基于量子随机行走和多维混沌的三维图像加密算法*

刘瀚扬[1)] 华南[1)] 王一诺[2)] 梁俊卿[1)] 马鸿洋[2)†]

1) (青岛理工大学信息与控制工程学院, 青岛 266520)

2) (青岛理工大学理学院, 青岛 266520)

(2022 年 3 月 15 日收到; 2022 年 4 月 14 日收到修改稿)

随着互联网的发展, 人们对于信息安全的需求日益增加, 而经典的加密技术存在着密钥空间小、易破解的缺陷, 图像加密技术在保护图像信息安全和隐私内容等方面的问题亟待解决. 量子随机行走作为一种新型量子密钥生成器, 其密钥空间大, 与经典随机行走相比计算速度与安全性有着明显的提高. 本文提出一种基于量子随机行走并涉及 Lorenz 和 Rossler 多维混沌的三维图像加密算法. 首先应用高斯金字塔对图像进行处理然后按照一定比例将处理后的图像切割成 4 份; 其次使用量子随机行走生成的随机序列与多维混沌中的 Lorenz 混沌系统生成的随机序列对分成的若干块子图像进行汉明距离计算然后进行合成, 并且对图像 RGB 三通道之间进行欧氏距离计算; 最后将汉明距离与欧式距离取余得到的序列值作为初始值输入多维混沌中的 Rossler 系统, 生成随机序列作为密钥对图像的 RGB 通道进行异或操作得到加密后的图像, 对应解密方案为加密过程逆过程. 此外, 本文采用基于离散余弦变换和奇异值分解的盲水印嵌入算法将水印信息嵌入到加密后的图像中, 实现接收方可以通过提取水印, 根据水印信息的完整性来判断传输过程中图像是否遭受到攻击破坏, 如无遭受恶意攻击, 则对图像进行解密操作. 这一操作完善了对图像信息安全的保护. 实验结果表明加密后图像的峰值信噪比稳定在 7—9 之间加密效果较好, 灰度差评分接近 1, 加密图像的相关性均匀分布, 其相关性系数接近 0, 密钥空间 2^{128} 且加密后的直方图分布均匀, 具有较高的抵御统计分析攻击的能力.

关键词: 量子随机行走, 混沌模型, 图像加密, 盲水印

PACS: 03.65.–w, 03.67.Ac, 03.67.Dd, 95.10.Fh **DOI**: 10.7498/aps.71.20220466

1 引 言

随着互联网的普及, 暴露在公共网络通信中的文字、音频、图像、视频等易受到第三方恶意攻击和窃听, 因此通过加密数字图像保护图像信息安全和隐私内容显得极为重要.

量子密码学[1–4]作为经典密码与量子力学原理相结合的产物在加密通信等方面有着巨大的作用. 在过去的几十年里, 经典的随机行走和马尔可夫链被用作发展计算机科学和数学算法的框架. 量子力学原理与经典的随机行走相结合, 提供了一种新的模式, 即量子随机行走. 1687 年, Aharonov 等[5]最早提出了一维量子随机行走, 利用量子态相干性使得量子随机行走比经典随机行走扩散速度更快. 随着研究的发展, Farhi 和 Gutmann[6] 于 1998 年提出了连续时间量子随机行走的概念, 在量子随机行走的研究道路上起着重要的作用; Childs 等[7]

* 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)、山东省高等教育科技计划项目 (批准号: J18KZ012) 和山东省自然科学基金联合基金 (批准号: ZR202108020011) 资助的课题.

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

© 2022 中国物理学会 Chinese Physical Society

于 2003 年提出了一种连续时间的量子随机行走算法. 量子随机行走算法被证明相比于经典算法具有指数级的速度[8,9]和更高的安全性[10,11]. 2001 年, Watrous[12]将经典随机行走量子化, 得到了离散时间量子随机行走的概念. 从此, 量子随机行走的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. 其中, 离散时间量子随机行走具有不确定性, 被广泛应用于量子及经典密码学中[13−19]. Gods 和 Zhan[20]在 2019 年以组合方法构建的三个离散时间量子行走模型和 2021 年 Singh 等[21]进行的离散时间量子游走的通用量子计算为本文提供了思想基础, Tsafack 等[22]于 2020 年发表的基于量子随机行走的光学图像加密算法和 2021 年王一诺等[23]发表的基于 DNA 编码与交替量子随机行走的彩色图像加密算法给本文提供了重要的研究方向. 本文采用量子随机行走算法来产生随机序列, 与混沌模型相结合, 整合出新的混合的随机密钥串, 提高加密安全性.

