物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于DNA编码与交替量子随机行走的彩色图像加密算法

王一诺 宋昭阳 马玉林 华南 马鸿洋

Color image encryption algorithm based on DNA code and alternating quantum random walk

Wang Yi-Nuo Song Zhao-Yang Ma Yu-Lin Hua Nan Ma Hong-Yang

引用信息 Citation: Acta Physica Sinica, 70, 230302 (2021) DOI: 10.7498/aps.70.20211255
在线阅读 View online: https://doi.org/10.7498/aps.70.20211255
当期内容 View table of contents: http://wulixb.iphy.ac.cn

基于 DNA 编码与交替量子随机行走的彩色图像加密算法*

王一诺[1)] 宋昭阳[2)] 马玉林[2)] 华南[2)] 马鸿洋[1)†]

1) (青岛理工大学理学院, 青岛 266520)

2) (青岛理工大学信息与控制工程学院, 青岛 266520)

(2021 年 7 月 5 日收到; 2021 年 8 月 4 日收到修改稿)

近年来, 图像加密技术备受关注. 随着人们对通信隐私及网络安全重视程度的提高, 对信息加密技术的要求更加严格, 图像作为信息的载体之一, 因携带信息的有效性和生动性而受到重视. 本文提出一种基于 DNA 编码与交替量子随机行走的彩色图像加密算法. 量子随机行走作为出色的密码学工具参与算法流程中各个部分, DNA 编码作为核心加密方式完成算法. 本文详细描述加密、解密流程, 并对所提出算法进行仿真实验验证与结果分析. 仿真阶段设计模拟密钥参数, 编码进行彩色图像加密、解密实验, 并进行了相关分析. 实验结果表明, 本文提出的彩色图像加密算法能够进行安全有效的彩色图像加密, 且相关分析表示其加密后图像直方图平稳、像素相关性系数趋近于 0、密钥空间 2^{128}, 三通道信息熵达到 7.997 以上, 能够抵御统计攻击、穷举攻击等攻击手段. 此外, DNA 编码除新颖的编码及运算方式之外还有其独特的生物学特性, 为密码学的研究提供了新的思路与方向.

关键词: 量子信息, 量子随机行走, 图像加密, DNA 编码

PACS: 03.65.–w, 03.67.Ac, 03.67.Dd, 42.50.Ex **DOI:** 10.7498/aps.70.20211255

1 引 言

通信领域与计算机网络技术飞速发展, 人们生活、工作越来越依赖于此的当下, 信息传递的安全性问题成为了被社会各界广泛关注的焦点. 由于互联网是一个开放与共享的社区, 这在一定程度上方便了信息交互, 同时使得信息安全性保障成为亟待解决的难题. 信息又分多个种类, 其中图像信息因其生动形象的特性被人们广泛应用. 本文正式基于上述事实提出的基于量子随机行走与 DNA 编码技术结合的彩色图像加密算法, 以期提高图像信息传递安全性.

量子算法[1–5]及相关应用在通信[6–11]等各领域[12–16]受到关注, 在图像处理中更是得到重视[17–20]. 其运算速度[21,22]、安全性[23,24]等方面相较于经典算法具有显著优势. 量子随机行走作为量子算法的重要工具参与算法流程各个步骤. 1993 年, 以色列物理学家 Aharonov 等[25]提出量子随机行走为经典随机行走在量子力学中的对应概念. 随着研究的推进, 其概念被细分为连续时间量子随机行走和离散时间量子随机行走, 二者分别为 1998 年美国 MIT 的 Farhi 和日本东北大学的 Gutmann[26]提出, 2001 年加拿大滑铁卢大学的 Watrous[27]由经典随机行走直接量子化得到的. 其中, 离散时间量子随机行走因具有混沌动力学行为而被应用于量

* 国家自然科学基金 (批准号: 11975132, 61772295)、山东省自然科学基金 (批准号: ZR2019YQ01) 和山东省高等教育科技计划 (批准号: J18KZ012) 资助的课题.

† 通信作者. E-mail: hongyang_ma@aliyun.com

子及经典密码学系统中[28–32]. 滑铁卢大学的Chris和Zhan[33]在2019年以组合方法构建的3个离散时间量子行走模型为我们提供了研究思路; Abd-El-Atty等[34]2021年研究发表的基于量子随机行走的光学图像加密算法为本文提供了研究方向及重要参考. 本文研究以离散时间交替量子随机行走构建的随机概率分布矩阵作为加密工具, 多次参与图像加密过程的彩色图像加密算法.

DNA编码因具有存储量大、并行处理能力强等诸多良好特性而受到研究人员的关注. 相比于基于数学问题的传统密码学, DNA密码不仅立足于数学问题, 同时也依赖于生物技术, 这使得DNA密码更加难以破译, 具有更高的安全性. 1994年, Adleman[35]进行了世界上第一个DNA计算实验并在《科学》杂志上发表了相关成果, 这一成果揭示了DNA分子除其稳定的遗传特性外还具有计算能力, 自此开辟了一个新的信息时代. 随着研究的深入, 新的以DNA为信息载体的密码学领域应运而生. 2000年, Leier等[36]基于DNA双链设计了两种密码学方法; 2003年, Chen[37]提出了基于碳纳米管的消息转换和DNA的分子密码学系统; 2005年, Chang等[38]提出了3种基于DNA的并行减法器, 正式验证了两个大质数的乘积能够被分解; 2007年, Lu等[39]通过将现代DNA生物技术微阵列应用于密码技术, 设计出对称密钥密码系统; 在Lu等研究成果的基础上, 2010年, Lai等[40]进一步提出了一种非对称加密和签名密码系统DNA-PKC; 2012年, Wei等[41]提出基于DNA序列操作和超混沌系统的彩色图像加密算法; 2017年, Niu等[42]提出基于超混沌映射和核苷酸序列数据库的图像加密算法. 通过前人对DNA密码学[43–45]的研究以及其在图像加密方面[46–48]的应用, 已构建了基本的DNA密码学逻辑结构, 为本文的研究提供了基础.

本文第2节介绍背景知识以及描述为完成提出算法进行的相关工作; 算法的具体实现过程在第3节进行详细描述, 包括了加密以及解密步骤; 随后在第4节中附上了仿真结果, 对提出的算法进行了性能分析.

2 相关工作

2.1 量子随机行走

量子随机行走包括连续时间量子随机行走和离散时间量子随机行走两个部分, 本文提出的工作以离散时间量子随机行走为工具进行开展. 离散时间量子随机行走主要包含4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. 本文应用离散时间交替量子随机行走 (如图1所示).

