$|\Psi_0\rangle=U^t|\Psi_0\rangle$，在坐标 (x,y) 处找到该粒子的概率为：

$$P=\left|\langle x,y,0|U^t|\Psi_0\rangle\right|^2+\left|\langle x,y,1|U^t|\Psi_0\rangle\right|^2$$

1.2　NCQI 表示

NCQI 是通用量子图像表示 NEQR 的改进，通过对彩色图像的（R,G,B）三通道分别进行 NEQR 表示，其中（R,G,B）分别表示红绿蓝三基色，这样 NCQI 模型就可以处理 24 位的彩色图像。一个$2^n\times2^n$的彩色图像，其所需的量子比特为（$2n$+24）个，整幅图像可以表示为：

$$|I\rangle=\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\left|C_{yx}\right\rangle\otimes|yx\rangle=$$

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\left|R_{yx}\right\rangle\left|G_{yx}\right\rangle\left|B_{yx}\right\rangle\otimes|yx\rangle \tag{3}$$

其中$\left|C_{yx}\right\rangle$存储了$|yx\rangle$处像素的颜色信息，并由 R, G, B 三通道进行灰度值存储。将图 2 用 NCQI 模型表示为：

$$\begin{aligned}|I\rangle=\frac{1}{2^n}(&|11111111\ 11011111\ 11010000\rangle\otimes|0...0\ 0...0\rangle+\\&|11110010\ 10110100\ 10100001\rangle\otimes|0...0\ 0...1\rangle+\\&|11100100\ 11010101\ 10110001\rangle\otimes|0...1\ 0...0\rangle+\\&|11110000\ 10111101\ 10101101\rangle\otimes|0...1\ 0...1\rangle+...)\end{aligned}$$

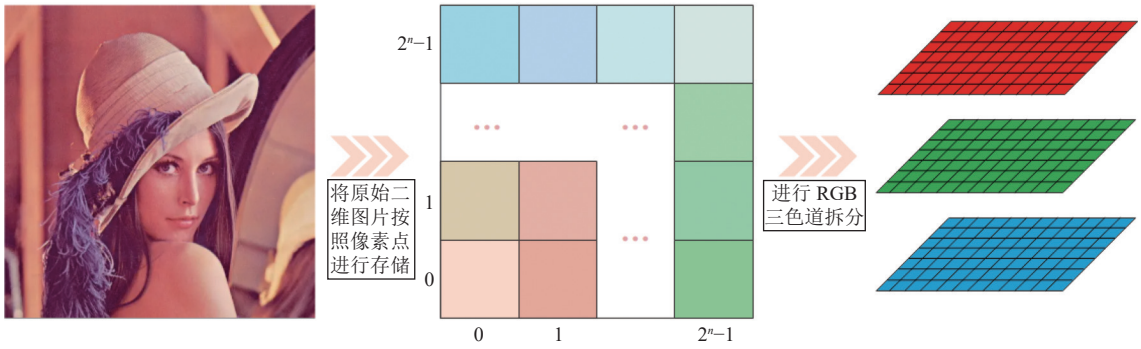

图 2　将二维彩色图像进行 RGB 三通道拆分

1.3　量子异或操作

为了对整个量子图像实行量子异或 XOR 操作，需要将其分为2^{2n}个子操作K_{yx}，每一个子操作对一个具体的像素值进行异或操作，整个子异或操作用一个跟图像相同大小的矩阵 $\boldsymbol{K}$ 表示为：

$$\boldsymbol{K}=\begin{pmatrix}K_{0\,1}&\cdots&K_{0\,2^n-1}\\\vdots&&\vdots\\K_{2^n-1\,0}&\cdots&K_{2^n-1\,2^n-1}\end{pmatrix} \tag{4}$$

式中，$k_{yx}=m_{yx}^0m_{yx}^1m_{yx}^2m_{yx}^3,\cdots,m_{yx}^{23},m_{yx}^i\in0,1$，并根据$k_{ij}$生成量子门操作序列 $\boldsymbol{B}$：

$$\boldsymbol{B}=\begin{pmatrix}B_{0\,1}&\cdots&B_{0\,2^n-1}\\\vdots&&\vdots\\B_{2^n-1\,0}&\cdots&B_{2^n-1\,2^n-1}\end{pmatrix} \tag{5}$$

式中，$B_{yx}=T_{yx}^0T_{yx}^1\cdots T_{yx}^{23}$，其中$T_{yx}^i=\begin{cases}X & m_{yx}^i=1\\ I & m_{yx}^i=0\end{cases}$，当$m_{yx}^i=1$时，表示对像素序列$|C_{YX}\rangle$中的第 i+1 个量子比特实行 X 门操作；当$m_{yx}^i=0$时，对像素序列$|C_{YX}\rangle$中的第 i+1 个量子比特实行 I 门操作。X 门与 I 门的矩阵形式如下所示：

$$\sigma_X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \sigma_I=\begin{pmatrix}1&0\\0&1\end{pmatrix} \tag{6}$$