混沌系统[24]具有较难预测性、初始值敏感性等特性, 在密码学领域得到了极大的应用[25−28]. 利用混沌系统产生的随机序列对二进制的数据流图像信息进行加密, 具有抗攻击能力强、安全性高的特点. Assad 和 Farajallah[29]提出利用混沌伪随机数生成器在加密或解密图像过程中产生稳健的较长的一串离散值序列, 进而控制参数的变化, Wang 等[30]提出一个以幂指数函数和模运算的结构集成的混沌系统, 针对彩色图像的三通道 RGB 分量中的像素位置置乱达到加密效果. Kumar 等[31]提出利用 DNA密码规则将图像的 RGB 通道中的像素值转换为 DNA 序列. 在像素层面上使用 Lorenz-Rossler 混沌系统对新生成的 DNA 序列行扩散操作, 在 bit 层面上二维 (2D) logistic 映射用于在混淆阶段对扩散后的 RGB 通道执行按位混沌马尾处理, Huang 等[32]利用 Rolsser 超混沌系统生成扰乱和扩散矩阵, 提出一种基于 Rossler 超混沌和压缩感知技术的双图像压缩-加密算法. Rakesh 等[33]利用混沌系统的混淆和扩散特点, 在图像加密算法中表现出良好的性能. Huang 和 Ye[34]利用置换扩散的经典结构和双二维混沌系统, 设计了一种高效的自适应混沌图像加密算法模型, 有效地抵抗选择明文和已知明文攻击, 具有较高的安全性. Wang 等[35]通过随机密钥对混沌系统的初始值和控制参数进行初始化, SHA-512 算法对图像像素点的坐标进行置换, 使加密后的图像与原始图像产生混淆关系, 设计了一个基于分割的图像排列策略和一个包含三个模型的有效图像扩散策略方案, 通过仿真实验, 验证该算法的鲁棒性和对蛮力攻击、统计分析攻击、明文攻击、差分攻击的有效性. Zhou 等[36]通过 SHA-512 哈希函数和随机小数点序列生成与明文相关的密钥流, 以及基于 ncc 的位级图像混淆和扩散操作, 增加了密钥空间和动态密码特性, 提出的新型图像加密的组合混沌系统具有良好的混沌特性和安全性.

2 相关工作

2.1 量子随机行走

量子随机行走作为一种新型的密钥生成器, 密钥空间大, 量子随机行走拥有优于经典的特性, 其携带信息的量子态的扩散速度与经典相比有二次方的增长.

量子随机行走主要由硬币空间 $\mathcal{H}^{\mathrm{wC}}$ 和行走者的位置空间 $\mathcal{H}^{\mathrm{wP}}$ 组成, 因此量子随机行走的作用空间为 $\mathcal{H}=\mathcal{H}^{\mathrm{wC}}\otimes\mathcal{H}^{\mathrm{wP}}$. 量子随机行走的过程分为两步, 第一步是硬币算子作用在二维希尔伯特空间 $\mathcal{H}^{\mathrm{wC}}$ 的硬币态上, 之后把酉算子作用在量子随机行走的希尔伯特空间 $\mathcal{H}$ 上, 行走者根据硬币态的状态进行下一步行走. 假定量子随机行走硬币算符始终选择相同的算符 $\widehat{C}$:

$$\widehat{C}=\begin{pmatrix}\cos\theta & \sin\theta\\ \sin\theta & -\cos\theta\end{pmatrix}, \tag{1}$$

当 $\theta=\dfrac{\pi}{4}$ 时, 硬币算符 $\widehat{C}=\dfrac{\sqrt{2}}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

转移算符 R 在量子随机行走中的作用是根据硬币态的状态决定行走者下一步行走的方向. 当硬币态为 $|0\rangle$ 时, 行走者将向某一方向前进一步; 当状态为 $|1\rangle$ 时, 行走者将向反方向前进一步, 转移算符 R 可以表示为

$$R=|0\rangle\langle 0|\otimes\sum|a+1\rangle\langle a|+|1\rangle\langle 1|\otimes\sum|a-1\rangle\langle a|. \tag{2}$$

