# 基于Hopfield网络“伪吸引子”与交替量子随机行走的抗攻击彩色图像加密方案

宋昭阳[1],王一诺[2],王浩文[1],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. 青岛理工大学信息与控制工程学院,山东青岛 266520)

**摘 要:** 近年来,图像信息的安全传输已成为互联网领域的重要研究课题. 本文提出了一种将Hopfield网络伪吸引子特性与交替量子随机行走概率分布矩阵相结合的抗攻击彩色图像加密方案. 研究发现,若控制Hopfield网络状态矩阵的精度参数,将交替量子随机行走产生的概率分布矩阵4分块中的1个子块$\boldsymbol{M}_1$作为伪随机数矩阵参与加密,Hopfield网络的训练矩阵与输入矩阵分别为矩阵$\boldsymbol{M}_1$的4分块中的2个对角子块之一时,能产生伪吸引子. 该伪吸引子的矩阵形式通过张量运算、进制转换等处理后,能作为密钥矩阵对原始图像进行基于空间域上的像素值排序自适应置乱以及元素数值的混淆,生成加密图像. 其中,密钥矩阵是图像加密中的关键部分,具备优异统计学属性的密钥矩阵能极大的提高图像加密的效果. 本文所提加密方案在统计学特性测试中,实现了平均信息熵为7.999 4,像素数改变率的平均值为99.621 8%,统一平均变化强度的平均值为33.537 9%,平均相关性为0.003 9等. 同时本文还对所提加密方案进行了各种噪声模拟测试以验证其实际应用中遇到常见噪声及攻击干扰情况下的鲁棒性.

**关键词:** 信息安全;图像加密;神经网络;Hopfield网络;量子随机行走

**基金项目:** 国家自然科学基金(No.11975132);山东省自然科学基金(No.ZR2021MF049,No.ZR2019YQ01);山东省自然科学基金联合基金(No.ZR202108020011)

**中图分类号:** TP309.7;TN919.81 **文献标识码:** A **文章编号:** 0372-2112(2023)08-2030-13

**电子学报URL:**http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211391

# Anti-Attack Color Image Encryption Scheme Based on Hopfield Network “Pseudo Attractor” and Alternating Quantum Random Walk

SONG Zhao-yang[1], WANG Yi-nuo[2], WANG Hao-wen[1], MA Hong-yang[2]
(1. *School of Information and Control Engineering*, *Qingdao University of Technology*, *Qingdao*, *Shandong* 266520, *China*;
2. *School of Science*, *Qingdao University of Technology*, *Qingdao*, *Shandong* 266520, *China*)

**Abstract:** The secure transmission of image information has attracted wide attention in the field of the Internet in recent years. We propose an attack-resistant color image encryption scheme that combines the pseudo-attractor property of Hopfield network with the probability distribution matrix of alternating quantum random walk. We find that by controlling the accuracy parameters of the Hopfield network state matrix, one sub-block $\boldsymbol{M}_1$ of the 4-block probability distribution matrices generated by the alternating quantum random walk is involved in the encryption as a pseudo-random number matrix. And when the training matrix and the input matrix of Hopfield network are one of the 2 diagonal sub-blocks of the 4-block matrix $\boldsymbol{M}_1$, respectively, the pseudo-attractor can be generated. The matrix form of this pseudo-attractor, after processing by tensor calculation and binary conversion, can be used as a key matrix to generate an encrypted image based on adaptive permutation of pixel value ordering on the spatial domain and confusion of element values for the original image. The key matrix is a critical part of image encryption, and a key matrix with excellent statistical properties can obviously improve the effectiveness of image encryption. In the statistical characteristic test, the encryption scheme proposed in this paper achieves an average information entropy of 7.999 4, an average value of 99.621 8% of the number of pixels changed rate (NPCR), an average of 33.537 9% of the uniform average change intensity (UACI), and an average correlation decreases to 0.003 9. Our encryption scheme is also tested in the presence of various noise simulations to verify its robustness against common noise and attack interference in practical applications.

收稿日期:2021-10-12;修回日期:2022-05-25;责任编辑:孙瑶

Key words: information security; image encryption; neural network; Hopfield network; quantum random walk
Foundation Item(s): National Natural Science Foundation of China (No.11975132); Natural Science Foundation of Shandong Province of China (No.ZR2021MF049, No.ZR2019YQ01, No.ZR202108020011)

## 1 引言

神经密码学作为计算机科学与密码学的交叉学科,主要研究结合神经网络的加密方案,由Lauria最早提出[1]. 密码学中强调非线性变换的引入,而神经网络的一大明显特征便是非线性,同时因为神经网络相关领域理论与应用技术的日趋成熟,还使其具备以矩阵方式计算、海量的吞吐和超大规模的并行计算能力等新特性. 上述特性都为加密领域尤其是图像加密领域带来了新的思路与研究方向,使将神经网络应用于加密领域成为新的重点研究课题[2~5].

Hopfield网络[6,7],是Hopfield在伊辛模型的基础上于1982年提出的. Hopfield网络允许机器存储“记忆”,该网络类似于人类大脑处理信息的模式,能做到依靠残缺信息来“回忆”其完整的信息,其也被称为离散Hopfield网络(Discrete Hopfield Neutral Network, DHNN). 1984年,Hopfield又提出了连续Hopfield网络(Continues Hopfield Neutral Network,CHNN)[8]. 1990年,Bruck[9]研究了Hopfiled网络收敛条件,证明了在将Hebbian学习规则作为权重矩阵设计方法且矩阵对角线元素为0的前提下,DHNN将收敛到稳定状态. Weisbuch等人[10]和Storkey等人[11]研究了Hopfield网络的吸引子性质. Wuensche等人[12]研究了Hopfield网络的容量问题,并对容量不足时产生“错误联想记忆”的情况进行了理论上的解释.

将Hopfield网络运用到图像加密中的主要方式有三种. 第一种是将Hopfield网络用作伪随机数生成器. 如徐子同等人[13]借助三维的Hopfield网络生成伪随机数序列,并通过多次迭代进一步提高伪随机数序列的统计学特性后,对图像矩阵进行混淆处理;随后利用二次置乱算法对混淆后的图像矩阵进行扩散处理,完成原始图像的加密. 第二种是将Hopfield网络作为置乱矩阵. 如Wang等人[14]借助混沌系统演化生成的伪随机数序列,对原始图像矩阵进行混淆处理;同时借助Hopfield网络生成自扩散序列,对混淆后的图像矩阵进行扩散处理,完成对原始图像的加密. 第三种是前两者的结合,将Hopfield网络既用于伪随机数序列的生成又用作置乱矩阵. 如Lakshmi等人[15]借助Hopfield网络生成伪随机序列对图像矩阵进行数值混淆;之后再将Hopfield网络作为置乱矩阵,对混淆后的图像矩阵进行置乱,完成原始图像的加密.

量子计算,在Benioff[16]提出图灵机的量子力学模型后,于1980年建立了正式的理论模型. 量子计算借助量子态的特殊属性,如叠加、纠缠等来进行计算[17],被证实有潜力处理经典计算机在有效时间内无法实现的计算[18,19]. 但量子计算遵循“丘奇-图灵”命题,即不考虑时效性的前提下,经典计算机与量子计算机能完成的工作在理论上相同. 只是针对某些问题,运用量子算法[20~23]能够在时间复杂度上明显优于经典算法. 量子随机行走是典型的量子算法,是经典随机行走在量子领域的对应,最早由Aharonov等人[24]提出,包括连续时间量子随机行走[25]与离散时间量子随机行走[26]. Baryshnikov等人[27]研究了量子随机行走在二维与一维坐标空间中的区别,同时阐述了二维量子随机行走的优势与其独具的性质. Yang等人[28]研究了一维量子随机行走的特性并将其首次运用于量子图像加密. Abd等人[29]分析了二维量子随机行走概率分布矩阵的统计学特性,将其运用到图像加密中. 本文对仅借助量子随机行走概率分布矩阵进行图像加密的方案进行了统计学特性分析,包括相关性、直方图、信息熵等,发现其统计学特性并不能达到经典图像加密所需的标准. 但其具备伪随机生成器所需的初始条件极度敏感,状态空间无限等特性,当与其他加密技术结合进一步提升密钥的统计学特性时,便能达到满足统计学要求的加密效果[30].

本文借鉴了丁群等人[31]和Caporale等人[32]提出的加密方案,并创新性地提出一种将神经网络与量子算法相结合的彩色图像加密方案. 在本文方案中利用离散时间量子随机行走生成伪随机数序列矩阵,将其产生的概率分布矩阵4分块中的1个子块M1作为伪随机数矩阵参与加密. DHNN的训练矩阵与输入矩阵分别为矩阵M1的4分块中的2个对角子块之一时,该网络最终将收敛到伪吸引子上. 该伪吸引子的对应矩阵通过一系列的处理后便可以作为密钥矩阵来进行图像加密. 本文所提加密方案产生的密钥矩阵具备优良的统计学特性,在保证原始图像有效加密的同时,能有效降低算法图像加密过程的时间复杂度. 同时经过仿真与理论分析,我们认为本文所提方案具备抵抗如暴力攻击、明文攻击、噪声攻击、剪切攻击等常见攻击的能力.