将 B_{yx}作用于该图处于 $g(y,x)$处像素 $|g(y,x)\rangle$时，有$B_{yx}|g(Y,X)\rangle=B_{YX}\otimes_{i=1}^{24}|C_{YX}\rangle=\otimes_{i=1}^{24}\left|C_{YX}^i\oplus m_{YX}^i\right\rangle=|f(Y,X)\rangle$，其中$|f(Y,X)\rangle$表示的是进行像素置乱之后的新像素值。把 B 作用到整个图像，此时有：

$$B|I\rangle=\prod_{x=0}^{2^n-1}\prod_{y=0}^{2^n-1}B_{yx}|I\rangle=\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\otimes_{i=0}^{23}\left|C_{yx}^i\oplus m_{yx}^i\right\rangle|yx\rangle=$$

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|f(y,x)\rangle|yx\rangle \tag{7}$$

1.4　基础量子门线路

由两个量子比特构成的量子或门∪、量子与门∩，其作用效果如图 3 所示，线路中使用了交换门

与 Toffoli 门以及一个辅助量子比特。

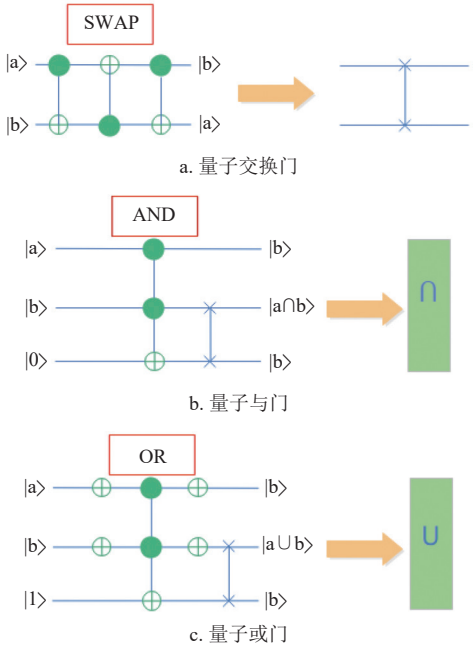

图 3 双量子比特与门和或门

2 量子图像加密与解密模型

本文提出了一种基于 AQW 与量子异或操作的量子彩色图像加密模型，在本模型中，首先对一幅彩色图像进行 RGB 三通道拆分，并构建量子线路以 NCQI 模型存储于量子计算机中，得到量子图像，再根据双方事先约定好的密钥进行 AQW，同时构建量子异或线路，完成对图像的加密操作，解密方案是加密方案的逆过程，本方案的加密流程如图 4 所示。

2.1 彩色量子图像的制备

在对彩色量子图像进行操作之前，需要先将其存储于量子计算机上，用 24+2n 个量子比特存储一幅$2^n\times 2^n$大小的图片，首先将它们初始化为$|0\rangle$态，即$|\varphi_0\rangle=|0\rangle^{\otimes 24+2n}$，使用 Hadamard 门和恒等门 I 分别作用于初始态中表示位置与像素的量子比特，此时得到一个空白量子图像$|\varphi_1\rangle$：

$$|\varphi_1\rangle=(I|0\rangle)^{\otimes 24}\otimes(H|0\rangle)^{\otimes 2n} \tag{8}$$

接着对$|\varphi_1\rangle$设置颜色信息，因为一共有2^{2n}个颜色需要设置，所以整个步骤可以划分为2^{2n}个子操作，对于(Y,X)处颜色，量子操作w_{YX}为：

$$w_{YX}=\left(I\otimes\sum_{y=0}^{2^n-1}\sum_{\substack{x=0\\(yx)\neq YX}}^{2^n-1}|yx\rangle\langle yx|\right)+\Omega_{YX}\otimes|YX\rangle\langle YX| \tag{9}$$

式中，$\Omega_{YX}=\otimes_{i=0}^{23}\Omega_{YX}^{i}$，$\Omega_{YX}^{i}$的作用效果是设置$(Y,X)$处表示颜色信息的第 i 个比特位的值，即：