一维空间的量子随机行走的每一步操作都可以用全局 U 来表示:

$$U=RC=R(\widehat{C}\otimes I). \tag{3}$$

在交替量子随机行走中 $\mathcal{H}^{\mathrm{wP}}$ 是由位置态 $\{|\boldsymbol{x},\boldsymbol{y}\rangle, x,y\in Z\}$ 张量而成, 在二维空间内两个方向

交替行走. 因此在量子随机行走过程中, 反复作用于量子随机行走系统的酉算子可以表示为

$$\hat{U} = \hat{R}_y(I \otimes \hat{C})\hat{R}_x(I \otimes \hat{C}), \tag{4}$$

$$\widehat{R}_y = |0\rangle\langle 0| \otimes \sum_{b,a\in Z} |a+1,b\rangle\langle a,b| + |1\rangle\langle 1| \otimes \sum_{b,a\in Z} |a-1,b\rangle\langle a,b|, \tag{5}$$

$$\widehat{R}_x = |0\rangle\langle 0| \otimes \sum_{b,a\in Z} |a,b+1\rangle\langle a,b| + |1\rangle\langle 1| \otimes \sum_{b,a\in Z} |a,b-1\rangle\langle a,b|. \tag{6}$$

当硬币态是$|0\rangle$或者$|1\rangle$时, $\widehat{R}_y$作用于行走者, 使其沿 y轴向上 (向下) 行走, $\widehat{R}_x$作用于行走者, 使其沿 x轴向右 (向左) 行走, 如图 1 所示.

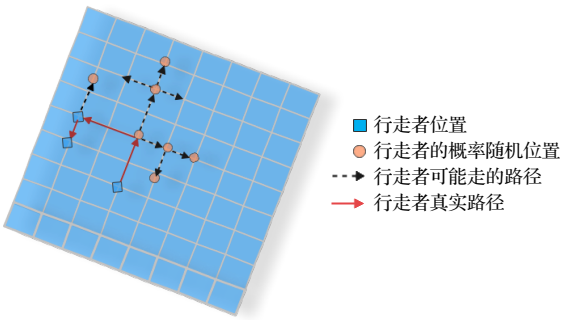

图 1 量子随机行走

Fig. 1. Quantum random walk.

假设初始时刻行走者局域在位置$(x,y)=(0,0)$处, 初始量子随机行走的量子态则可以表示为$|\psi_0\rangle = |00\rangle \otimes (\cos\theta|0\rangle + \sin\theta|1\rangle)$, 行走 N_{step}步之后, 整个体系最终的量子态为$\left|\psi_{N_{\text{step}}}\right\rangle = \hat{U}^{N_{\text{step}}}|\psi_0\rangle$, 在位置$(x,y)$发现行走者的概率为

$$P_{x,y,N_{\text{step}}} = \sum \left|\langle x,y,0|\,\hat{U}^{N_{\text{step}}}|\psi_0\rangle\right|^2 + \sum \left|\langle x,y,1|\,\hat{U}^{N_{\text{step}}}|\psi_0\rangle\right|^2. \tag{7}$$

2.2 Rossler 混沌模型

相比低维的混沌模型, Rossler 结构更为复杂, 抵御攻击能力更强, 具有一个非线性项, 可以由含参数的三维 (3D) 非线性常微分方程组组成, 其具体形式为

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = -\omega y - z, \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = \omega x + \eta y, \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = \tau + z(x-\gamma), \end{cases} \tag{8}$$

其中, ω, η, τ, γ为系统的参数. 本文称 ω为自然频率, 是表征系统在没有外界干扰时转动快慢的量, 如图 2 所示.

Rossler 振子在混沌动力学中也是研究比较多的一个模型. 但用单一的混沌模型生成的随机序列来对图像加密易被破解, 抗攻击性能差.

2.3 Lorenz 混沌模型

Lorenz 混沌模型也可以由三个含参数的非线性常微分方程组组成, 其形式为:

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = \sigma(y-x), \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = \rho x - y - xz, \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = xy - \mu z, \end{cases} \tag{9}$$

其中 三个参数分别为普朗特数 σ, 瑞利数 ρ, 方向比 μ, 如图 3 所示.