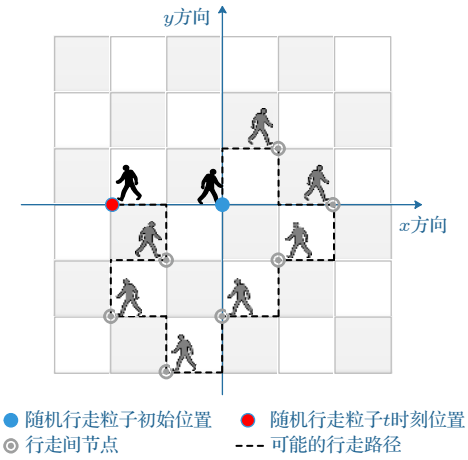

图 1 双方向格点上交替量子随机行走

Fig. 1. Alternating quantum random walking on the bidirectional grid.

量子随机行走由两部分构成, 即行走者位置空间$H_{\rm w}$和硬币空间$H_{\rm c}$二者共同构成量子随机行走体系的希尔伯特空间$\boldsymbol{H}=\boldsymbol{H}_{\rm w}\otimes\boldsymbol{H}_{\rm c}$. 在量子随机行走过程中, 每一步的行走选择相同的硬币抛掷算符$\hat{\boldsymbol{C}}$:

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

特别地, 当$\theta=\pi/4$时,

$$\hat{\boldsymbol{C}}=\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}. \tag{2}$$

硬币的抛掷完成后, 行走者的动态由条件位移算符$\boldsymbol{S}_{\rm i}$规定:

$$\boldsymbol{S}_{\rm i}\left|x\right\rangle=\left|x+(-1)^{c}\right\rangle,\ c=0,1, \tag{3}$$

其中$\left|x\right\rangle\,(x\in\mathbb{Z})$为构成行走者位置空间的基矢; 两个基矢$\left|c\right\rangle\,(c=0,1)$线性组合构成硬币空间. (3)式可以描述为: 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.

在本文用到的交替量子随机行走中, 行走者在x, y两个方向上交替进行行走, 则整个量子随机行走过程中的行走算符$\hat{\boldsymbol{U}}$可描述为

$$\hat{\boldsymbol{U}}=\hat{\boldsymbol{S}}_{y}\left(\boldsymbol{I}\otimes\boldsymbol{H}_{\rm c}\right)\hat{\boldsymbol{S}}_{x}\left(\boldsymbol{I}\otimes\boldsymbol{H}_{\rm c}\right), \tag{4}$$

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

$$\hat{\boldsymbol{S}}_y = \sum_{x,y}^{N}(|x,(y+1) \bmod N,0\rangle\langle x,y,0| + |x,(y-1) \bmod N,1\rangle\langle x,y,1|), \tag{5}$$

其中 N 表示位移算符在 y 轴上移动的格点数. $\hat{\boldsymbol{S}}_x$ 为量子随机行走在 x 轴各点行走的位移算符, 其描述与 $\hat{\boldsymbol{S}}_y$ 相同.

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

$$|\psi_0\rangle = |\varphi_0\rangle_{\rm w} \otimes (\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle)_{\rm c}. \tag{6}$$

量子随机行走进行 T 步后系统状态为

$$|\psi_T\rangle = \hat{\boldsymbol{U}}^T\,|\psi_0\rangle\,. \tag{7}$$

出现在坐标 $(x_x,\ y_y)$ 的概率为

$$P\,(x,y,T) = \left|\langle x,y,0|\,\hat{\boldsymbol{U}}^T\,|\psi_0\rangle\right|^2 + \left|\langle x,y,1|\,\hat{\boldsymbol{U}}^T\,|\psi_0\rangle\right|^2. \tag{8}$$

2.2 DNA 编码

在过去的研究中, 专家学者们已经构建了一套基本的 DNA 编码结构. 从生物模型出发, DNA 序列由以下 4 个核酸碱基组成: A (腺嘌呤), G (鸟嘌呤), C (胞嘧啶), T (胸腺嘧啶). 其中, A 与 T 互补, C 与 G 互补. 将以上的限制写入编码规则, 分别用 2 位二进制数对每个核酸碱基进行编码得到 8 种符合生物模型规则的编码方案, 如表 1 所列.

表 1 8 种 DNA 编码方案

Table 1. Eight DNA coding schemes.

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

注: 满足DNA的生物学特性A-T互补、G-C互补.

本文使用表 1 所述 DNA 编码规则对彩色图像进行编码. 首先将彩色图像拆分为 R, G, B 3 个色彩通道, 随即将每个通道编码为一个二进制矩阵, 对于单个通道的 8 位二进制矩阵可用 4 位 DNA 序列对其矩阵各数据进行编码. 例如: 红色通道第一位像素值为 157, 将其转换为二进制序列得到 10011101; 对此二进制序列使用表 1 中方案 1 进行编码则可得到长度为 4 的 DNA 序列——CGTG. 而对应相同的二进制序列可以选择不同的方案进行加密, 如对应上述二进制序列, 选择方案 5 对其进行编码则得到的 DNA 序列为 ATGT. 而在解码时, 若选择加密方案对 DNA 序列进行解码则会得到原二进制数据, 例如对方案 1 生成的 DNA 序列 CGTG 使用方案 1 进行解密则可得到 10011101, 为原始二进制序列; 而当使用方案 1 外的任意方案, 例如使用方案 4 对其解码, 此时对 DNA 序列 CGTG 进行解码得到的二进制序列为 00111011 与原二进制不同. 因此无法确定加密以及解密的 DNA 编码方案, 就无法得知原始二进制序列, 这是使用 DNA 编码加密的手段之一.

基于以上 8 种编码方案, 根据二进制传统加减法可以获得对应的 8 种 DNA 序列的加减法方案, 在此使用编码方案 1 对应的加、减法方案 1 进行举例, 具体如表 2 所列.

表 2 DNA 编码方案 1 对应的加法方案 1

Table 2. Addition plan 1 corresponding to DNA coding plan 1.

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

表 3 DNA 编码方案 1 对应的减法方案 1

Table 3. DNA coding scheme 1 corresponding to subtraction scheme 1.

−	A	G	C	T
A	A	G	C	T
G	T	A	G	C
C	C	T	A	G
T	G	C	T	A

从表 2 和表 3 可以看出, 相同 DNA 编码对应的加、减法结果是唯一对应的, 因此可以利用其加减规则对图像进行加密.

3 算法提出

本文提出的加密算法主要由以下几部分组成: 1) 通过改变参数 (N, T, α(硬币算符初态参数)、β(硬币算符抛掷参数)) 的大小控制交替量子随机行走产生与所需加密图像对应的随机概率分布矩

阵; 2) 通过将量子随机行走与 DNA 编码以及 DNA 运算相结合的方式完成对原图像的置乱加密; 3) 异或操作完成进一步加密. 下面展示具体算法.