## 2 相关工作

### 2.1 DHNN介绍

DHNN是一种多输入、含阈值的二值非线性动态系统. 其神经元的激励函数多为双极值函数或阶跃函数,神经元的取值为{–1, 1}或{0, 1}. 取值为0或–1表示当

前神经元处于抑制状态,取值为1表示当前神经元处于激活状态.DHNN为单层神经网络,其内的所有神经元节点均连接到同一网络其余神经元节点上,如图1所示.

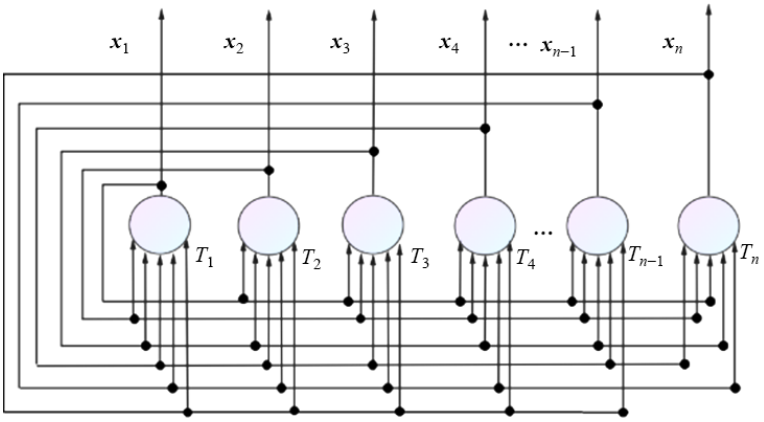


图1 DHNN的拓扑结构与工作方式

DHNN权重设计一般采用外积和法,借助Hebbian学习规则[32]提前训练得到,其核心公式为

$$\boldsymbol{W}=\sum_{p=1}^{P}\boldsymbol{X}^{p}\left(\boldsymbol{X}^{p}\right)^{\mathrm{T}} \tag{1}$$

此处$w_{ii}=0$即节点间无自反馈,该公式改写为

$$\boldsymbol{W}=\sum_{p=1}^{P}\left[\boldsymbol{X}^{p}\left(\boldsymbol{X}^{p}\right)^{\mathrm{T}}-\boldsymbol{I}\right] \tag{2}$$

其中,$\boldsymbol{I}$为单位矩阵,$\boldsymbol{X}$为系统状态.

DHNN中每个节点功能相同,单个节点的输出对应该节点的最终状态,用$x_i$表示,所有节点的状态构成网络的状态$\boldsymbol{X}=\left[x_1,x_2,x_3,x_4,\cdots,x_{n-1},x_n\right]^{\mathrm{T}}$.当DHNN得到来自外界的输入,便进入到激活状态.初始状态为

$$\boldsymbol{X}(0)=\left[x_1(0),x_2(0),x_3(0),\cdots,x_{n-1}(0),x_n(0)\right]^{\mathrm{T}} \tag{3}$$

该网络停止的条件为DHNN的各个神经元状态不再改变.

DHNN中转移函数多采用符号函数:

$$\begin{aligned}&x_i=\operatorname{sgn}\left(\theta_i\right)=\begin{cases}1, & \theta_i\geqslant 0\\ -1, & \theta_i<0\end{cases}\quad i=1,2,\cdots,n\\&\theta_i=\sum_{i=1}^{n}\left(w_{ij}x_i-T_i\right)\quad j=1,2,\cdots,n\end{aligned} \tag{4}$$

在本文中选取$T_i=0$.

DHNN的两种神经元状态演化模式分别是同步模式与异步模式.

异步模式:网络运行时每次只有一个神经元1按式(4)进行状态的调整计算,其他神经元的状态均保持不变,其神经元的变换规则为

$$x_{\mathrm{i}}(t+1)=\begin{cases}\operatorname{sgn}\left[\theta_i(t)\right], & i=j\\ x_i(t), & i\neq j\end{cases} \tag{5}$$

节点之间没有自反馈,构成一个完全图模型.当DHNN中处于抑制状态的神经元节点所受刺激超过设定阈值时将进入到激活状态,即出现从0或–1到1的跃迁.

同步模式:网络所有神经元同时调整,其神经元的变换规则为

$$x_{\mathrm{i}}(t+1)=\operatorname{sgn}\left[\ \theta_i(t)\right]\quad i=1,2,\cdots,n \tag{6}$$

DHNN能稳定状态是因为Hopfield将动力学中的能量函数$E$引入到该网络中.其工作模式为

$$\begin{aligned}&E(t)=-\frac{1}{2}\boldsymbol{X}^{\mathrm{T}}(t)\boldsymbol{W}\boldsymbol{X}(t)+\boldsymbol{X}^{\mathrm{T}}(t)T\\&\Delta E=\Delta E(t+1)-\Delta E(t)\end{aligned} \tag{7}$$

DHNN网络迭代过程中,能量会逐渐降低.当$\Delta E=0$时,系统的能量达到最低点,系统进入稳定状态.

## 2.2 DHNN网络吸引子与伪吸引子

考虑DHNN网络有$M$个样本输入时,$X^m$相互正交,$m=1,2,3,\cdots,M,x\in\left\{-1,1\right\}^n$,则

$$\left(\boldsymbol{X}^{m}\right)^{\mathrm{T}}\boldsymbol{X}^{k}=\begin{cases}0, & m\neq k\\ n, & m=k\end{cases} \tag{8}$$

$$\boldsymbol{W}\boldsymbol{X}^{k}=\sum_{m=1}^{m}\left[\boldsymbol{X}^{m}\left(\boldsymbol{X}^{m}\right)^{\mathrm{T}}-\boldsymbol{I}\right]\boldsymbol{X}^{k}=(n-M)\boldsymbol{X}^{k} \tag{9}$$

因为$n>M$,所以

$$\begin{aligned}&f\left(\boldsymbol{W}\boldsymbol{X}^{m}\right)=f\left[(n-M)\boldsymbol{X}^{m}\right]\\&=\operatorname{sgn}\left[(n-M)\boldsymbol{X}^{m}\right]=\boldsymbol{X}^{m}\end{aligned} \tag{10}$$

由式(10)可知,当给定样本$\boldsymbol{X}^m(m=1,2,3,\cdots,M)$便是其理想的吸引子并在周围产生一定的吸引域.实际中,给定样本实现正交的条件过于苛刻,因此会产生一些样本外的点也产生吸引域,这些点便被是Hopfied网络的伪吸引子[11].图2展示了输入状态经过迭代最终收敛到伪吸引子处达到稳态的演化过程,图3展示了DHNN中吸引子所对应的期望输出矩阵与伪吸引子所对应的实际输出矩阵的对比,并量化表示出DHNN迭代过程中能量函数的变化情况.

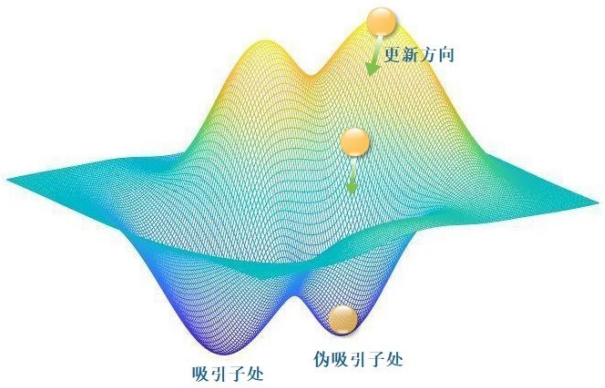


图2　DHNN中“能量”变化图

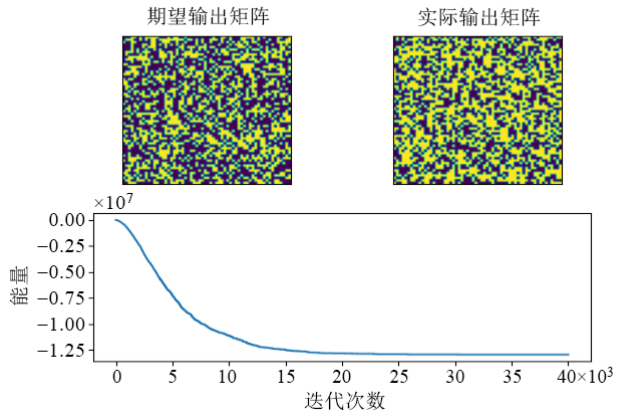


图3　DHNN吸引子与伪吸引子对比以及能量函数变化

### 2.3　量子随机行走

本文以离散时间量子随机行走为理论基础. 离散时间量子随机行走主要包含四个要素:行走者、行走者携带的硬币、硬币抛掷方式,以及行走规则.