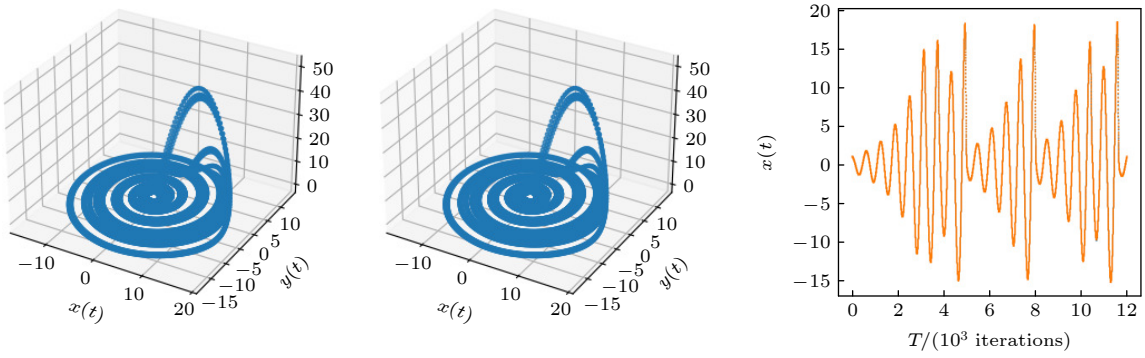

图 2 Rossler 混沌模型

Fig. 2. Rossler chaotic model.

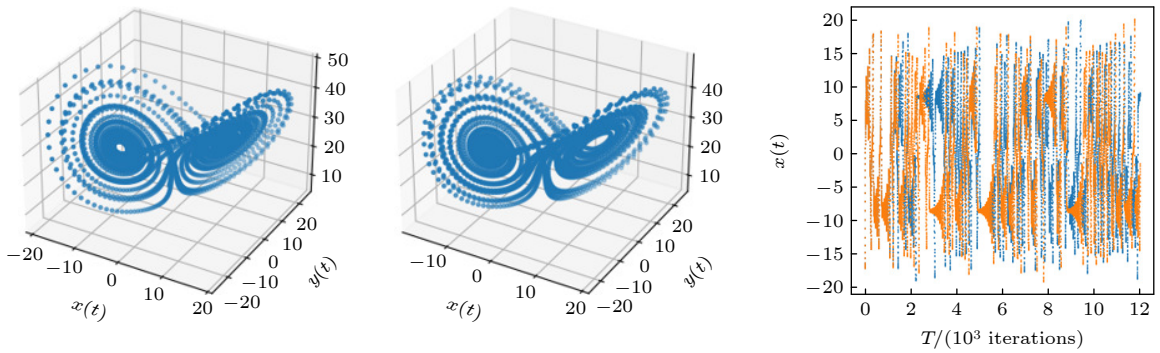

图 3 Lorenz 混沌模型

Fig. 3. Lorenz chaotic model.

3 算法流程

基于上述 Lorenz 和 Rossler 混沌模型及量子随机行走的理论, 得出基于量子随机行走和多维混沌的三维图像加密算法的流程分为 7 个步骤: 图像分割, 概率矩阵的生成与转化, Arnold 置乱, 利用欧式距离与汉明距离求序列, 密钥的生成, 以及传输过程中的盲水印的嵌入和提取.

3.1 图像分割

高斯金字塔是为了以多分辨率来解释图像而诞生的一种简单有效的方法. 本文采用高斯金字塔进行图像分割, 作为加密步骤前的处理工作, 将处理后的图像按照一定比例切割成若干份, 分块加密与整体加密相比提升了图像的安全性能. 高斯金字塔主要分成两个步骤: 第一步对图像做低通滤波, 达到平滑效果; 第二步对得到的平滑帧图, 做下抽样, 即可获得一系列的缩小的图像. 将这些图像组合在一起, 构造出高斯金字塔.

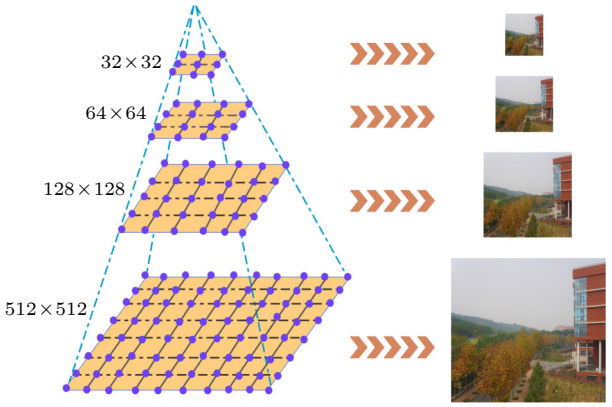

图 4 高斯金字塔结构图

Fig. 4. Gaussian pyramid structure.