3.1 加密过程

第一步: 将彩色图像 $(m,\ n,\ 3)$ 拆分为 3 个彩色通道矩阵: $\boldsymbol{R}(m,\ n)$, $\boldsymbol{G}(m,\ n)$, $\boldsymbol{B}(m,\ n)$, 并将 R, G, B 3 通道矩阵分别转换为二进制矩阵 $\boldsymbol{R}_1$, $\boldsymbol{G}_1$, $\boldsymbol{B}_1$, 然后执行 DNA 编码规则中的 a 方案 $(a\in\mathbb{Z},(1,8))$ 对 3 个二进制矩阵进行编码, 得到 3 个大小为 $(m,\ n\times 4)$ 的矩阵.

以下为加密步骤一对应算法 1 伪代码.

算法 1 图片三通道矩阵进行 DNA 编码

输入 图片 DNA 编码规则

输出 经过 DNA 编码后的图片三通道矩阵

function DNAcodingforImg (image)
  img_B img_G img_R ← image[0, : 0] image[0, : 1] image[0, : 2]
  $A=00,\ T=01,\ C=10,\ D=11$
  for $i=1$ to n **do**
    temp ← img_B_G_R[i]
    temp : Binarysystem ← Decimal system
    temp(ATGC) ← temp(Binarysystem)
  end for
  newImage ← img_B img_G img_R
  return newImage
end function

第二步: 利用交替量子随机行走, 通过设置其关键参数: $(N_1,\ T_1,\ \alpha,\ \beta)$ 生成随机概率分布矩阵 $\boldsymbol{P}$ (称作密钥矩阵), 并将其调整为加密图像的大小得到 $\boldsymbol{P}_1$:

$$\boldsymbol{P}_1=\text{resize}\left(\boldsymbol{P},[m\quad n]\right),\tag{9}$$

将得到的随机概率分布矩阵 $\boldsymbol{P}_1$ 中各元素按照 $k=\text{fix}\left(\text{Re}\boldsymbol{P}_1\times 10^{12}\right)\bmod 256$ 转换为 0—255 之间的十进制整数, 进而转换为 8 位二进制矩阵 $\boldsymbol{P}_2$.

以下为加密步骤二对应算法 2 伪代码.

算法 2 生成量子随机行走概率矩阵

输入 量子随机行走概率矩阵的关键参数 DNA 编码规则

输出 经过 DNA 编码后的量子随机行走概率矩阵

function DNAcodingforQW (N,T,α,β)
  coin0 ← $[1,0]$
  coin1 ← $[0,1]$
  Cosbeta ← $\cos(\alpha)$
  Sinbeta ← $\sin(\beta)$
  $\text{posn0}_x,\text{posn0}_y=\text{zeros}(P)$
  $\text{posn0}_x[N],\text{posn0}_y[N]=1$
  QWPmatrix ← Cosbeta, Sinbeta
  for $i=1$ to n **do**
    temp ← QWPmatrix[i]
    temp : Binarysystem ← Decimal system
    temp(ATGC) ← temp(Binarysy- stem)
  end for
  return QWPmatrix
end function

第三步: 将密钥矩阵中元素按降序排列获得向量 $\boldsymbol{V}$, 利用向量 $\boldsymbol{W}$ 检索向量 $\boldsymbol{V}$ 中 $\boldsymbol{P}_1$ 元素形成索引; 利用索引向量 $\boldsymbol{W}$ 完成对矩阵 $\boldsymbol{R}_1$, $\boldsymbol{G}_1$, $\boldsymbol{B}_1$ 的置乱重排生成 $(m,\ n\times 4)$ 的矩阵 $\boldsymbol{R}_2$, $\boldsymbol{G}_2$, $\boldsymbol{B}_2$.

以下为加密步骤三对应算法 3 伪代码.

算法 3 图像时域置乱

输入 量子随机行走概率矩阵 newImage

输出 时域置乱后的图像

function Matrixscrambling (QWPmatrix,image)
  QWPmatrixafterArgsort ← QWPmmtrix.argsort()
  newImage = zeros($\boldsymbol{P}$)
  for $i=1$ to n **do**
    temp ← QWPmatrixafterArgsort[i]
    newImage[i] = image[temp]
  end for
  return newImage
end function

第四步: 将矩阵 $\boldsymbol{P}_2$ 使用与矩阵 $\boldsymbol{R}_1$, $\boldsymbol{G}_1$, $\boldsymbol{B}_1$ 相同的 DNA 编码方案 a 进行编码, 得到矩阵 $\boldsymbol{P}_3$, 随后使矩阵 $\boldsymbol{R}_2$, $\boldsymbol{G}_2$, $\boldsymbol{B}_2$ 分别与矩阵 $\boldsymbol{P}_3$ 进行方案 a 的加法, 得到矩阵 $\boldsymbol{R}_3$, $\boldsymbol{G}_3$, $\boldsymbol{B}_3$, 即:

$$\boldsymbol{R}_3=\boldsymbol{P}_3+\boldsymbol{R}_2,\ \boldsymbol{G}_3=\boldsymbol{P}_3+\boldsymbol{G}_2,\ \boldsymbol{B}_3=\boldsymbol{P}_3+\boldsymbol{B}_2.\tag{10}$$

接着, 使用 DNA 编码规则中的方案 b $(b\in Z,(1,8),\ b\neq a)$ 对矩阵 $\boldsymbol{R}_3$, $\boldsymbol{G}_3$, $\boldsymbol{B}_3$ 进行解码操作, 得到 3 个二进制矩阵: $\boldsymbol{R}_4$, $\boldsymbol{G}_4$, $\boldsymbol{B}_4$.

以下为加密步骤四对应算法 4 伪代码.

算法 4 QWPmatrix 与 newImage 的 DNA 加法

输入 QWPmatrix newImage

输出 经过 DNA 加法处理后的矩阵

```
function DNAaddtion (QWPmatrix, image)
    QWPmatrixafterArgsort ← QWPmatrix.argsort()
    newImage = zeros(P)
    for i = 1 to n do
        temp ← QWPmatrixafterArgsort[i]
        newImage[i] = image[temp]
    end for
    return afterDNAaddtionImage
end function
```

第五步: 将矩阵 $\boldsymbol{R}_4$, $\boldsymbol{G}_4$, $\boldsymbol{B}_4$ 分别与 $\boldsymbol{P}_2$ 中对应元素进行按位异或运算得到矩阵 $\boldsymbol{R}_5$, $\boldsymbol{G}_5$, $\boldsymbol{B}_5$, 将三通道加密完成后的矩阵 $\boldsymbol{R}_5$, $\boldsymbol{G}_5$, $\boldsymbol{B}_5$ 组合获得加密后的彩色图像 E.