一维离散时间量子随机行走由两部分构成,包括行走者位置空间$H_w$和硬币空间$H_c$. 二者构成量子随机行走体系的希尔伯特空间$\hat{H}=H_w\otimes H_c$. 在量子随机行走过程中,每一步的行走由相同的硬币抛掷算符$\hat{C}$决定:

$$\hat{C}=\begin{pmatrix}\cos\beta & \sin\beta\\ \sin\beta & -\cos\beta\end{pmatrix} \tag{11}$$

硬币抛掷完成后,行走者的动作由条件位移算符$S_i$规定:

$$S_i|x\rangle=\left|x+(-1)^c\right\rangle,\ c=0,1 \tag{12}$$

其中,$|x\rangle(x\in\mathbf{Z})$构成行走者位置空间的基矢;两个基矢$|c\rangle$线性组合构成硬币空间. 规定:当硬币态为$|0\rangle$时,操控行走者右移一个单位;当硬币态为$|1\rangle$时,操控行走者左移一个单位. 同时规定:

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}\quad |1\rangle=\begin{pmatrix}0\\1\end{pmatrix} \tag{13}$$

在本文所采用的交替量子随机行走中,通过硬币算符控制的行走者在任意选取的$x$和$y$两个垂直方向上交替行走,整个量子随机行走过程中的行走算符$\hat{U}$可描述为

$$\hat{U}=\hat{S}_y\left(I\otimes H_c\right)\hat{S}_x\left(I\otimes H_c\right) \tag{14}$$

其中,$\hat{S}_y$和$\hat{S}_x$为量子随机行走在$y$轴、$x$轴各点移动的位移算符:

$$\begin{aligned}\hat{S}_y=&\sum_{x,y}^{N}\left(\left|x,\left(y+1\right)\bmod N,0\right\rangle\left\langle x,y,0\right|\right)\\&+\sum_{x,y}^{N}\left(\left|x,\left(y-1\right)\bmod N,1\right\rangle\left\langle x,y,1\right|\right)\end{aligned} \tag{15}$$

$$\begin{aligned}\hat{S}_x=&\sum_{x,y}^{N}\left(\left|\left(x+1\right)\bmod N,y,0\right\rangle\left\langle x,y,0\right|\right)\\&+\sum_{x,y}^{N}\left(\left|\left(x-1\right)\bmod N,y,1\right\rangle\left\langle x,y,1\right|\right)\end{aligned} \tag{16}$$

假设初始时刻行走者所在位置为$\left(0_x,0_y\right)$,硬币处于叠加态$H_c=\cos\alpha|0\rangle+\sin\alpha|1\rangle$,则初始时刻系统状态为

$$\left|\psi_0\right\rangle=\left|\varphi_0\right\rangle_w\otimes\left(\cos\alpha|0\rangle+\sin\alpha|1\rangle\right)_c \tag{17}$$

则进行$T$步行走后系统状态可表示为

$$\left|\psi_T\right\rangle=\hat{U}^T\left|\psi_0\right\rangle \tag{18}$$

## 3　算法分析

### 3.1　加密过程

#### 3.1.1　制备量子随机行走概率分布矩阵

**步骤1**:生成伪随机数矩阵. 由于本文采用交替量子随机行走生成概率分布矩阵,矩阵中对应元素数据为行走者出现在该位置坐标$\left(x_x,y_y\right)$的概率$P(x,y,T)$,由上文可以推知:

$$P(x,y,T)=\left|\left\langle x,y,0\right|\hat{U}^T\left|\psi_0\right\rangle\right|^2+\left|\left\langle x,y,1\right|\hat{U}^T\left|\psi_0\right\rangle\right|^2 \tag{19}$$

故所得的概率分布矩阵以及其4个子空间矩阵为

$$\boldsymbol{M}=\begin{pmatrix}P_{11}&\cdots&P_{1n}\\ \vdots&\ddots&\vdots\\ P_{11}&\cdots&P_{nn}\end{pmatrix},\ \boldsymbol{M}_1=\begin{pmatrix}P_{11}&\cdots&P_{1\frac{n}{2}}\\ \vdots&\ddots&\vdots\\ P_{\frac{n}{2}1}&\cdots&P_{\frac{n}{2}\frac{n}{2}}\end{pmatrix},\ \boldsymbol{M}_2=\begin{pmatrix}P_{1\frac{n}{2}}&\cdots&P_{1n}\\ \vdots&\ddots&\vdots\\ P_{\frac{n}{2}\frac{n}{2}}&\cdots&P_{\frac{n}{2}n}\end{pmatrix},\ \boldsymbol{M}_3=\begin{pmatrix}P_{\frac{n}{2}1}&\cdots&P_{\frac{n}{2}\frac{n}{2}}\\ \vdots&\ddots&\vdots\\ P_{n1}&\cdots&P_{n\frac{n}{2}}\end{pmatrix},\ \boldsymbol{M}_4=\begin{pmatrix}P_{\frac{n}{2}\frac{n}{2}}&\cdots&P_{\frac{n}{2}n}\\ \vdots&\ddots&\vdots\\ P_{\frac{n}{2}n}&\cdots&p_{nn}\end{pmatrix} \tag{20}$$

因本文采用的量子随机行走策略为行走者位于$H_w$与$H_c$所构成的希尔伯特空间$\hat{H}$的中心，故最终生成的4个子矩阵$\boldsymbol{M}_1,\boldsymbol{M}_2,\boldsymbol{M}_3,\boldsymbol{M}_4$关于点$P_{\frac{n}{2}\frac{n}{2}}$中心对称. 为提高加密质量，本文仅选取$\hat{\boldsymbol{M}}=\boldsymbol{M}_1$作为所需伪随机数矩阵参与加密.

**步骤 2**：对所选矩阵$\hat{\boldsymbol{M}}$进行数据处理得到矩阵**QWPmatrix**. 本文将数据精度控制到$10^{-14}$，为适用于RGB图像的像素取值区间，需将矩阵$\hat{\boldsymbol{M}}$内元素区间进行数据处理得到所需的矩阵：

$$\mathbf{QWPmatrix}=(\hat{\boldsymbol{M}}\times 10^{14})\bmod 256 \tag{21}$$

### 3.1.2 制备加密密钥矩阵

**步骤 1**：得到DHNN的状态矩阵**RestoredW**. 截取$\hat{\boldsymbol{M}}$的子矩阵$\boldsymbol{\Psi}_1$和$\boldsymbol{\Psi}_2$分别作为DHNN的训练矩阵与输入矩阵：

$$\boldsymbol{\Psi}_1=\begin{pmatrix} P_{\frac{n}{4}1} & \cdots & P_{\frac{n}{4}\frac{n}{4}} \\ \vdots & \ddots & \vdots \\ P_{\frac{n}{2}1} & \cdots & P_{\frac{n}{2}\frac{n}{4}} \end{pmatrix},\quad \boldsymbol{\Psi}_2=\begin{pmatrix} P_{1\frac{n}{4}} & \cdots & P_{1\frac{n}{2}} \\ \vdots & \ddots & \vdots \\ P_{\frac{n}{4}\frac{n}{4}} & \cdots & P_{\frac{n}{4}\frac{n}{2}} \end{pmatrix} \tag{22}$$

由于本文提出的加密方案设计时只需DHNN训练一个矩阵，即式(2)中$p=1$，因此可以将上文Hebbian学习规则式(2)简写为

$$\boldsymbol{W}=\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}-\boldsymbol{I} \tag{23}$$

通过DHNN对输入矩阵进行处理，使能量函数变化率$\Delta E(t)=0$，DHNN达到稳态后得到所需的状态矩阵**RestoredW**. 其中能量函数变化率$\Delta E(t)$表示如下：

$$\begin{aligned}\Delta E(t)&=E(t+1)-E(t)\\&=-\Delta\boldsymbol{X}^{\mathrm{T}}(t)[\boldsymbol{W}\boldsymbol{X}(t)-T]-\frac{1}{2}\Delta\boldsymbol{X}^{\mathrm{T}}(t)\boldsymbol{W}\Delta\boldsymbol{X}(t)\\&=-\Delta\boldsymbol{X}^{\mathrm{T}}(t)\mathrm{net}(t)-\frac{1}{2}\Delta\boldsymbol{X}^{\mathrm{T}}(t)\boldsymbol{W}\Delta\boldsymbol{X}(t)\end{aligned} \tag{24}$$

**步骤 2**：得到加密所需密钥矩阵**Keymatrix**. 将得到的DHNN状态矩阵**RestoredW**与其自身的转置矩阵**RestoredW**$^{\mathrm{T}}$进行张量运算得到一个临时矩阵：**TempW**=**RestoredW**$\otimes$**Restored W**$^{\mathrm{T}}$. 对**TempW**进行一维向量化：

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1\omega} \\ \vdots & \ddots & \vdots \\ \varphi_{\omega 1} & \cdots & \varphi_{\omega\omega} \end{pmatrix}\rightarrow(\varphi_{11},\varphi_{12},\cdots,\varphi_{\omega 1},\cdots,\varphi_{\omega\omega}) \tag{25}$$

由于DHNN为二值神经网络，故所得的向量**TempW**中元素取值区间为{−1, 1}. 为适应加密，将矩阵**TempW**中元素每隔8位进行一次合并，将元素区间映射为0~255的十进制整数元素. 截取向量的前$n^2$个元素进行向量矩阵化得到**KeyMatrix**为

$$\begin{aligned}&(\varphi_1,\varphi_2,\cdots,\varphi_\omega,\cdots,\varphi_{\omega^2})\longrightarrow\left(\xi_1,\xi_2,\cdots,\xi_j,\cdots,\xi_{\frac{\omega^2}{8}}\right)\\&(\xi_1,\xi_2,\cdots,\xi_i,\cdots,\xi_{n^2})\longrightarrow\begin{pmatrix} \xi_{11} & \cdots & \xi_{1n} \\ \vdots & \ddots & \vdots \\ \xi_{n1} & \cdots & \xi_{nn} \end{pmatrix}\end{aligned} \tag{26}$$