高斯金字塔是通过对一张图采用逐级下采样来获得的. 最下层是原始图片, 越往上图的尺寸越小, 如图 4 所示.

$$A_z(x,y)=\sum_{m=-2}^{2}\sum_{n=-2}^{2}w(m,n)A_{z-1}(2x+m,2y+n), \tag{10}$$

其中 $A_z(x,y)$ 为第 z 层高斯金字塔图像; A_0 为原始图像; $A_1,\cdots,A_z$ 表示高斯金字塔的第一层到第 z 层. $w(m,n)=h(m)h(n)$ 是有低通特性的窗口函数, 其中 h 为高斯密度分布函数.

3.2 概率矩阵的生成与转化

根据上述量子随机行走理论, 设定最适合的参数 (N_{step}, P, λ_1, λ_2), 得到二维量子随机行走生成概率分布 P.

$$P_{x,y,N_{\text{step}}}=\sum\left|\langle x,y,0|\,\hat{U}^{N_{\text{step}}}\,|\psi_0\rangle\right|^2+\sum\left|\langle x,y,1|\,\hat{U}^{N_{\text{step}}}\,|\psi_0\rangle\right|^2, \tag{11}$$

$$|\psi_0\rangle=|00\rangle\otimes(\cos a|0\rangle+\sin a|1\rangle), \tag{12}$$

$$M=(P_{x,y,N_{\text{step}}}\times C)\bmod 2^k, \tag{13}$$

其中, (x,y) 为行走者出现的坐标位置, N_{step} 为步数, $|\psi_0\rangle$ 为行走者的初始状态算符, λ_1 为硬币算法初态参数, λ_2 是硬币算符抛掷参数, $\hat{U}$ 为行走算符, C 为整数, k 表示每一个位置所生成随机数的二进制位数. 将所有的余数排序得到 Z_1 取长为 L 的片段为信息 M_1, 重复上述步骤 g 次得到 $M_2,M_3,\cdots,M_g$, 即所得随机序列 $m=M_1,M_2,M_3,\cdots,M_g$.

3.3 Arnold 置乱

二维 Arnold 变换因其变换简单、有周期性的

特点常被用来进行置乱图像操作, 本文首先对彩色图像的三通道进行分离, 然后针对分离后的三通道灰度图的各个像素点做 x 轴方向的错位切换, 再做 y 轴方向的错位切换, 并按照 (14) 式进行模运算, 达到图像置乱的效果. Arnold 映射方程为

$$\begin{bmatrix} x'_{i+1} \\ y'_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & W \\ V & WV+1 \end{bmatrix} \begin{bmatrix} x'_i \\ y'_i \end{bmatrix} \bmod (O), \tag{14}$$

其中 (x'_i, y'_i) 为原图像像素坐标点, (x'_{i+1}, y'_{i+1}) 为置乱后图像像素坐标点, W 和 V 为设定的参数, i 表示当前变换的次数, mod 为取模运算, O 为正方形图像的宽度. 以分割后图像中的一张为例进行研究, 如图 5 所示.

3.4 利用欧式距离与汉明距离求序列

欧式距离是衡量多维空间中两个点之间的绝对距离的常见度量方式. 将序列 $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 看作 n 维空间点 α, 将 $\beta = (\beta_1, \beta_2, \cdots, \beta_n)$ 看作 n 维空间点 β, 根据 n 维空间的欧式距离得到 α 与 β 的欧式距离并对得到的欧式距离让其结果在 (0—255) 之间:

$$d_i = \sqrt{\sum_{k=1}^{n} (\alpha_i - \beta_i)^2 D_i} = |\bmod|(d_i, 256). \tag{15}$$

基于 (15) 式得到 R, G, B 三通道的欧式距离 D_{RG}, D_{RB}, D_{GB},

$$D = [D_{\mathrm{RG}}, D_{\mathrm{RB}}, D_{\mathrm{GB}}, D_{\mathrm{RG}}, D_{\mathrm{RB}}, D_{\mathrm{GB}}, D_{\mathrm{RG}}, D_{\mathrm{RB}}, D_{\mathrm{GB}}]. \tag{16}$$