$$\Omega_{YX}^{i}:\left|0\oplus C_{YX}^{i}\right\rangle \tag{10}$$

将w_{YX}作用于$|\varphi_1\rangle$，设置(Y,X)位置的颜色值：

$$\begin{aligned}
&w_{yx}|\varphi_1\rangle=\\
&w_{YX}\left(\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|0\rangle^{\otimes 24}|yx\rangle\right)=\\
&\frac{1}{2^n}w_{YX}\left(\sum_{\substack{y=0\\(yx)\neq(YX)}}^{2^n-1}\sum_{x=0}^{2^n-1}|0\rangle^{\otimes 24}|yx\rangle+|0\rangle^{\otimes 24}|YX\rangle\right)=\\
&\frac{1}{2^n}\left(\sum_{\substack{y=0\\(yx)\neq(YX)}}^{2^n-1}\sum_{x=0}^{2^n-1}|0\rangle^{\otimes 24}|yx\rangle+\Omega_{YX}|0\rangle^{\otimes 24}|YX\rangle\right)=\\
&\frac{1}{2^n}\left(\sum_{\substack{y=0\\(yx)\neq(YX)}}^{2^n-1}\sum_{x=0}^{2^n-1}|0\rangle^{\otimes 24}|yx\rangle+\otimes_{i=0}^{23}|C_{YX}|YX\rangle\right)
\end{aligned} \tag{11}$$

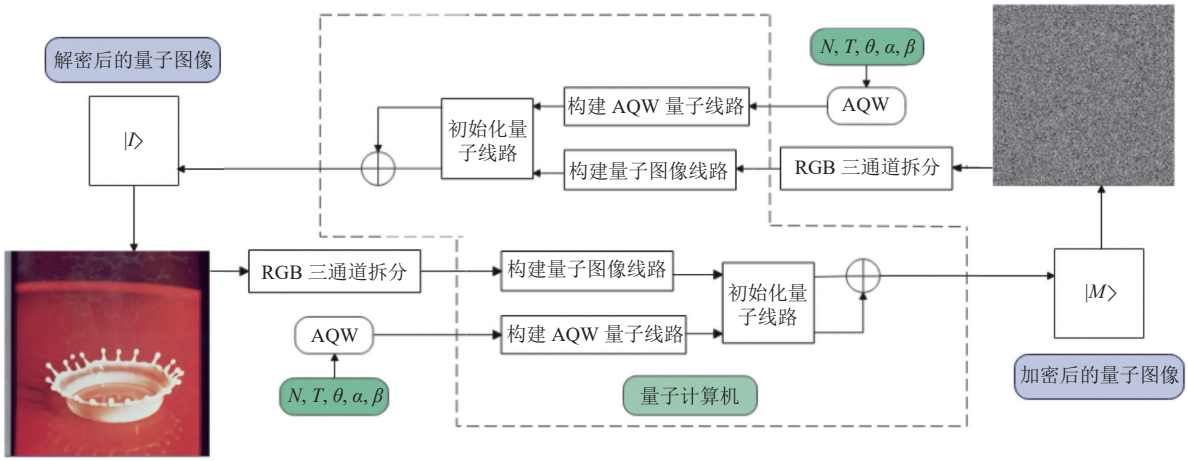

图 4 量子图像加密与解密模型

最终对中间态$|\varphi_1\rangle$执行2^{2n}次w_{YX}操作后，将原始空白量子图像像素值都设置为所需值，得到了彩色量子图像$|\phi_2\rangle$为：

$$w|\varphi_1\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\Omega_{YX}|0\rangle^{\otimes 24}|YX\rangle=$$

$$\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=0}^{23}\left|C_{YX}^{i}\right\rangle|YX\rangle=|\varphi_2\rangle \tag{12}$$

把图 2 所示的彩色图像存储于量子计算机中，其制备线路如图 5 所示。

2.2　量子异或线路

利用 1.4 节中的几个简单量子线路，可以将其扩展并设计两个二值矩阵的量子异或门线路，如图 6 所示，其中C_{YX}^{AQW}表示通过 AQW 二值矩阵构建的量子线路中的颜色信息，C_{YX}为根据原始图像构建的量子线路中的颜色信息。