### 3.1.3 图像加密

**步骤 1**：对原始图像的对应矩阵**OriImage**的三通道数据分别进行混淆. 将密钥矩阵**KeyMatrix**与原始图像$\boldsymbol{I}$的三个通道矩阵$\boldsymbol{I}$_**B**，$\boldsymbol{I}$_**G**，$\boldsymbol{I}$_**R**分别异或得到$\boldsymbol{I}_1$_**B**，$\boldsymbol{I}_1$_**G**，$\boldsymbol{I}_1$_**R**如下：

$$\begin{aligned}\boldsymbol{I}_E\_\mathbf{B}&=\mathbf{KeyMatrix}\oplus\boldsymbol{I}\_\mathbf{B}\\\boldsymbol{I}_E\_\mathbf{G}&=\mathbf{KeyMatrix}\oplus\boldsymbol{I}\_\mathbf{G}\\\boldsymbol{I}_E\_\mathbf{R}&=\mathbf{KeyMatrix}\oplus\boldsymbol{I}\_\mathbf{R}\end{aligned} \tag{27}$$

**步骤 2**：对$\boldsymbol{I}_1$_**B**，$\boldsymbol{I}_1$_**G**，$\boldsymbol{I}_1$_**R**进行一维向量化处理得到$\boldsymbol{I}_2$_**B**，$\boldsymbol{I}_2$_**G**，$\boldsymbol{I}_2$_**R**，将矩阵**KeyMatrix**同样一维向量化处理后，按其索引进行排序得到加密所需的顺序表$\Omega$，按照$\Omega$中索引值$i$对应索引项$\Omega(i)$的位置的值对$\boldsymbol{I}_2$的三个通道分别进行三次迭代置乱得到$\boldsymbol{I}_E$_**B**，$\boldsymbol{I}_E$_**G**，$\boldsymbol{I}_E$_**R**，单次置乱算法如图4所示.

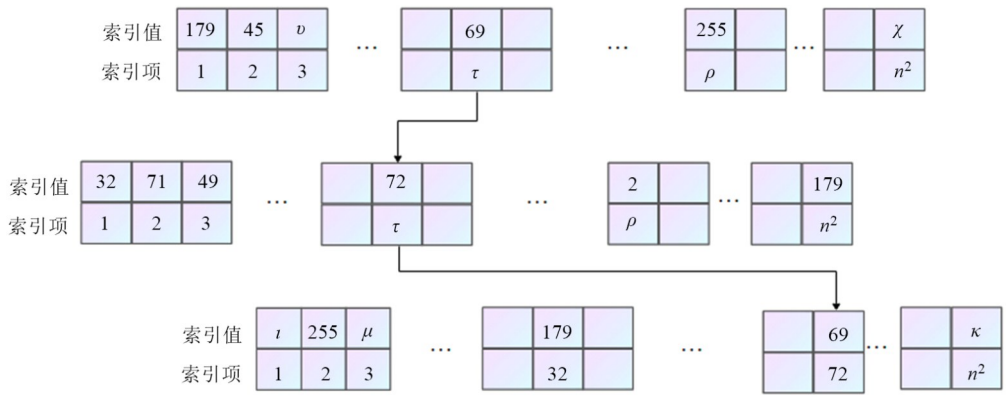


图4 基于Hopfield网络“伪吸引子”与交替量子随机行走的抗攻击彩色图像加密方案的单次置乱算法

**步骤 3**:将 $\boldsymbol{I}_E\_\mathbf{B}$,$\boldsymbol{I}_E\_\mathbf{G}$,$\boldsymbol{I}_E\_\mathbf{R}$ 还原为原始矩阵形式,按顺序合并得到最终加密图像 **EngImage**.

### 3.2　解密过程

#### 3.2.1　制备解密密钥矩阵

由于量子随机行走概率矩阵具备伪随机性,当选取的量子随机行走参数 $\alpha,\beta,N$ 不变时,生成的新的概率分布矩阵 $\boldsymbol{M}'=\boldsymbol{M}$,对 $\boldsymbol{M}'$ 进行与 $\boldsymbol{M}$ 相同的处理后,重新生成的密钥矩阵:

$$\mathbf{KeyMatrix}'=\mathbf{KeyMatrix} \tag{28}$$

#### 3.2.2　加密图像解密

**步骤 1**:对加密后的图像 **EncImage** 逆置乱,将 RGB 图像 **EncImage** 的矩阵形式 $\boldsymbol{I}_E$ 分解为 $\boldsymbol{I}_E\_\mathbf{B}$,$\boldsymbol{I}_E\_\mathbf{G}$,$\boldsymbol{I}_E\_\mathbf{R}$,并进行一维向量化处理得到 $\boldsymbol{I}_E\_\mathbf{B}'$,$\boldsymbol{I}_E\_\mathbf{G}'$,$\boldsymbol{I}_E\_\mathbf{R}'$,按其索引进行排序得到加密所需的索引表 $\Omega'$,按照 $\Omega'$ 中索引值 $i$ 对应的索引项 $\Omega'(i)$ 位置的值对 $\boldsymbol{I}_E\_\mathbf{B}'$,$\boldsymbol{I}_E\_\mathbf{G}'$,$\boldsymbol{I}_E\_\mathbf{R}'$ 分别进行 3 次迭代逆置乱,得到 $\boldsymbol{I}_E\_\mathbf{B}''$,$\boldsymbol{I}_E\_\mathbf{G}''$,$\boldsymbol{I}_E\_\mathbf{R}''$,具体逆置乱算法如图 5 所示.

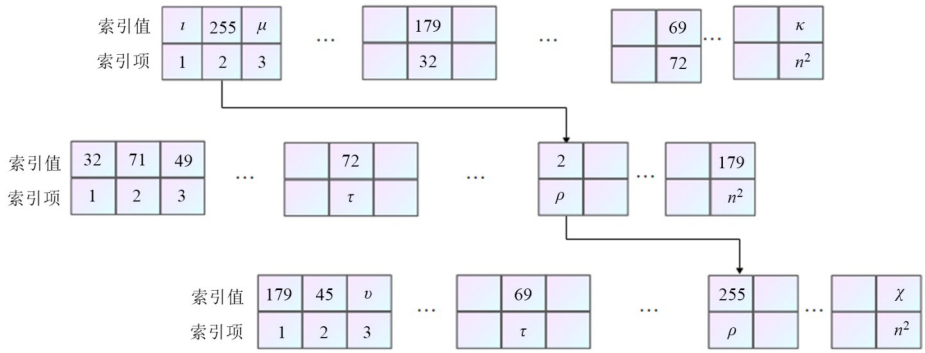


图 5　基于Hopfield网络“伪吸引子”与交替量子随机行走的抗攻击彩色图像加密方案的单次逆置乱算法

**步骤 2**:对加密图像进行混淆还原,将 $\boldsymbol{I}_E\_\mathbf{B}''$,$\boldsymbol{I}_E\_\mathbf{G}''$,$\boldsymbol{I}_E\_\mathbf{R}''$ 转换为原始矩阵形式并将其与 **KeyMatrix**′分别进行异或得到 $\boldsymbol{I}_D\_\mathbf{B}$,$\boldsymbol{I}_D\_\mathbf{G}$,$\boldsymbol{I}_D\_\mathbf{R}$:

$$\boldsymbol{I}_D\_\mathbf{B}=\mathbf{KeyMatrix}\oplus\boldsymbol{I}_E\_\mathbf{B}''$$

$$\boldsymbol{I}_D\_\mathbf{G}=\mathbf{KeyMatrix}\oplus\boldsymbol{I}_E\_\mathbf{G}''$$

$$\boldsymbol{I}_D\_\mathbf{R}=\mathbf{KeyMatrix}\oplus\boldsymbol{I}_E\_\mathbf{R}'' \tag{29}$$

**步骤 3**:将 $\boldsymbol{I}_D\_\mathbf{B}$,$\boldsymbol{I}_D\_\mathbf{G}$,$\boldsymbol{I}_D\_\mathbf{R}$ 按通道顺序进行合并,即可得到未加密前的原始图像对应矩阵 **OriImage**.

本文所提加解密方案的流程如图 6 所示.