根据序列 $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 和 $\beta = (\beta_1, \beta_2, \cdots, \beta_n)$, 得到汉明距离的定义为

$$\begin{cases} H(\alpha, \beta) = \sum_{i=1}^{n} h(\alpha_i, \beta_i), \\ h(\alpha_i, \beta_i) = \begin{cases} 0, \alpha_i = \beta_i, \\ 1, \alpha_i \neq \beta_i. \end{cases} \end{cases} \tag{17}$$

利用 Lorenz 混沌模型, 设定适当参数和初始值生成随机序列 $q = Q_1, Q_2, Q_3, \cdots, Q_g$.

将 3.2 节概率矩阵的生成与转化中得到量子随机行走生成的随机序列 m 与 Lorenz 混沌系统生成的混沌序列 q 的长度进行比较, 即

$$\begin{aligned} \text{if } \ & \mathrm{Num_{walk}} \geqslant \mathrm{Num_{lorenz}}, \\ & \mathrm{Num_{walk}} = \mathrm{Num_{lorenz}}, \\ \text{else } \ & \mathrm{Num_{walk}} < \mathrm{Num_{lorenz}}, \\ & \mathrm{Num_{lorenz}} = \mathrm{Num_{walk}}. \end{aligned} \tag{18}$$

基于汉明距离公式和上述判断公式将步骤二中得到量子随机行走生成密钥和 Lorenz 混沌模型生成的密钥进行汉明距离求值得到:

$$H = [H_{(m_1,q_1)}, H_{(m_2,q_2)}, H_{(m_3,q_3)}, H_{(m_4,q_4)}, H_{(m_5,q_5)}, H_{(m_6,q_6)}, H_{(m_7,q_7)}, H_{(m_8,q_8)}, H_{(m_9,q_9)}]. \tag{19}$$

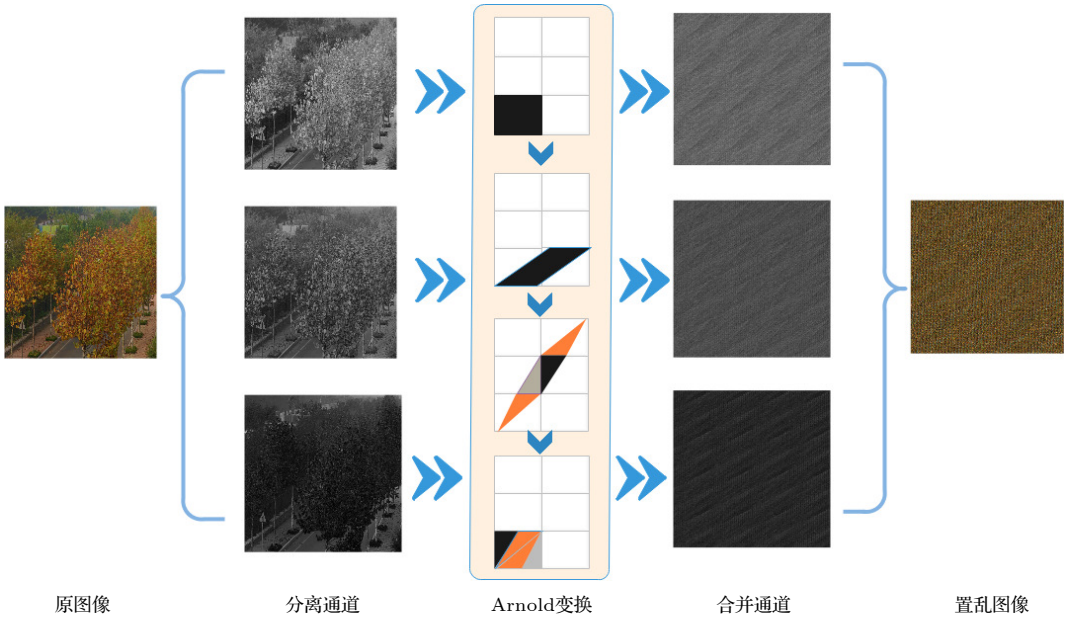

图 5 Arnold 变换

Fig. 5. Arnold transform.