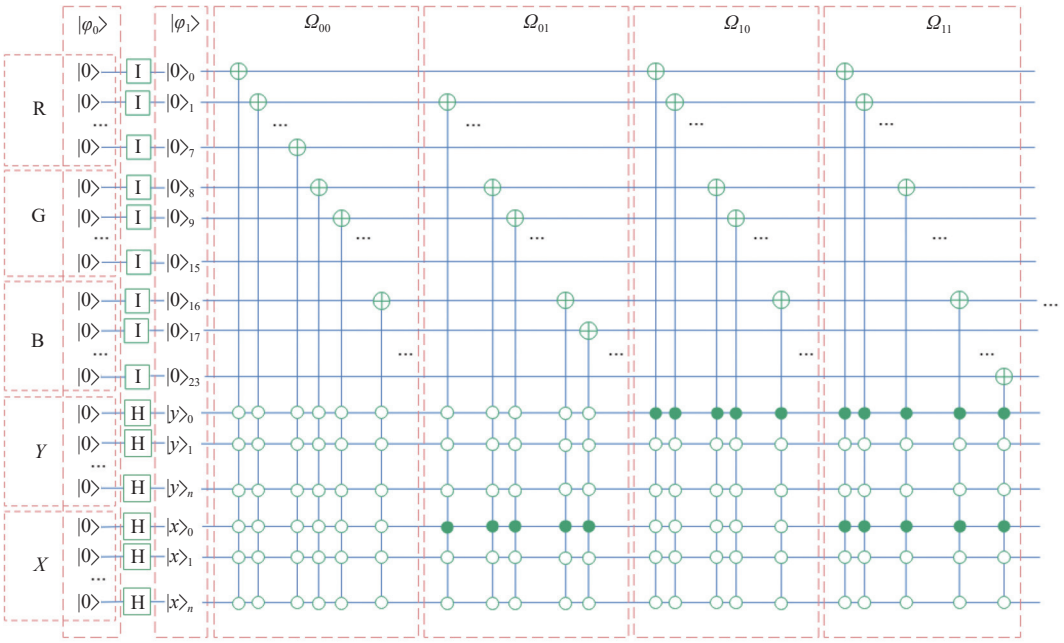

图 5　量子彩色图像制备线路

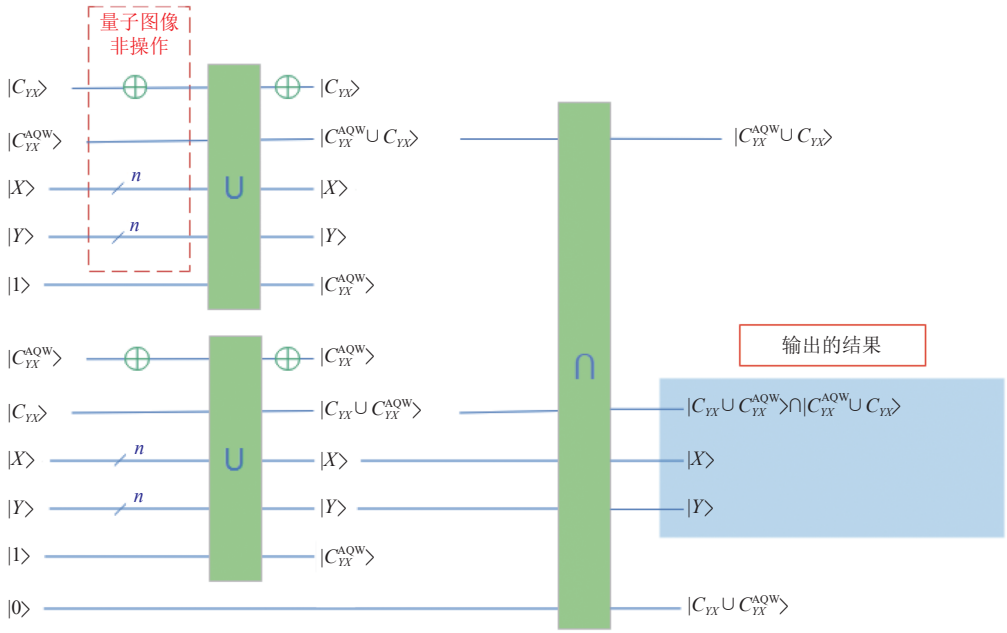

图 6　两个二值矩阵的量子异或门线路

2.3 量子图像加密模型

本文将原始像素矩阵$I_0(M\times N)$拆分成三通道像素矩阵$\boldsymbol{R}_0(M\times N)$，$\boldsymbol{G}_0(M\times N)$，$\boldsymbol{B}_0(M\times N)$，并根据上文内容，以 NCQI 模型存入量子计算机中，得到$|I\rangle=\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\left|C_{yx}\right\rangle\otimes|yx\rangle$。

1）选择 AQW 的一组参数$(N,T,\theta,\alpha,\beta)$，其中$N$表示控制概率矩阵的大小，$T$表示行走的次数，也是执行 U 操作的次数，$\theta$控制硬币算子$C$，$(\alpha,\beta)$是硬币初始态的参数，并作为图像加密的密钥提前分发给通信双方。

2）粒子在$N\times N$大小的空间里，沿xy两个方向依次行走T步之后，根据其在每一点出现的概率生成 AQW 概率矩阵$\boldsymbol{P}$，并调整其大小为对应的加密图像大小$2^n\times 2^n$，即：

$$P_1=\text{resize}(\boldsymbol{P},[2^n\times 2^n])$$

3）转换P_1中每一个元素的值，使之变成 0～255 之间的整数：

$$P_{yx}^{*}=(P_{yx}\times 10^{12})\bmod 256$$

4）将P_{yx}^{*}中元素转换成 8 位二进制，不足 8 位的高位补零，假设 p*$_{00}$=26，转换成二进制后为 11010，高位补零到八位，转换成 00011010，待所有元素转换后生成矩阵$\boldsymbol{K}_{YX}=\begin{pmatrix}k_{00}&\cdots&k_{02^n-1}\\ \vdots&&\vdots\\ k_{2^n-1}&\cdots&k_{2^n-12^n-1}\end{pmatrix}$，其中$k_{yx}=m_{yx}^0m_{yx}^1m_{yx}^2\cdots m_{yx}^{23}$，$m_{yx}^i\in 0,1$是$p_{yx}$的二进制表示，$x$与$y$分别表示矩阵中对应的位置关系。