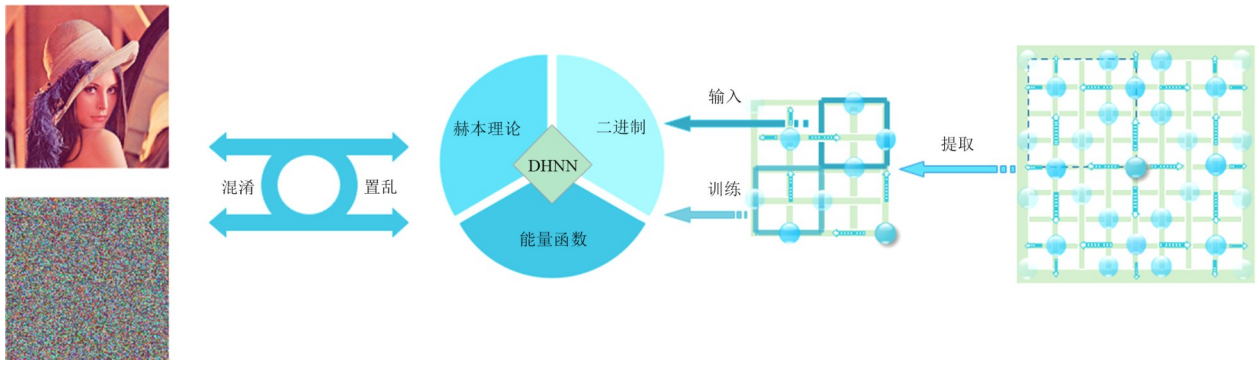


图 6　加解密流程图

## 4　仿真分析

为验证所提方案的抗攻击能力,包含加密图像的有效性、安全性,以及应对各种实际应用中复杂环境的鲁棒性,本文进行了实验仿真. 选取像素大小为 512×512 的 3 张彩色图片进行本文加密方案所述的加密及解密,并对加密前后图像进行像素相关性分析、直方图分析、密钥敏感度分析、抗噪声干扰能力和密钥空间等安全性分析.

### 4.1　实验参数以及解密结果

为验证所提出加密方案的效果,本文在实验仿真部分选取 Lena,Lemon,Sakura 这 3 幅彩色图像,在量子随机行走部分,随机选取参数:$N=240,\alpha=\dfrac{\pi}{23},\beta=\dfrac{\pi}{41}$. 采用上述参数生成的密钥矩阵在不添加噪声干扰下,加密与解密效果如图 7 所示.

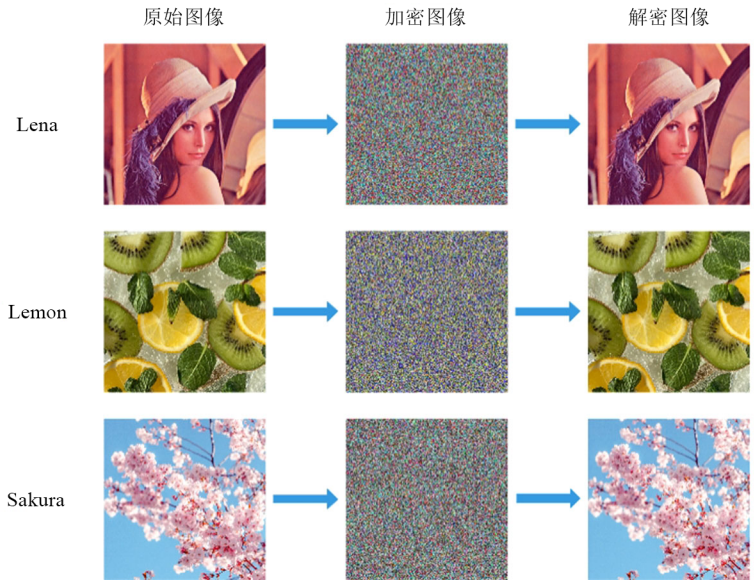


图7 算法加密与解密效果图

## 4.2 统计学分析

### 4.2.1 相关性分析

相邻像素相关性用于衡量相邻像素值的相关程度. 普通图像中的相邻像素值在水平、垂直以及对角方向上都具有很强的相关性,图像加密算法会打破这些相邻像素间的相关性,而破坏程度便能反应加密算法效果,即加密后图像的相邻像素的相关值应尽可能地接近零[33]. 相关性分析公式为

$$R_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{30}$$

本文加密方案分别针对Lena,Lemon,Sakura这3幅图像的RGB三通道在水平垂直与对角方向上对加密前后的相关性进行了分析对比. 相关数据见表1,具体的像素分布表现如图8至图10所示.

### 4.2.2 直方图分析

直方图能直观地显示图像灰度值的统计信息和分布情况. 未加密图像的直方图具有明显的统计学规律,针对统计规律的攻击方案被称为统计分析攻击. 为抵抗统计攻击,加密图像的直方图必须是均匀并且完全不同于明文图像直方图. 直方图的方差能有效量化加密算法抵御统计分析攻击能力. 方差越小,说明像素分布越均匀,图像显示的统计信息就越少,信息越无法准确预测,图像加密方案就越安全[34],本文分别对Lena,Lemon,Sakura这3幅图像的RGB三通道进行直方图分析,具体的直方图分析如图11至图13所示.

### 4.2.3 信息熵分析

熵通常用来描述事物的混乱程度. 信息熵分析是对信息随机性的度量方式,RGB图像的像素值范围为

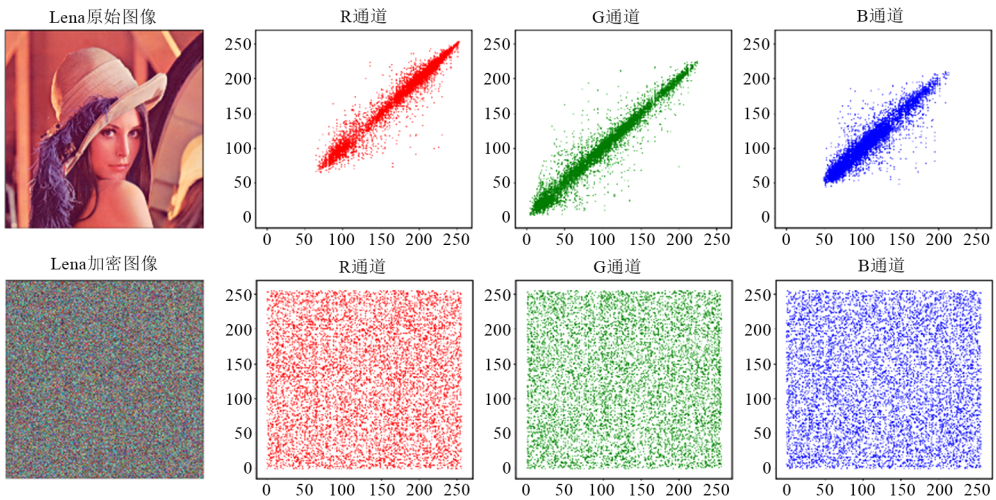


图8 Lena图像加密前后相关性分析对比

**表1　相关性分析**

| 图像 | 加密状态 | 通道 | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|---|
| Lena | 加密前 | Red | 0.980 1 | 0.988 9 | 0.966 8 |
| | | Green | 0.971 1 | 0.984 3 | 0.958 5 |
| | | Blue | 0.928 8 | 0.955 8 | 0.914 6 |
| | 加密后 | Red | 0.003 7 | 0.006 2 | 0.005 6 |
| | | Green | 0.006 2 | 0.003 1 | 0.003 3 |
| | | Blue | 0.003 9 | 0.001 5 | 0.002 4 |
| Lemon | 加密前 | Red | 0.919 0 | 0.934 3 | 0.895 1 |
| | | Green | 0.876 5 | 0.894 7 | 0.828 4 |
| | | Blue | 0.983 1 | 0.980 0 | 0.965 0 |
| | 加密后 | Red | 0.001 1 | 0.005 1 | 0.007 4 |
| | | Green | 0.002 3 | 0.004 8 | 0.004 1 |
| | | Blue | 0.000 9 | 0.003 1 | 0.005 7 |
| Sakura | 加密前 | Red | 0.905 7 | 0.892 0 | 0.791 8 |
| | | Green | 0.925 1 | 0.910 2 | 0.826 6 |
| | | Blue | 0.918 0 | 0.900 4 | 0.803 0 |
| | 加密后 | Red | 0.003 7 | 0.006 1 | 0.002 4 |
| | | Green | 0.003 8 | 0.002 1 | 0.001 8 |
| | | Blue | 0.003 5 | 0.000 8 | 0.011 6 |

0~255,因此信息熵上限为8. 熵值越接近8,所携带信息量越多,抵抗统计攻击能力越强[35]. 信息熵公式如下:

$$H(m)=-\sum_{i=0}^{N-1}P\left(m_i\right)\log_2 P\left(m_i\right) \tag{31}$$

其中,$m_i$为灰度值,$P(m_i)$为$m_i$出现的概率.

本文分别对Lena,Lemon,Sakura这3幅图像的RGB三通道进行信息熵的分析,相关数据见表2.