以上算法流程图见图 2.

3.2 解密过程

解密过程可视作加密过程的逆过程, 其步骤可简述为以下 4 步.

第一步: 使用与加密过程相同的参数进行离散时间交替量子随机行走, 生成随机概率矩阵 $\boldsymbol{P}'$, 随后对 $\boldsymbol{P}'$ 元素进行降序排列生成向量 $\boldsymbol{V}'$, 因参数相同, 所以有 $\boldsymbol{V}'=\boldsymbol{V}$, $\boldsymbol{P}'=\boldsymbol{P}$; 使用向量 $\boldsymbol{W}'$ 对向量 $\boldsymbol{V}'$ 中的元素进行检索索引;

第二步: 将加密后的彩色图像 E 拆分为 3 个色彩通道矩阵: $\boldsymbol{R}'$, $\boldsymbol{G}'$, $\boldsymbol{B}'$, 并进一步转换为 8 位二进制矩阵 $\boldsymbol{R}'_1$, $\boldsymbol{G}'_1$, $\boldsymbol{B}'_1$; 同时将 $\boldsymbol{P}'$ 中各元素转换为 0—255 之间的十进制整数, 随后转换为 8 位二进制数, 获得的矩阵 $\boldsymbol{K}'$ 进行按位异或运算得到矩阵 $\boldsymbol{R}'_2$, $\boldsymbol{G}'_2$, $\boldsymbol{B}'_2$;

第三步: 分别使用 DNA 编码规则中的方案 b ($b\in Z,(1,8),b\neq a$ 与加密中相同) 对矩阵 $\boldsymbol{R}'_2$, $\boldsymbol{G}'_2$, $\boldsymbol{B}'_2$ 进行编码操作得到 3 个 DNA 矩阵 $\boldsymbol{R}'_3$, $\boldsymbol{G}'_3$, $\boldsymbol{B}'_3$; 执行 DNA 编码规则中的 a 方案 ($a\in Z,(1,8)$ 与加密中相同) 对矩阵 $\boldsymbol{P}'$ 进行 DNA 编码, 获得矩阵 $\boldsymbol{P}'_1$; 执行加密方案中 DNA 加法方案对应的减法方案, 按照以下式子进行运算得到矩阵 $\boldsymbol{R}'_4$, $\boldsymbol{G}'_4$, $\boldsymbol{B}'_4$:

$$\boldsymbol{R}'_4=\boldsymbol{R}'_3-\boldsymbol{P}'_1,\ \boldsymbol{G}'_4=\boldsymbol{G}'_3-\boldsymbol{P}'_1,\ \boldsymbol{B}'_4=\boldsymbol{B}'_3-\boldsymbol{P}'_1; \tag{11}$$

第四步: 将 $\boldsymbol{R}'_4$, $\boldsymbol{G}'_4$, $\boldsymbol{B}'_4$ 根据向量 $\boldsymbol{W}'$ 反置乱重排得到矩阵 $\boldsymbol{R}'_5$, $\boldsymbol{G}'_5$, $\boldsymbol{B}'_5$, 三通道组合获得原始彩色图像, 解密完成.

4 仿真结果与分析

为验证所提算法的有效性与安全性, 本文进行算法实验仿真, 对像素大小 290 × 290 的 3 张彩色图片进行算法所述的加密以及解密操作, 效果见图 3, 并对加密前后图像进行像素相关性分析、直方图分析、密钥空间等安全性分析.

4.1 实验仿真

为验证本文所提方法的有效性, 进行了相关仿真实验. 实验应用了如下 3 个 290 × 290 像素的彩色图像, 在量子漫步部分选取 $N=500$, $\alpha=\dfrac{\pi}{2}$, $\beta=\dfrac{\pi}{3}$ 在 DNA 加密与加法计算部分选用了表 1 中编号 1 的编码方式与编号 3 的解码方式, 进行表 2 和表 3 所示的运算. 仿真结果与具体分析如下.

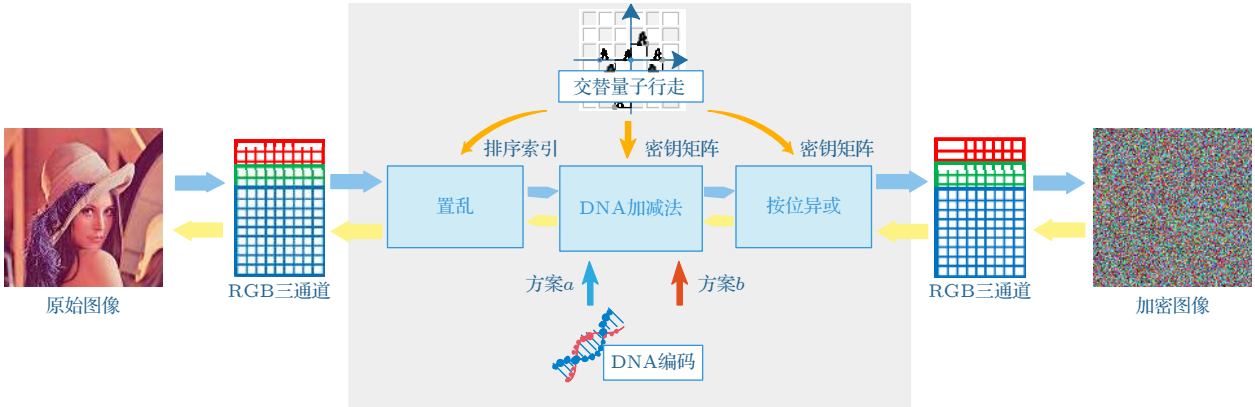

图 2 算法流程图

Fig. 2. Algorithm flowchart.

4.2 相关分析

相关分析首先采用相邻像素的相关性系数C_{AB}来分析原始图像与加密图像间的差异. 原始图像中相邻位置的像素具有很强的相关性, 而加密后图像相邻像素间应接近于零.

$$C_{AB}=\frac{\operatorname{cov}(A,B)}{\sqrt{D(A)}\sqrt{D(B)}}, \tag{12}$$

其中, A 和 B 分别表示相邻像素的值, $\operatorname{cov}(A,B)$ 为 A 和 B 的协方差, $\sqrt{D(A)}$ 和 $\sqrt{D(B)}$ 为 A 和 B 的方差. 这里对实验仿真中 3 组原始图像与解密图像分别进行水平、垂直、对角方向上的像素相关性分析, 结果如图 4—图 6 所示, 具体数据结果见表 4.