5）根据矩阵$\boldsymbol{K}_{YX}$，生成量子异或操作矩阵$\boldsymbol{B}_{YX}$，与k_{yx}同理，$b_{yx}=T_{yx}^0T_{yx}^1T_{yx}^2\cdots T_{yx}^{23}$，其中$T_{yx}^0\sim T_{yx}^7$控制的是量子线路中的 R 通道，$T_{yx}^8\sim T_{yx}^{15}$控制的是 G 通道，$T_{yx}^{16}\sim T_{yx}^{23}$控制的是 B 通道，$T_{yx}^i=\begin{cases}X,m_{yx}^i=1\\ I,m_{yx}^i=0\end{cases}$。

6）根据量子异或操作矩阵$\boldsymbol{B}_{YX}$，对$|I$进行置乱，得到加密后的量子图像$|M\rangle$为：

$$\begin{aligned}&B_{YX}|I\rangle=\\ &\prod_{x=0}^{2^n-1}\prod_{y=0}^{2^n-1}b_{yx}|I\rangle=\\ &\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\otimes_{i=0}^{23}\left|C_{yx}^i\oplus m_{yx}^i\right\rangle|yx\rangle=\\ &\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|f(y,x)\rangle|yx\rangle=|M\rangle\end{aligned}\tag{13}$$

2.4 量子图像解密模型

解密算法是加密算法的逆过程，由于密钥提前已经发送给了通信双方，此时根据相同的 AQW 参数，将生成相同的 AQW 概率矩阵，重复加密过程中的步骤 1）～步骤 5），将得到量子异或操作矩阵$\boldsymbol{B}_{yx}$。

由矩阵$\boldsymbol{B}_{yx}$对加密后的量子图像$|M\rangle$进行解密，得到原始量子图像$|I\rangle$：

$$\begin{aligned}&B_{YX}|M\rangle=\prod_{x=0}^{2^n-1}\prod_{y=0}^{2^n-1}b_{yx}|M\rangle=\\ &\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\otimes_{i=0}^{23}\left|C_{yx}^i\oplus m_{yx}^i\oplus m_{yx}^i\right\rangle|yx\rangle=\\ &\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\otimes_{i=0}^{23}\left|C_{yx}^i\right\rangle|yx\rangle=\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|g(y,x)\rangle|yx\rangle=|I\rangle\end{aligned}\tag{14}$$

3 实验仿真与结果分析

本文选择 512×512 大小的图像进行实验，所需要的量子比特数量为 103 个，且处于相干时间无限长，保真度百分之百的理想状态下，现有的量子计算机无法满足实验需要，所以本实验将在经典计算机上使用 pycharm 软件通过模拟仿真实现。在经典计算机中，将量子图像转换成像素矩阵，异或操作转换成酉矩阵，H 门与 I 门也用相应的酉矩阵进行替代。对 3 幅相同大小的彩色图像进行三通道拆分后，分别与生成的 AQW 概率矩阵进行加密与解密，从图 7 的仿真结果可知，密文图像呈现随机噪声形式，解密图像与原始图像完全相同。

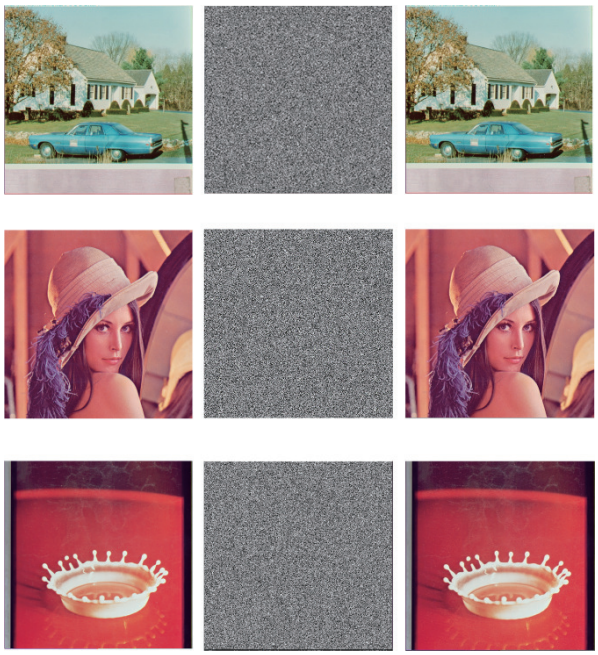

图 7 加密与解密效果图

3.1　信息分析

信息分析一般包括相邻像素相关性分析与直方图分析，是攻击者可以通过对获取到的密文信息进行统计分析，从而得到明文图像的方法。

1）相邻像素相关性分析

对于图像而言，相邻像素点的像素值之间存在着很高的相关性，攻击者可以利用其中一个像素点的信息去预测周围像素点的像素值，从而破解整个或部分图像信息，相关系数计算公式为：