**表2　信息熵分析**

| 图像 | 通道 | 信息熵/bit |
|---|---|---|
| Lena加密后 | Red | 7.999 3 |
| | Green | 7.999 3 |
| | Blue | 7.999 4 |
| Lemon加密后 | Red | 7.999 6 |
| | Green | 7.999 5 |
| | Blue | 7.999 3 |
| Sakura加密后 | Red | 7.999 4 |
| | Green | 7.999 3 |
| | Blue | 7.999 6 |

### 4.2.4　密钥灵敏度分析

有效的密钥灵敏度意味着改变密钥中一个比特将导致50%以上的密文图像发生改变[36],采用NPCR和UACI来表示对同一图像采用不同密钥加密生成的加密图像之间变化像素的数量和像素的平均变化强度. NPCR和UACI的理想值分别为99.61%和33.46%. 加密方案的NPCI和UACI的计算值越高表明加密方案抵抗差分攻击的能力越强.

$$D(i,j)=f(x)=\begin{cases}1, & \text{if } C_1(i,j)\neq C_2(i,j)\\ 0, & \text{otherwise}\end{cases} \tag{32}$$

$$\begin{aligned}\mathrm{NPCR}&=\frac{\sum_{i,j}D(i,j)}{\Im\times\Re}\times 100\%\\ \mathrm{UACI}&=\frac{1}{\Im\times\Re}\left[\sum_{i,j}\frac{C_1(i,j)-C_2(i,j)}{255}\right]\times 100\%\end{aligned} \tag{33}$$

其中,$\Im$和$\Re$为加密图像的长和宽,$C_1$和$C_2$为不同密钥加密后的图像.

本文分别对Lena,Lemon,Sakura这3幅图像的RGB三通道进行密钥灵敏度分析,相关数据见表3.

**表3　密钥敏感度分析**

| 图像 | 通道 | NPCR/% | UACI/% |
|---|---|---|---|
| Lena | Red | 99.618 9 | 33.516 3 |
| | Green | 99.630 6 | 33.548 8 |
| | Blue | 99.615 5 | 33.496 8 |
| Lemon | Red | 99.598 3 | 33.576 6 |
| | Green | 99.631 1 | 33.532 7 |
| | Blue | 99.623 8 | 33.546 9 |
| Sakura | Red | 99.642 2 | 33.551 7 |
| | Green | 99.612 5 | 33.543 9 |
| | Blue | 99.623 3 | 33.527 7 |

### 4.2.5　密钥空间

密钥空间指用于生成密钥的所有可能密钥的集合,是决定加密系统抗暴力攻击强度的决定因素之一. 在2进制加密算法中为密钥大小为128位的加密算法定义了大小为$2^{128}$的密钥空间,使用现代高性能计算机尝试所有可能的密钥需要大约1 000年的时间. 因此,密钥大小为128位的密码系统对暴力攻击具有鲁棒性[37]. 在本文的加密算法中,由于量子随机行走的状态空间无限,故理论密钥空间为无穷. 在仿真分析中,为保证加密的质量与效率,本文将量子随机行走参数精度控制到$10^{-14}$,实际可用密钥空间为$10^{60}$远超过$2^{128}$,故具备极强的抗暴力攻击能力.

### 4.2.6　明文攻击

已知明文攻击:攻击者通过获取解密成功后的图片与密文图片进行对比,恢复密钥.

由于本文的算法具备良好的扩散效果,攻击者通过此种方法获得密钥和直接暴力攻击难度接近,所以本文的加密方案可以有效抵抗已知明文攻击.

选择明文攻击:攻击者在无须密钥的前提下,以某种手段实现输入原始图像便能得到加密后的图像.