图 4(a)—图 4(c) 分别为 Lena 原始图像在水平、垂直、对角方向上的相关性分析, 图 4(d)—图 4(f) 为 Lena 加密后图像对应的水平、垂直、对角方向上相关性分析得到的图像. 可以清晰地看出原始图

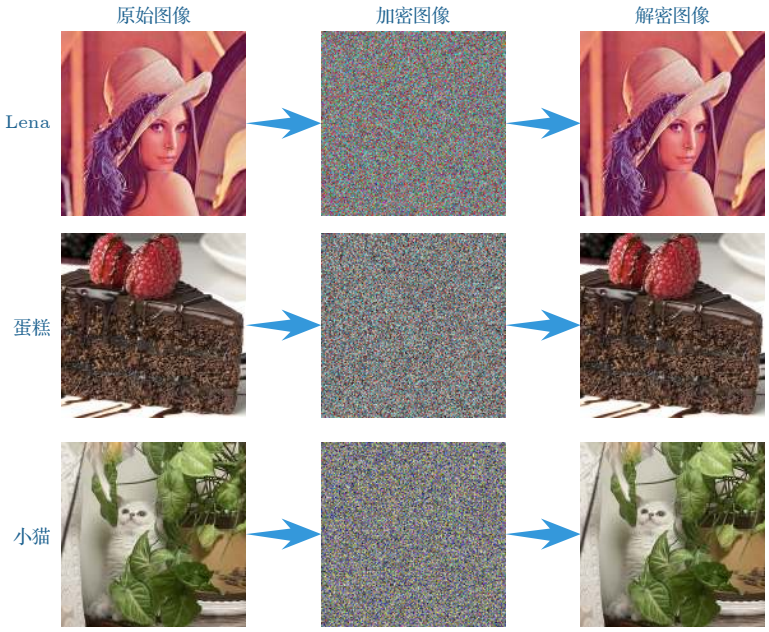

图 3 加密算法仿真效果图

Fig. 3. Encryption algorithm simulation renderings.

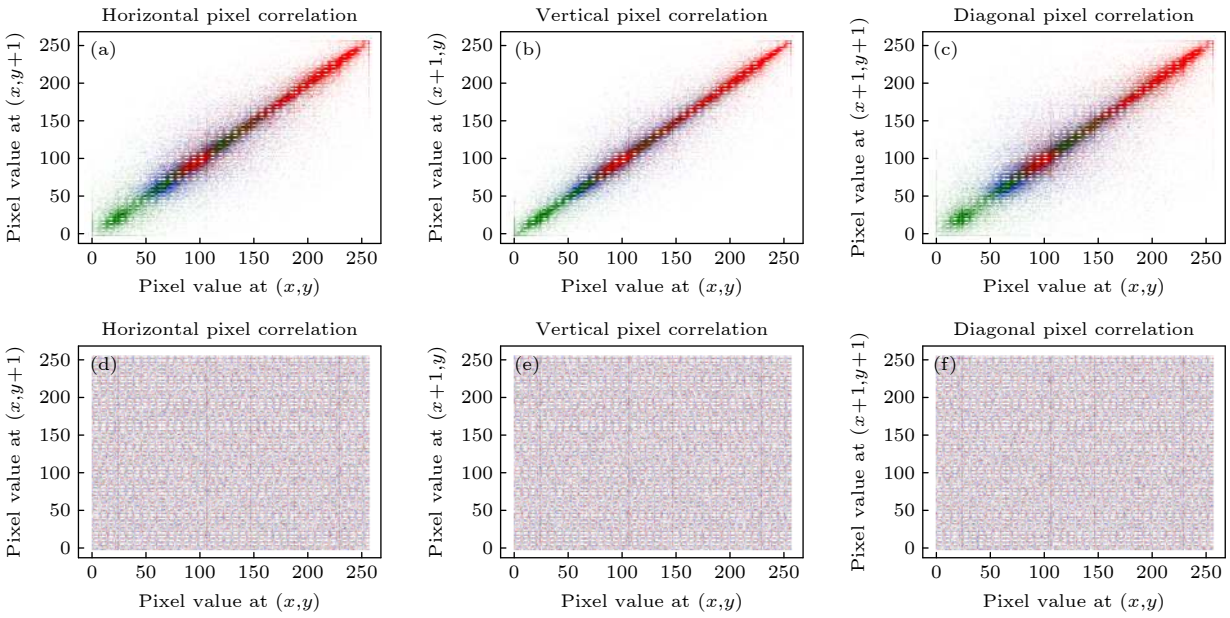

图 4 Lena 图像加密前后相关性分析

Fig. 4. Correlation analysis of images before and after Lena encryption.

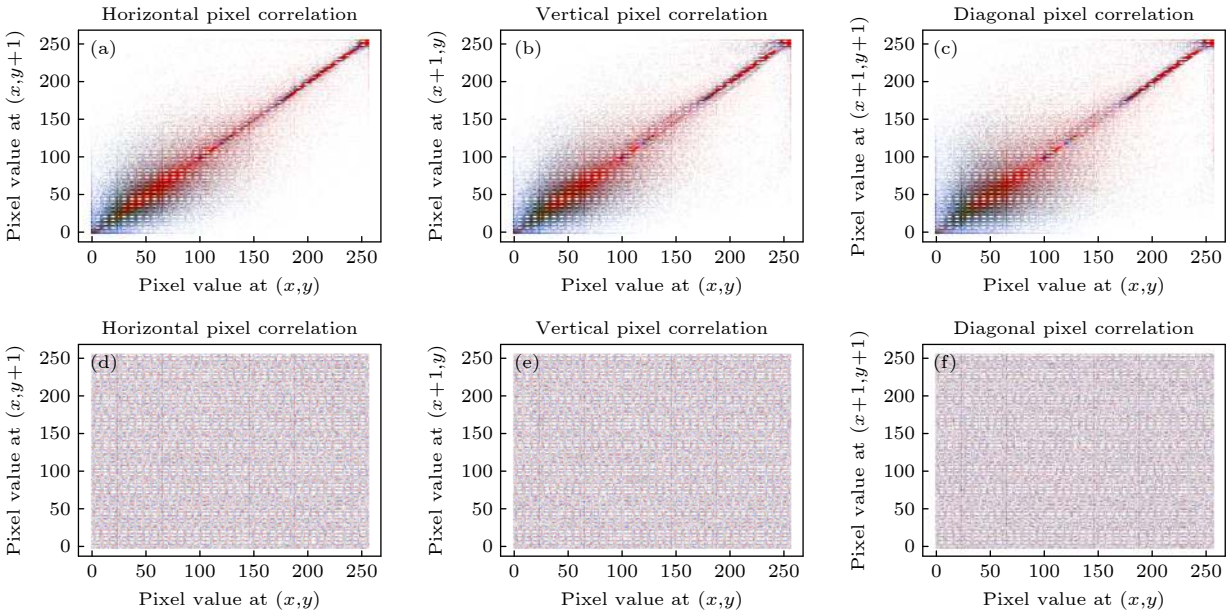

图 5 蛋糕图像加密前后相关性分析

Fig. 5. Correlation analysis of images before and after cake encryption.