$$\delta_{yx}=\frac{\operatorname{cov}(y,x)}{\sqrt{D(y)}\sqrt{D(x)}} \tag{15}$$

式中，y、x 为相邻的两个像素；$\operatorname{cov}(y,x)$为协方差公式，$\operatorname{cov}(y,x)=\frac{1}{N}\sum_{i=0}^{N-1}(y_i-E(y))(x_i-E(x))$，$N$ 为图像大小，$E(x)$为均值；$D(y)=\frac{1}{N}\sum_{i=0}^{N-1}(x_i-E(x))^2$方差，其值越接近 1，表明像素值之间的相关性越强，越接近 0，表明相关性越弱。实验结果如图 8～图 10 所示。

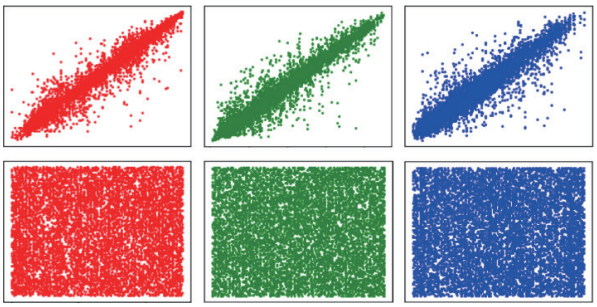

图 8　汽车图像加密前后相关性分析

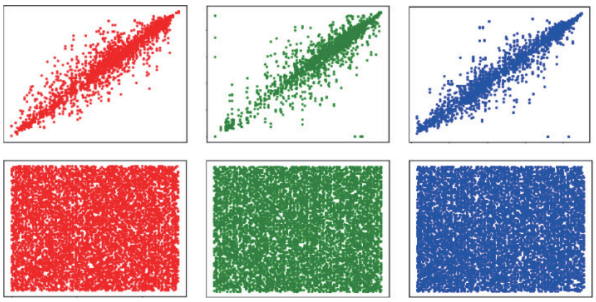

图 9　Lena 图像加密前后相关性分析

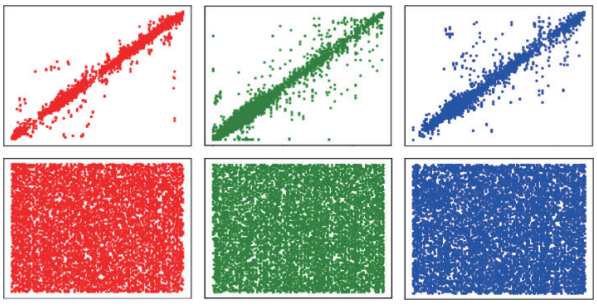

图 10　水波图像加密前后相关性分析

2）直方图分析

直方图分析反映了整个像素图像中各个像素值相对于其他像素值的分布情况，原始图像的直方图如图 11 所示，表现出明显的统计学规律，加密后的直方图分布越均匀，则方差越小，表明加密算法对像素的置乱越显著，抵御攻击者统计分析攻击的能力越强。实验结果表明，加密后的直方图像素均匀分布，具有良好的加密效果。

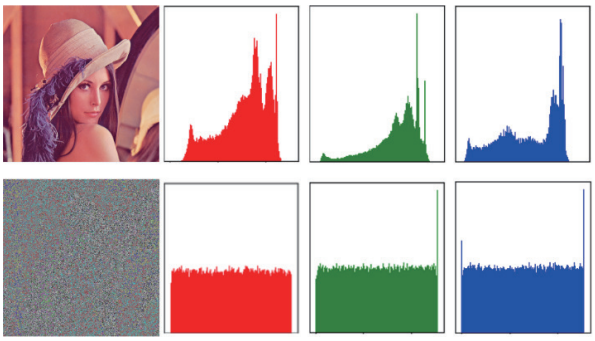

图 11　Lena 图像加密前后直方图分析

3.2　暴力攻击

1）对于一个理想的图像加密算法，密钥中一个微小的改变应该对加密结果产生完全不同的效果，通常用像素变化率 NPCR 和统一平均变化强度 UACI 来评估不同密钥对图像加密的影响，计算公式如下：

$$\mathrm{NPCR}=\frac{\sum_{y,x}D(y,x)}{M\times N}\times 100\%$$

$$\mathrm{UACI}=\frac{1}{M\times N}\frac{\sum_{y,x}(g_1(y,x)-g_2(y,x))}{255}\times 100\%$$