攻击者利用这一安全弱点,使用选择的纯文本攻击来破解加密算法. 由于本文加密算法中引入了原始图像像素信息作为权重参数,参与到量子随机行走概

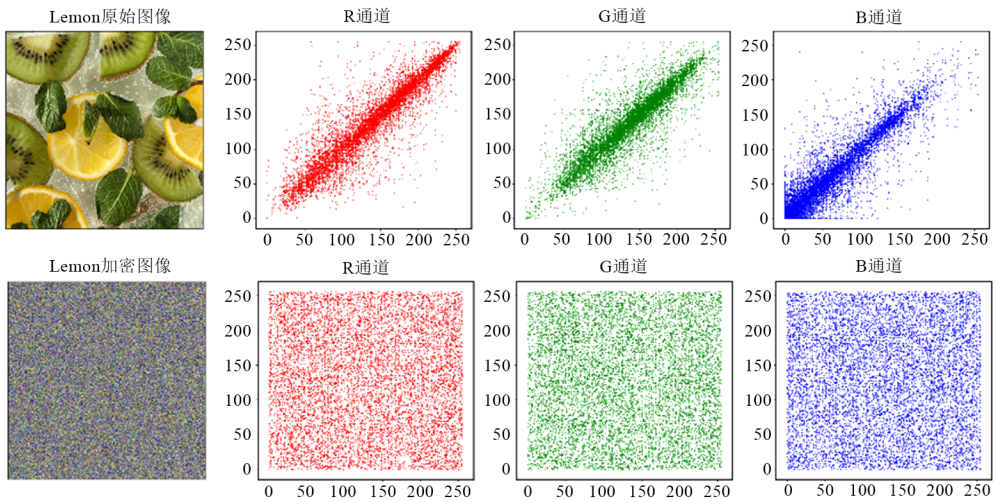


图9 Lemon图像加密前后相关性分析对比

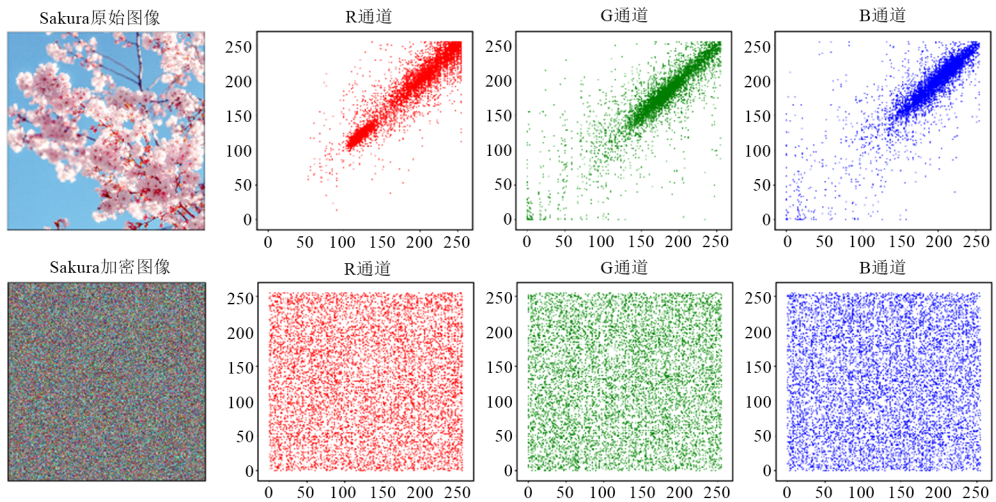


图10 Sakura图像加密前后像素点分布

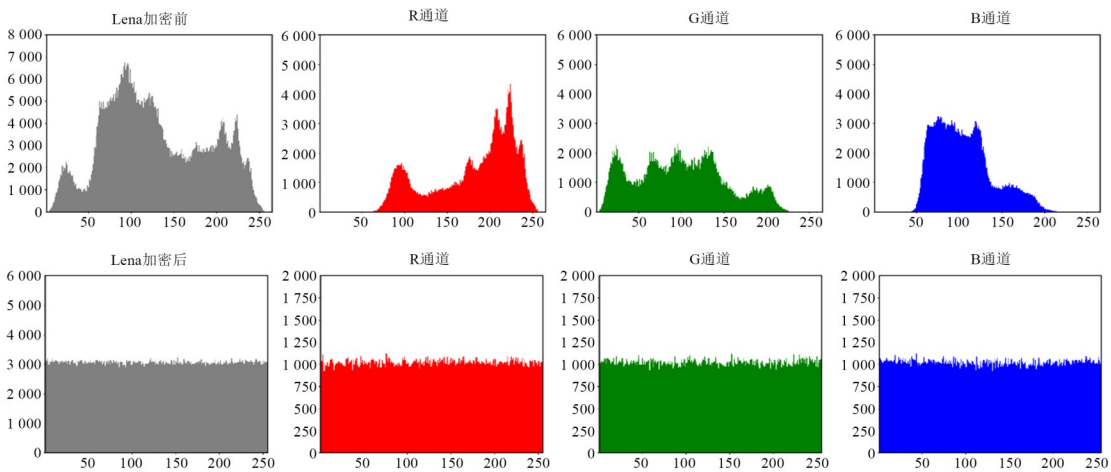


图11 Lena图像加密前后像素点分布

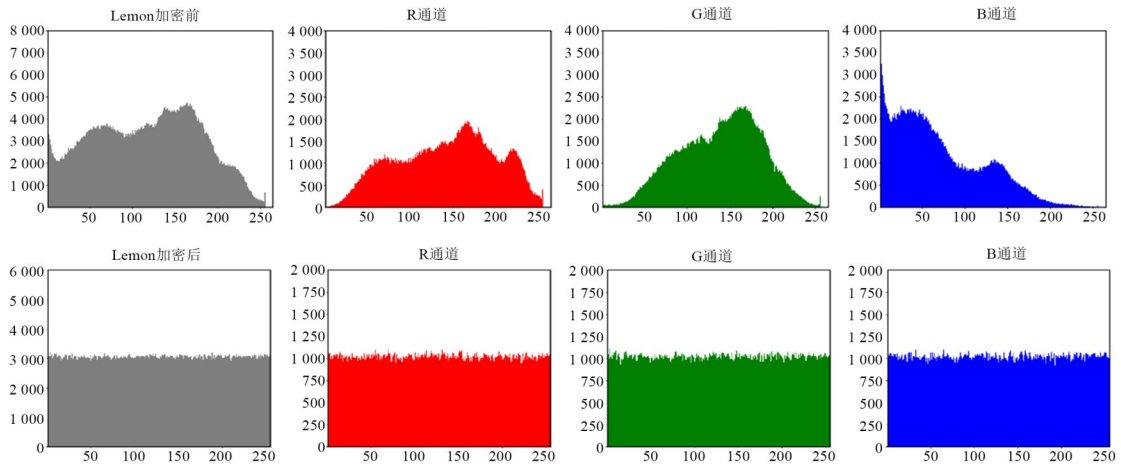


图12　Lemon图像加密前后像素点分布

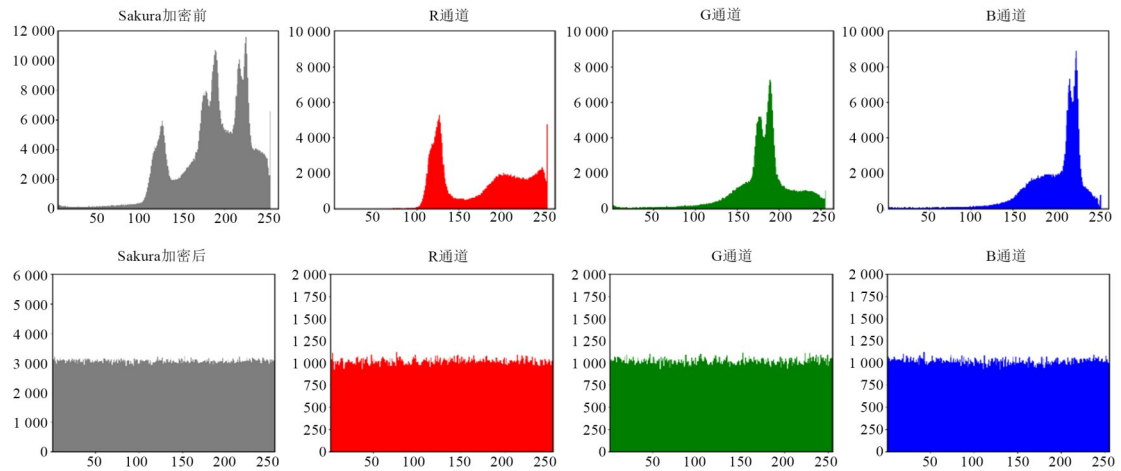


图13　Sakura图像加密前后像素点分布

率分布矩阵参数的选取中,进行不同图像的加密时,能极大程度地避免出现密钥相同的情况,因此可以有效避免攻击者通过选择明文攻击进行加密图像的破译.

### 4.2.7　时间复杂度分析

时间复杂度分析是衡量加密方案性能的重要指标,其将直接影响加密效率[38]. 在分析本文加密方案的算法复杂度时,需做两个前提假定:①不考虑生成密钥矩阵的时间复杂度,因为其与图像信息无直接关系,仅与密钥相关;②本文涉及的经典计算机的矩阵遍历时间复杂度均为$O(n^2)$. 在两个假定下,本文的算法复杂度主要由所需加密图像进行的混淆与置乱两部分的时间复杂度构成,其中混淆过程由一次密钥矩阵与所需加密矩阵的异或完成,其时间复杂度为$O(n^2)$,置乱过程由三次迭代置乱组成,其时间复杂度为$O(3n^2)$,故本文加密的时间复杂度为$O(4n^2)$. 本文对比了经典的加密方案(如DES方案、AES方案),同时选取被图像加密领域广泛应用的经典混沌加密算法作为对比. 在AMD Ryzen™ 75 800处理器、16 GB RAM和Windows11操作系统上使用python3.9在Pycharm平台实施本文方案和上述其他方案,并利用python中的time包来进行时间计量工作. 选取像素值512×512像素的Lena作为对比的图像,其中利用DES算法完成图像加密的时间为1.765 19 s,AES算法完成图像加密的时间为0.726 59 s,混沌加密算法完成图像加密的时间为0.538 67 s,本文所提算法完成图像加密的时间为0.372 44 s. 通过对比可以得出,本文算法在不考虑密钥矩阵生成时间的前提下,较之传统算法具备极大的加密速度优势.

### 4.2.8　抗噪声分析

噪声在图像传输过程中会因为各种环境因素产生,同时也可能出现攻击者通过恶意攻击干扰图像传输进而产生噪声的情况[39]. 因此,针对抗噪声的鲁棒性分析是测试图像加密方案优劣的重要指标[40]. 本文针对噪声问题进行了高斯噪声与椒盐噪声的模拟分析,针对加密图像因各种原因导致的丢包问题进行了剪切

攻击的模拟分析. 图14展示了Lena加密图像在添加高斯噪声、椒盐噪声以及剪切攻击后解密的图像.

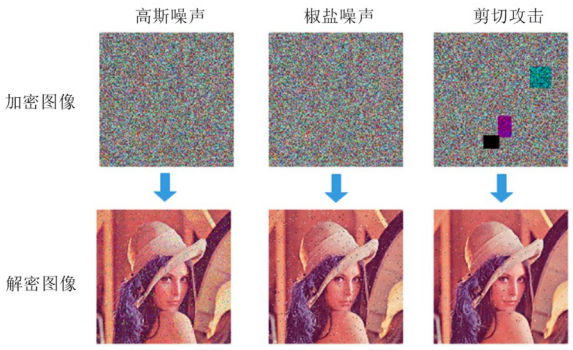


图14 Lena密文图像添加噪声后产生的变化

### 4.3 加密方案对比

将本文加密方案与参考文献中选取的相关加密方案从平均NPCR、平均UACI、密钥空间大小是否能够抵抗暴力破解,以及平均相关性和信息熵方面进行对比分析,得出的数据见表4.

表4 平均相关性和信息熵对比分析

| 算法 | 平均NPCR/% | 平均UACI/% | 密钥空间 | 平均相关性 | 熵/bit |
|---|---|---|---|---|---|
| 文献[13] | 99.623 3 | 33.476 6 | $>2^{128}$ | 0.010 7 | 7.999 3 |
| 文献[41] | | | $>2^{128}$ | 0.009 9 | |
| 文献[42] | | | $>2^{128}$ | 0.012 9 | |
| 文献[43] | 99.615 8 | 33.455 7 | $>2^{128}$ | | 7.997 1 |
| 文献[44] | 99.613 0 | 33.460 5 | $>2^{128}$ | | 7.997 3 |
| 文献[45] | 99.570 5 | 35.080 6 | $>2^{128}$ | 0.002 4 | 7.996 6 |

## 5 结论

本文进行了量子理论与机器学习在图像加密领域的应用研究,通过仿真分析加密效果、对比其他加密方案,证实了本文所提的结合了Hopfield网络伪吸引子与交替量子随机行走的彩色图像加密方案的可行性,表明了将量子理论与机器学习算法应用到图像加密领域具备广阔的应用前景. 本文所提加密方案中,量子随机行走生成的概率密度矩阵与Hopfield网络的伪吸引子所对应的矩阵形式都作为重要的工具参与到了加密矩阵的制备之中,在之后的研究工作中也希望能将二者的优势更好地发挥出来.

## 附录

**(1)参数精度的选取**

本文采用python进行仿真分析,在python中,浮点数的默认有效精度为17位,在进行仿真分析时,发现若采用默认的有效精度,加密效果将出现不稳定的现象,如NPCR和UACI有几率达不到99.61%和33.46%的理想值,即密钥的敏感度开始下降. 最终经过测试,借助python自带的包将有效精度控制到14位进行仿真分析.

**(2)密钥空间的得出**

量子随机行走的实际密钥空间由$\alpha$和$\beta$决定. $\alpha$为硬币算符初态参数,$\beta$为硬币算符抛掷参数. 若不考虑精度问题,密钥空间的大小便是$\alpha$和$\beta$可取值量的乘积,因$\alpha$和$\beta$二者的取值范围为0到$2\pi$的任意值,故由$\alpha$和$\beta$决定的密钥空间理论值为无限大. 但仿真分析时,因采用经典计算机进行分析,无法验证无限精度下的可能性,故只能控制精度到一定范围进行研究. 本文在分析中,考虑到参数精度的问题,令$\vartheta=3\ 141\ 592\ 653\ 589\ 793.\ 238\ 462\ 643\ 383\ 27$,令$K_1$与$K_2$为30位的随机数,如

$$K_1=2\ 564\ 823\ 796\ 521\ 785.475\ 638\ 962\ 148\ 03,$$

$$K_2=0\ 562\ 789\ 324\ 747\ 325.145\ 624\ 856\ 254\ 63,$$

$\alpha=\dfrac{\vartheta}{K_1}\bmod(2\pi),\beta=\dfrac{\vartheta}{K_1}\bmod(2\pi)$. 经过验证的有效密钥空间大小由仿真时采用的总随机数长度决定,因为使用十进制计算,故密钥空间为1 060. 同时,本文也借助python的decimal包进行提升模拟精度可能性的测试,进一步探索扩充本文加密方案的密钥空间的可能性.