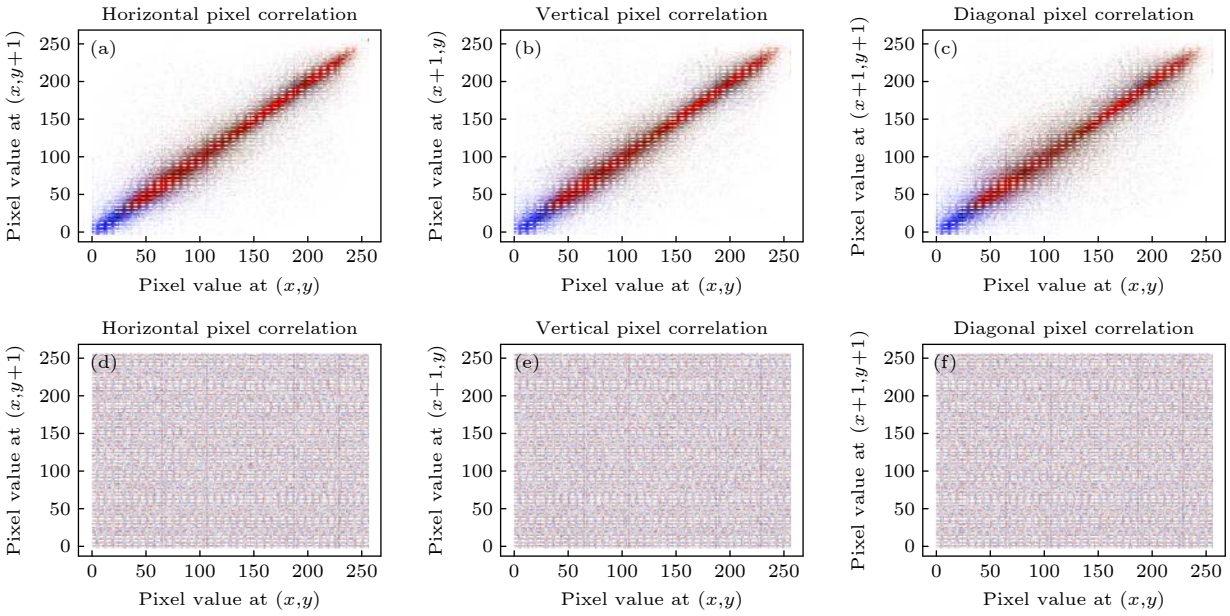

图 6 小猫图像加密前后相关性分析

Fig. 6. Correlation analysis of images before and after cat encryption.

像与加密后图像在像素相关性上的差别, 证明了所提算法的有效性.

从以上图表分析可以看出, 全部加密后图像的像素相关性分析的数值都接近于零, 因此本文所提算法有出色的抵御相关性分析的能力. 表 5 给出本文提出的算法与文献 [42,49,50] 提出算法的三方向相关性数据对比

密钥敏感性分析是指, 在图像加密过程中, 当密钥参数发生少量变化, 加密后的图像将会发生相应改变. 在这里用 NPCR (像素数改变率) 与 UACI (统一平均变化强度) 来表示对原始图像图像采用有微小区别的不同密钥加密后生成的加密图像之间的变化像素数量及其平均变化强度, 参考值分别为 NPCR = 99.6094%, UACI = 33.4635%, 其数值越接近该参考值说明算法密钥敏感性越强, 则该算法安全性更强. 相关数据见表 6.

表 7 给出本文与文献 [42, 49, 50] 的 NPCR, UACI 数据对比.

除此之外, 本文对原始图像和加密图像进行了统计分析, 图 7(a)—图 7(c) 为原始图像的 R, G, B 3 个通道的直方图, 图 7(d)—图 7(f) 对应的为加密图像的直方图. 可以看出左侧原始图像统计数据中 3 个通道各有一些值较为集中, 而右侧加密图像部分直方图数据较为均匀, 这表明想要对加密后图像进行统计攻击将会十分艰难.

表 4 像素相关性分析数据

Table 4. Pixel correlation analysis data.

图像	方向	数值	
		原始图像	加密图像
Lena	水平	0.9275	0.0017
	垂直	0.9603	–0.0005
	对角	0.8941	0.0007
小猫	水平	0.9429	0.0026
	垂直	0.9377	0.0009
	对角	0.9097	–0.0012
蛋糕	水平	0.9229	0.0076
	垂直	0.9056	0.0017
	对角	0.8647	0.0017

表 5 相关性分析数据对比

Table 5. Correlation analysis data comparison.

算法	通道	平均相关性
本文	Red	水平: 0.0040
	Green	垂直: 0.0010
	Blue	对角: 0.0012
文献[42]	Red	水平: 0.0042
	Green	垂直: 0.0033
	Blue	对角: 0.0024
文献[49]	Red	水平: 0.0025
	Green	垂直: 0.0010
	Blue	对角: 0.0022
文献[50]	Red	水平: 0.0012
	Green	垂直: 0.0011
	Blue	对角: 0.0032