式中，$D(y,x)=\begin{cases}1 & g_1(y,x)\neq g_2(y,x)\\ 0 & g_1(y,x)=g_2(y,x)\end{cases}$，NPCR 和UACI 的理想值应为 99.609 4% 和 33.463 5%。本实验采用的两组密钥，分别为$(\frac{\pi}{3},\frac{\pi}{2})$，$(\frac{\pi}{3}-10^{-11},\frac{\pi}{2})$，实验结果如表 1 所示。

表 1　测试图片 NPCR 与 UACI 结果　%

基色	车		Lena		水波	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
R	99.592 0	33.453 6	99.588 9	33.603 3	99.606 4	33.489 4
G	99.593 0	33.478 1	99.596 4	33.494 1	99.599 9	33.383 3
B	99.598 2	33.504 90	99.586 1	33.436 9	99.595 8	33.385 7

接下来给出本算法与文献 [21,23,36] 的比较结

果，如表 2 所示。

表 2 几种方法的 NPCR 与 UACI 数据对比 %

算法	NPCR平均值	UACI平均值
本文	99.595 1	33.469 9
文献[21]	99.625 7	33.483 5
文献[23]	99.598 6	33.447 7
文献[36]	99.605 0	—

2）熵是用来度量事物复杂度的物理量，对于安全性分析来说是一个重要参考指标，如果其信息熵的值趋近于 8，则表明其像素扩散随机性好，应对统计攻击的能力强。信息熵的计算公式为：

$$H(\partial)=-\sum_{i=0}^{N-1}P(\partial_i)\log_2 P(\partial_i) \tag{16}$$

式中，∂_i表示∂点像素的灰度值；$P(\partial_i)$是灰度值∂_i出现的概率，计算结果如表 3 所示。

表 3 测试图片信息熵

基色	车	Lena	水波
R	7.998	7.998	7.997
G	7.998	7.998	7.998
B	7.998	7.998	7.997

4 结 束 语

本文提出的基于量子随机行走与异或操作的量子图像加密模型，防止了攻击者通过已知的明文部分和对应的密文对整个图像进行破译。本文模型可以安全地传输量子图像。虽然在现有技术下无法对量子图像进行直接操作，但是在模拟仿真中证明了本文技术思路的有效性与安全性，展示了量子图像处理技术的广阔应用前景。

参 考 文 献

[1] 张语桐. 网络通信安全中图像加密算法的研究[D]. 哈尔滨: 东北林业大学, 2015.
ZHANG Y T. The study of image encryption algorithm on network communication security[D]. Harbin: Northeast Forestry University, 2015

[2] 吴玲玲, 张建伟, 葛琪. Arnold 变换及其逆变换[J]. 微计算机信息, 2010, 26(14): 206-208.
WU L L, ZHANG J W, GE Q. Arnold transformation algorithm and anti-arnold transformation algorithm[J]. Microcomputer Information, 2010, 26(14): 206-208.

[3] 孙光民, 王皓. 基于魔方密码的图像加密解密技术[J]. 北京工业大学学报, 2021, 47(8): 833-841.
SUN G M, WANG H. Image encryption and decryption technology based on rubik's cube and dynamic password[J]. Journal of Beijing University of Technology, 2021, 47(8): 833-841.

[4] MATTHEWS R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

[5] BARIK R C, CHANGDER S. Perceptual accessible image encryption scheme conjugating multiple chaotic maps[J]. IET Image Processing, 2020, 14(11): 2457-2468.

[6] 迈克尔, 尼尔森, 艾萨克, 等. 量子计算和量子信息: 量子计算[M]. 赵千川, 译. 北京: 清华大学出版社, 2004.
MICHAEL A N, CHUANG I L. Quantum computing and quantum information: Quantum computing[M]. translated by ZHAO Q C. Beijing: Tsinghua University Press, 2004.

[7] SHOR P. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th Annual Symposium on Foundations of Computer Science. [S.l.]: IEEE Press, 1994: 124-134.

[8] GROVER L K. A fast quantum mechanical algorithm for database search[C]//Proceedings of the 28th Annual ACM Symposium on Theory of Computing. [S.l.]: ACM Press, 1996: 212-219.

[9] 姜瑶瑶, 张文彬, 初鹏程, 等. 基于置换群的多粒子环上量子行走的反馈搜索算法[J]. 物理学报, 2022, 71(3): 7-17.
JIANG Y Y, ZHANG W B, CHU P C, et al. Feedback search algorithm for multi-particle quantum walks over a ring based on permutation groups[J]. Acta Physica Sinca, 2022, 71(3): 7-17.

[10] WANG H W, XUE Y J, MA Y L, et al. Determination of quantum toric error correction code threshold using convolutional neural network decoders[J]. Chinese Physics B, 2022, 31(1): 170-176.