### 参考文献

[1] LAURIA F E. Non-linguistic Neurocrytology and the Shannon theorem[J]. Structures: From Physics to General Systems, 1992 ,2: 238-244.

[2] BIGDELI N, FARID Y, AFSHAR K. A robust hybrid method for image encryption based on Hopfield neural network[J]. Computers & Electrical Engineering, 2012, 38(2): 356-369.

[3] PRAKASH M, BALASUBRAMANIAM P, LAKSHMANAN S. Synchronization of Markovian jumping inertial neural networks and its applications in image encryption[J]. Neural Networks, 2016, 83: 86-93.

[4] WANG X Y, YANG L, LIU R, et al. A chaotic image encryption algorithm based on perceptron model[J]. Nonlinear Dynamics, 2010, 62(3): 615-621.

[5] LIAN S G. A block cipher based on chaotic neural networks[J]. Neurocomputing, 2009, 72(4/5/6): 1296-1301.

[6] HOPFIELD J J. Neural networks and physical systems with emergent collective computational abilities[J]. Proceedings of the National Academy of Sciences, 1982, 79 (8): 2554-2558.

[7] 韩力群. 人工神经网络理论、设计及应用[M]. 2版. 北京: 化学工业出版社, 2007.
HAN L Q. Theory, Design and Application of Artificial Neural Network[M]. 2nd ed. Beijing: Chemical Industry Press, 2007. (in Chinese)

[8] HOPFIELD J J. Neurons with graded response have collective computational properties like those of two-state neurons[J]. Proceedings of the National Academy of Sciences, 1984, 81(10): 3088-3092.

[9] BRUCK J. On the convergence properties of the Hopfield model[J]. Proceedings of the IEEE, 1990, 78(10): 1579-1585.

[10] WEISBUCH G, FOGELMAN-SOULIE F. Scaling laws for the attractors of Hopfield networks[J]. Journal De Physique Lettres, 1985, 46(14): 623-630.

[11] STORKEY A J, VALABREGUE R. The Basins of attraction of a new Hopfield learning rule[J]. Neural Networks, 1999, 12(6): 869-876.

[12] WUENSCHE A. Discrete dynamical networks and their attractor basins[J]. Complexity International, 1998, 6: 3-21.

[13] 徐子同, 高涛, 于正同, 等. 基于离散型Hopfield神经网络的图像加密算法[J]. 计算机技术与发展, 2021, 31(6): 106-111.
XU Z T, GAO T, YU Z T, et al. Image encryption algorithm based on discrete hopfield neural network[J]. Computer Technology and Development, 2021, 31(6): 106-111. (in Chinese)

[14] WANG X Y, LI Z M. A color image encryption algorithm based on Hopfield chaotic neural network[J]. Optics and Lasers in Engineering, 2019, 115: 107-118.

[15] LAKSHMI C, THENMOZHI K, RAYAPPAN J B B, et al. Hopfield attractor-trusted neural network: An attack-resistant image encryption[J]. Neural Computing and Applications, 2020, 32(15): 11477-11489.

[16] BENIOFF P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines[J]. Journal of Statistical Physics, 1980, 22(5): 563-591.

[17] ZHOU N R, HUANG L X, GONG L H, et al. Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map[J]. Quantum Information Processing, 2020, 19(9): 284.

[18] ZHOU L, SHENG Y B, LONG G L. Device-independent quantum secure direct communication against collective attacks[J]. Science Bulletin, 2020, 65(1): 12-20.

[19] GAO F, QIN S J, HUANG W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol[J]. Science China Physics, Mechanics & Astronomy, 2019, 62(7): 70301.

[20] ZHOU Z R, SHENG Y B, NIU P H, et al. Measurement-device-independent quantum secure direct communication [J]. Science China Physics, Mechanics & Astronomy, 2020, 63(3): 230362.

[21] 高飞, 温巧燕, 秦素娟, 等. 基于对称密钥的量子公钥密码[J]. 中国科学: 物理学 力学 天文学, 2010, 40(1): 26-32.
GAO F, WEN Q Y, QIN S J, et al. Quantum public key cryptography based on symmetric key[J]. Scientia Sinica (Pysica, Mechanica & Astronomica), 2010, 40(1): 26-32. (in Chinese)

[22] 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, 2021, 31(1): 10301-10307.

[23] DAI J Y, MA Y, ZHOU N R. Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map[J]. Quantum Information Processing, 2021, 20(7): 246-270.

[24] AHARONOV Y, DAVIDOVICH L, ZAGURY N. Quantum random walks[J]. Physical Review A, 1993, 48(2): 1687-1690.

[25] FARHI E, GUTMANN S. Quantum computation and decision trees[J]. Physical Review A, 1998, 58(2): 915-928.

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

[27] BARYSHNIKOV Y, BRADY W, BRESSLER A, et al. Two-dimensional quantum random walk[J]. Journal of Statistical Physics, 2011, 142(1): 78-107.

[28] YANG Y G, PAN Q X, SUN S J, et al. Novel image encryption based on quantum walks[J]. Scientific Reports, 2015, 5: 7784.

[29] ABD A A, EL-LATIF, . Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption[J]. Physica A: Statistical Mechanics and Its Applications, 2020, 547: 123869-123889.

[30] 王一诺, 宋昭阳, 马玉林, 等. 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): 32-41.

WANG Y N, SONG Z Y, MA Y L, et al. Color image encryption algorithm based on DNA code and alternating quantum random walk[J]. Acta Physica Sinica, 2021, 70 (23): 32-41. (in Chinese)

[31] 丁群, 陆哲明, 孙晓军. 基于神经网络密码的图像加密[J]. 电子学报, 2004, 32(4): 677-679.
DING Q, LU Z M, SUN X J. The image encryption based on neural network cipher[J]. Acta Electronica Sinica, 2004, 32(4): 677-679. (in Chinese)

[32] CAPORALE N, DAN Y. Spike timing-dependent plasticity: A Hebbian learning rule[J]. Annual Review of Neuroscience, 2008, 31: 25-46.

[33] HEBB D O. The Organization of Behavior: A Neuropsychological Theory[M]. New York: Psychology Press, 2002.

[34] RAJA P S, MOHAN D N. A review on various image encryption techniques for secure image transmission[J]. International Journal of Advanced Research, 2014, 8: 1-14.

[35] YANG Y G, TIAN J, LEI H, ZHOU Y H, et al. Novel quantum image encryption using one-dimensional quantum cellular automata[J]. Information Sciences, 2016, 345: 257-270.

[36] ZHOU N R, HUA T X, GONG L H, et al. Quantum image encryption based on generalized Arnold transform and double random-phase encoding[J]. Quantum Information Processing, 2015, 14(4): 1193-1213.

[37] BENSIKADDOUR E H, BENTOUTOU Y, TALEB N. Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher[J]. Journal of King Saud University - Computer and Information Sciences, 2020, 32(1): 50-56.

[38] LIU C Y, DING Q. A color image encryption scheme based on a novel 3D chaotic mapping[J]. Complexity, 2020, 2020: 3837209-3837229.

[39] CHAI X, GAN Z, YANG K, et al. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations[J]. Signal Processing: Image Communication, 2017, 52: 6-19.

[40] YANG Y G, WANG B P, YANG Y L, et al. Visually meaningful image encryption based on universal embedding model[J]. Information Sciences, 2021, 562: 304-324.

[41] BABAEI M. A novel text and image encryption method based on chaos theory and DNA computing[J]. Natural Computing, 2013, 12(1): 101-107.

[42] TLELO-CUAUTLE E, DANIEL DÍAZ-MUÑOZ J, GONZÁLEZ-ZAPATA A M, et al. Chaotic image encryption using hopfield and hindmarsh-rose neurons implemented on FPGA[J]. Sensors (Basel, Switzerland), 2020, 20(5): 1326-1348.

[43] CHEN L, YIN H, HUANG T, et al. Chaos in fractional-order discrete neural networks with application to image encryption[J]. Neural Networks, 2020, 125: 174-184.

[44] CHEN L P, YIN H, YUAN L G, et al. A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations[J]. Frontiers of Information Technology & Electronic Engineering, 2020, 21(6): 866-879.

[45] ABANDA Y, TIEDEU A. Image encryption by chaos mixing[J]. IET Image Processing, 2016, 10(10): 742-750.

## 作者简介

**宋昭阳** 男,1996年出生,山东青岛人. 青岛理工大学信息与控制工程学院硕士研究生. 主要研究方向为量子机器学习与量子图像处理.
E-mail: 18853817685@163.com

**王一诺** 女,1998年出生,山东济南人. 青岛理工大学信息与控制工程学院硕士研究生. 主要研究方向为量子计算与量子图像处理.
E-mail: 202021060806@qut.edu.cn

**王浩文** 男,1998年出生,山东潍坊人. 青岛理工大学信息与控制工程学院硕士研究生. 主要研究方向为拓扑量子纠错与机器学习.
E-mail: 17806249178@163.com

**马鸿洋(通讯作者)** 男,1976年出生,山东青岛人. 青岛理工大学理学院教授. 主要研究方向为量子信息安全、网络通信协议研究. 中国电子学会会员:E190011364M.
E-mail: hongyang_ma@aliyun.com