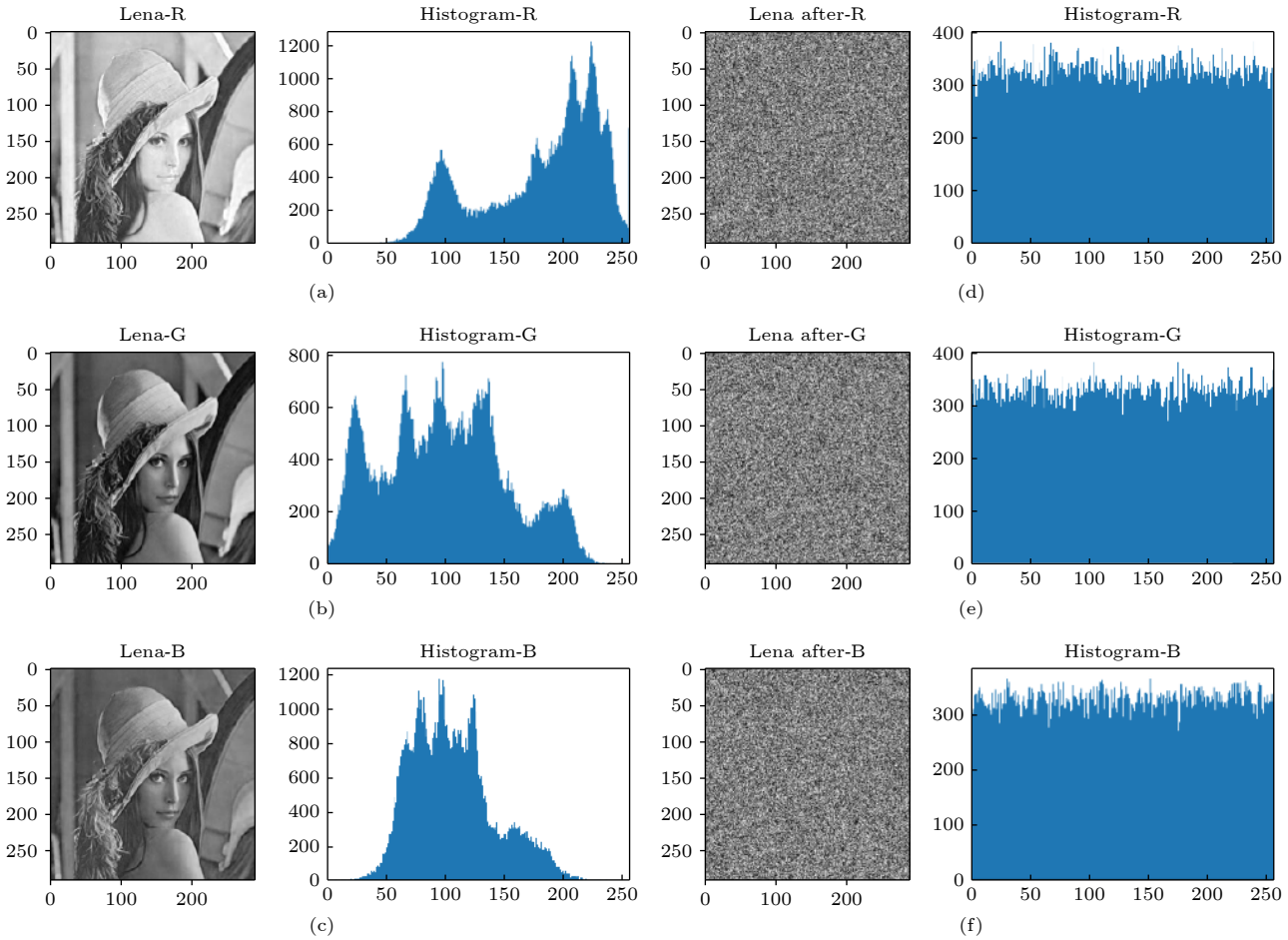

图 7 Lena 图像加密前后三通道直方图分析

Fig. 7. Analysis of R, G, B three-channel histogram before and after lena image encryption.

表 6 密钥敏感性分析数据

Table 6. Key sensitivity analysis data.

图像	通道	NPCR	UACI
Lena	Red	99.6040%	33.4005%
	Green	99.6195%	33.2311%
	Blue	99.5826%	33.5902%
小猫	Red	99.6326%	33.6785%
	Green	99.6124%	33.4455%
	Blue	99.6147%	33.5784%
蛋糕	Red	99.6124%	33.4461%
	Green	99.6528%	33.5315%
	Blue	99.7004%	33.4499%

表 7 NPCR, UACI 数据对比

Table 7. Comparison of NPCR and UACI data.

算法	NPCR平均	UACI平均
本文	99.6257%	33.4835%
文献[42]	99.5506%	33.4055%
文献[49]	99.6554%	33.4675%
文献[50]	99.6150%	33.3900%

Lena 图像加密后图像三通道信息熵分别达到: R 通道 7.9977, G 通道 7.9978, B 通道 7.9976; 三通道密钥随机性灰度差异(GVD)达到: R 通道 0.9667, G 通道 0.9551, B 通道 0.9651. 在密钥空间方面, 由于量子随机行走在理论上可以提供无穷大的密钥空间, 在实验中, 当计算精度为 10^{-16} 时, 密钥空间可以达到 2^{128}. 目前计算机计算能力决定, 当密钥空间达到 2^{128} 时算法可以抵御任何形式的暴力攻击, 因此算法具有较好的抵御穷举攻击等攻击手段的能力.

5 结 论

本文进行了量子漫步与图像加密结合的相关研究并进行了有效实验, 证实所提出的基于量子随机行走的彩色图像加密方案有效且切实可行, 表明将量子相关理论技术引入经典图像处理中具有广阔的应用前景; 此外将 DNA 编码应用于加密方案中更是为图像加密技术前景提供了一种可能. 在此次加密方案中, 量子随机行走生成的随机概率分布矩阵作为重要工具参与加密过程, 在之后的研究中希望能够更大程度地应用, 发挥其优势作用. 此外 DNA 编码所具备的重要生物特性也具有更加深度的应用意义.