[11] 贺振兴, 范兴奎, 初鹏程, 等. 基于 Cayley 图上量子漫步的匿名通信方案[J]. 物理学报, 2020, 69(16): 47-55.
HE Z X, FAN X K, CHU P C, et al. Anonymous communication scheme based on quantum walk on Cayley graph[J]. Acta Physica Sinca, 2020, 69(16): 47-55.

[12] CHEN Z Y, QIU T H, ZHANG W B, et al. Effects of initial states on the quantum correlations in the generalized Grover search algorithm[J]. Chinese Physics B, 2021, 30(8): 161-168.

[13] AHARONOV Y, DAVIDOVICH L, ZAGURY N. Quantum random walks[J]. Physical Review A, 1993, 48(2): 1687.

[14] FARHI E, GUTMANN S. Quantum computation and decision trees[J]. Physical Review A, 1997, 58(2): 915-928.

[15] WATROUS J. Quantum simulations of classical random walks and undirected graph connectivity[J]. Journal of Computer & System Sciences, 2001, 62(2): 376-391.

[16] ANDRIS A, JULIA K, ALEXANDER R. Coins make quantum walks faster[C]//Proceedings of the 16th Annual ACM-SIAM Symposium on Discrete Algorithms. [S.l.]: ACM Press, 2005: 1099-1108.

[17] BRUN T A, CARTERET H A, AMBAINIS A. Quantum random walks with decoherent coins[J]. Physical Review A, 2003, 67(3): 2304-2304.

[18] DORIT A, ANDRIS A, JULIA K, et al. Quantum walks

on graphs[C]//Proceedings of ACM Symposium on Theory of Computation. [S.l.]: ACM Press, 2001: 50-59.

[19] BRUN T A, CARTERET H A, AMBAINIS A. Quantum Walks driven by many coins[J]. Physical Review A, 2002, 67(5): 2317-2318.

[20] QIANG X, YANG X, WU J, et al. An enhanced classical approach to graph isomorphism using continuous-time quantum walk[J]. Journal of Physics A Mathematical General, 2012, 45(4): 119-156.

[21] 王一诺, 宋昭阳, 马玉林. 基于 DNA 编码与交替量子随机行走的彩色图像加密算法[J]. 物理学报, 2021, 70(23): 115-124.
WANG Y N, SONG Z Y, MA Y L. Color image encryption algorithm based on DNA code and alternating quantum random walk[J]. Acta Physica Sinca, 2021, 70(23): 115-124.

[22] MA Y, LI N, ZHANG W, et al. Image encryption scheme based on alternate quantum walks and discrete cosine transform[J]. Optics Express, 2021, 29: 28338-28351.

[23] 刘瀚扬, 华南, 王一诺, 等. 基于量子随机行走和多维混沌的三维图像加密算法[J]. 物理学报, 2022, 71(17): 30-45.
LIU H Y, HUA N, WANG Y N, et al. Three dimensional image encryption algorithm based on quantum random walk and multidimensional chaos[J]. Acta Physica Sinca, 2022, 71(17): 30-45.

[24] VLASOV A Y. Quantum computations and images recognition[EB/OL]. [2022-07-25]. https://arxiv.org/abs/quant-ph/9703010.

[25] BEACH G, LOMONT C, COHEN C. Quantum image processing (QuIP)[C]//32nd Applied Imagery Pattern Recognition Workshop (AIPR 2003). [S.l.]: IEEE Press, 2004: 39-44.

[26] LATORRE J I. Image compression and entanglement[J]. Computer Science, 2005, 10(31): 294-298.

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

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

[29] 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.

[30] SANG J, WANG S, LI Q. A novel quantum representation of color digital images[J]. Quantum Information Processing, 2017, 16(2): 42-56.

[31] le PHUC Q, ILIYASU A M, DONG F Y. Fast geometric transformations on quantum images[J]. IAENG International Journal of Applied Mathematics, 2010, 40(3): 2-5.

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

[33] WANG J, JIANG N, WANG L. Quantum image translation[J]. Quantum Information Processing, 2014, 14(5): 1-16.

[34] XU P, HE Z, QIU T, et al. Quantum image processing algorithm using edge extraction based on Kirsch operator[J]. Optics Express, 2020, 28(9): 12508-12517.

[35] 李丹, 燕婷, 郭瑞. 基于交替量子漫步的量子彩色图像加密算法[J]. 信息网络安全, 2021, 21(6): 45-51.
LI D, YAN T, GUO R. Quantum color image encryption algorithm based on alternating quantum walk[J]. Netinfo Security, 2021, 21(6): 45-51.

[36] 张健, 霍达. 基于混沌系统的量子彩色图像加密算法[J]. 西南交通大学学报, 2019, 54(2): 421-427.
ZHANG J, HUO D. Quantum colour image encryption algorithm based on chaotic systems[J]. Journal of Southwest Jiaotong University, 2019, 54(2): 421-427.

编　辑　税　红