参考文献

[1] Zheng R H, Xiao Y, Su S L, Chen Y H, Shi Z C, Song J, Xia Y, Zheng S B 2021 *Phys. Rev. A* **103** 052402
[2] Kang Y H, Shi Z C, Huang B H, Song J, Xia Y 2020 *Phys. Rev. A* **101** 032322
[3] Long G L 2001 *Phys. Rev. A* **64** 022307
[4] Long G L, Li X, Sun Y 2002 *Phys. Lett. A* **294** 143
[5] Li T, Zhang S, Fu X Q, Wang X, Wang Y, Lin J, Bao W S 2019 *Chin. Phys. B* **28** 120301
[6] Liu F, Zhang X, Xu P A, He Z X, Ma H Y 2020 *Int. J. Theor. Phys.* **59** 3491
[7] Zhou N R, Li J F, Yu Z B, Gong L H, A Farouk 2017 *Quantum Inf. Process.* **16** 1
[8] Gong L H, Li J F, Zhou N R 2018 *Laser Phys. Lett.* **15** 105204
[9] Hu X M, Huang C X, Sheng Y B, Zhou L, Liu B H, Guo Y, Zhang C, Xing W B, Huang Y F, Li C F, Guo G C 2021 *Phys. Rev. Lett.* **126** 010503
[10] Zhou L, Sheng Y B, Long G L 2020 *Sci. Bull.* **65** 12
[11] Yan Z H, Qin J L, Qin Z Z, Su X L, Jia X J, Xie C D, Peng K C 2021 *Fundam. Res.* **1** 43
[12] Zhao J B, Zhang W B, Ma Y L, Zhang X H, Ma H Y 2020 *Appl. Sci.* **10** 1935
[13] Qiu T H, Li H, Xie M, Liu Q, Ma H Y 2019 *Opt. Express* **27** 27477
[14] Ma H Y, Xu P A, Shao C H, Chen L B, Li J X, Pan Q 2019 *Int. J. Theor. Phys.* **58** 4241
[15] Li H S, Fan P, Xia H Y, Peng H L, Long G L 2020 *Sci. China Phys. Mech.* **63** 1
[16] Zheng R H, Kang Y H, Su S L, Song J, Xia Y 2020 *Phys. Rev. A* **102** 012609
[17] Ma H Y, He Z X, Xu P A, Dong Y M, Fan X K 2020 *Quantum Inf. Process* **19** 1
[18] Xu P A, He Z X, Qiu T H, Ma H Y 2020 *Opt. Express* **28** 12508
[19] Zhou N R, Huang L X, Gong L H, Zheng Q W 2020 *Quantum Inf. Process.* **19** 1
[20] Li H S, Fan P, Xia H Y, Peng H L, Long G L 2020 *Sci. China. Phys. Mech.* **63** 1
[21] Castagnoli G 2016 *Found Phys.* **46** 360
[22] Castagnoli G 2016 *Quanta* **5** 34
[23] Gong L H, Song H C, He C S, Liu Y, Zhou N R 2014 *Phys. Scr.* **89** 035101
[24] Li H H, Gong L H, Zhou N R 2020 *Chin. Phys. B* **29** 110304
[25] Aharonov Y, Davidovich L, Zagury N 1993 *Phys. Rev. A* **48** 1687
[26] Farhi E, Gutmann S 1998 *Phys. Rev. A* **58** 915
[27] Watrous J 2001 *Comput. Syst. Sci.* **62** 376
[28] Abd El-Latif A A, Abd-El-Atty B, Venegas-Andraca S E, Elwahsh H, Piran M J, Bashir A K, Song O, Mazurczyk W 2020 *IEEE Access* **8** 92687
[29] Abd-El-Atty B, Iliyasu A M, Alaskar H, Abd El-Latif A A 2020 *Sensors* **20** 3108
[30] Abd EL-Latif A A, Abd-El-Atty B, Venegas-Andraca S E 2020 *Physica A* **547** 123869
[31] Abd El-Latif A A, Abd-El-Atty B, Elseuofi S, Khalifa H S, Alghamdi A S, Polat K, Amin M 2020 *Physica A* **541** 123687
[32] Abd-El-Atty B, Amin M, Iliyasu A M 2020 *Sci. Rep.* **10**
[33] Godsil C, Zhan H 2019 *J. Comb. Theory Ser. A* **167** 181
[34] Abd-El-Atty B, Iliyasu A M, Alanezi A, Abd EL-Latif A A 2021 *Opt. Lasers Eng.* **138** 106403
[35] Adleman L M 1994 *Science* **266** 1021

[36] Leier A, Richter C, Banzhaf W, Rauhe H 2000 *Biosystems* **57** 13
[37] Chen J 2003 *Proceedings of the 2003 International Symposium on Circuits and Systems* ISCAS'03. IEEE 2003 **3** III-III.
[38] Chang W L, Guo M, Ho M S H 2005 *IEEE Trans Nanobiosci.* **4** 149
[39] Lu M X, Lai X J, Xiao G Z, Qin L 2007 *Sci. China Inf. Sci.* **50** 324
[40] Lai X J, Lu M X, Qin L, Han J S, Fang X W 2010 *Sci. China Inf. Sci.* **53** 506
[41] Wei X, Guo L, Zhang Q, Zhang J, Lian S G 2012 *J. Syst. Softw.* **85** 290
[42] Niu Y, Zhang X, Han F 2017 *Comput. Intell. Neurosci.* **2017**
[43] Kalsi S, Kaur H, Chang V 2018 *J. Med. Syst.* **42** 1
[44] Basu S, Karuppiah M, Nasipuri M, Halder A K, Radhakrishnan 2019 *J. Syst. Archit.* **94** 24
[45] Biswas M R, Alam K M R, Tamura S, Morimoto Y 2019 *J. Syst. Archit.* **48** 102363
[46] Huang L, Wang S, Xiang J, Sun Y 2020 *Math. Prob. Eng.* **2020**
[47] Alghafis A, Firdousi F, Khan M, Batool A L, Amin M 2020 *Math. Comput. Simul.* **177** 441
[48] Eswaran P, Shankar K 2017 *Int. J. Pure Appl. Math.* **118** 393
[49] Lu Q, Zhu C, Deng X 2020 *IEEE Access* **8** 25664
[50] Wang Y, Ye S C, Wang Y 2020 *Microelectron. Comput.* **37** 71

Color image encryption algorithm based on DNA code and alternating quantum random walk*

Wang Yi-Nuo [1)] Song Zhao-Yang [2)] Ma Yu-Lin [2)]
Hua Nan [2)] Ma Hong-Yang [1)†]

1) (*School of Science, Qingdao University of Technology, Qingdao* 266520, *China*)

2) (*School of Information and Control Engineering, Qingdao University of Technology, Qingdao* 266520, *China*)

(Received 5 July 2021; revised manuscript received 4 August 2021)

Abstract

In recent years, image encryption technology has attracted much attention. As people pay more attention to communication privacy and network security, the requirements for information encryption technology are more stringent. As one of the information carriers, images are valuable for carrying the effectiveness and vividness of the information. This paper proposes a color image encryption algorithm based on DNA encoding and alternating quantum random walk. Quantum random walk is an excellent cryptographic tool that participates in all parts of the algorithm process, and DNA encoding is used as the core encryption method to complete the algorithm. This article describes the encryption and decryption process in detail, and conducts simulation experiments to verify and analyze the results of the proposed algorithm. In the simulation stage, we design the simulation key parameters, encode the color image encryption and decryption experiments, and carry out related analysis. The experimental results show that the color image encryption algorithm proposed in this paper can perform safe and effective color image encryption. The correlation analysis shows that the image histogram after encryption is stable, the pixel correlation coefficient approaches 0, and the key space is 2^{128}, the three-channel information entropy reaches more than 7.997, which can resist statistical attacks, brute force attacks and other attack methods. In addition, DNA coding has unique biological characteristics in addition to the novel coding and calculation methods, which provide new ideas and directions for cryptographic research.

Keywords: quantum information, quantum random walk, image encryption, DNA coding

PACS: 03.65.–w, 03.67.Ac, 03.67.Dd, 42.50.Ex **DOI:** 10.7498/aps.70.20211255

* Project supported by the National Natural Science Foundation of China (Grant Nos. 11975132, 61772295), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2019YQ01), and the Higher Educational Science and Technology Program of Shandong Province, China(Grant No. J18KZ012).

† Corresponding author. E-mail: hongyang_ma@aliyun.com