3.5 密钥的生成

将 3.4 节利用欧式距离与汉明距离求序列中得到的汉明距离 H 与欧式距离 D 取余, 即

$$\text{Key} = |\bmod|(D, H), \tag{20}$$

其中 Key 是一个长度为 9 的序列, 将 Key 均分成三份, 得到 $\widetilde{\text{Key}}$:

$$\widetilde{\text{Key}} = [\widetilde{\text{Key}_1}, \widetilde{\text{Key}_2}, \widetilde{\text{Key}_3}], \tag{21}$$

$$\widetilde{\text{Key}_i} = [\text{Key}_{3i-2}, \text{Key}_{3i-1}, \text{Key}_{3i}],\ (i = 1, 2, 3). \tag{22}$$

将得到的 $\widetilde{\text{Key}}$ 作为初始值输入到 Rossler 混沌模型中, 得到新的 Rossler 混沌模型的随机序列 $\widetilde{q} = \widetilde{Q}_1, \widetilde{Q}_2, \widetilde{Q}_3, \cdots, \widetilde{Q}_g$; 其中 Rosser 混沌模型生成的混沌序列是浮点数值, 需要将每个通道中的像素值修改为 0—255 的整数, 整数伪随机数序列转换公式如下:

$$t_i = \text{fix}\left(\bmod\left(s_i \times 10^{12}, 256\right)\right), \tag{23}$$

其中, s_i 是来自两个混沌系统的混沌序列. 然后对原始图像进行 Arnold 变换来进行置乱; 最后将得到的随机序列与置乱后的图像进行异或操作进行加密和解密, 如图 6 所示.

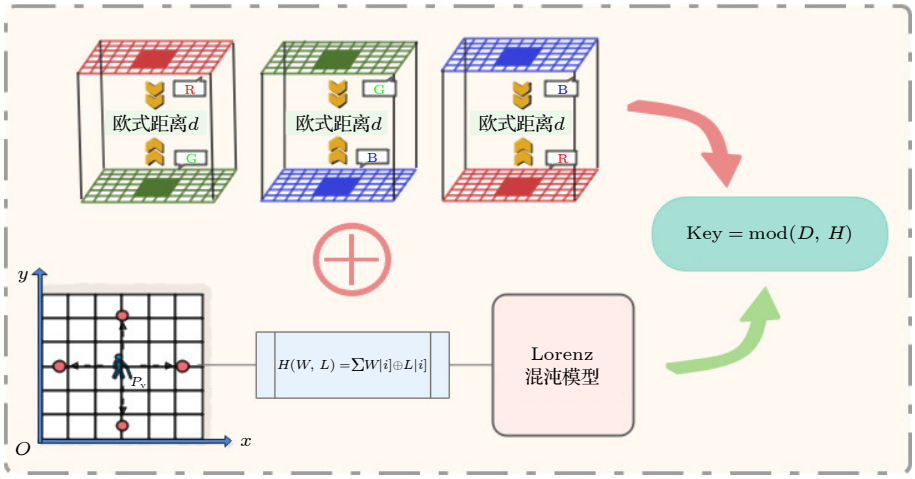

图 6 密钥生成

Fig. 6. Key generation.

3.6 盲水印的嵌入

离散余弦变换 (discrete cosine transform, DCT) 将图像空间表达式从空域转换为频域, 对原始图像进行 DCT 变换后, 生成互不相关的变换系数矩阵, 明文图像的主要能量压缩到部分低频系数中去 (即 DCT 矩阵的左上角), 使图像具有压缩比高、误码率小、信息集中等优点. 二维 DCT 变换如下:

$$F(u,v) = c(u)c(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j) \times \cos\left[\frac{(2i+1)\pi}{2N}u\right]\left[\frac{(2j+1)\pi}{2N}v\right], \tag{24}$$

其中

$$c(u),\ c(v) = \begin{cases} \sqrt{1/N},\ u=0,\ v=0, \\ \sqrt{2/N},\ u,v \neq 0. \end{cases} \tag{25}$$

在传输过程中, 盲水印算法在保护图像版权和防伪防篡改方面具有重要的作用. 本文选取混沌加密后的彩色图片作为载体图片, 将 64 × 64 的二维码图片作为水印信息, 按照 DCT 变换和奇异值分解 (singular balue decomposition, SVD) 两个过程进行嵌入和提取, 如图 7 所示.

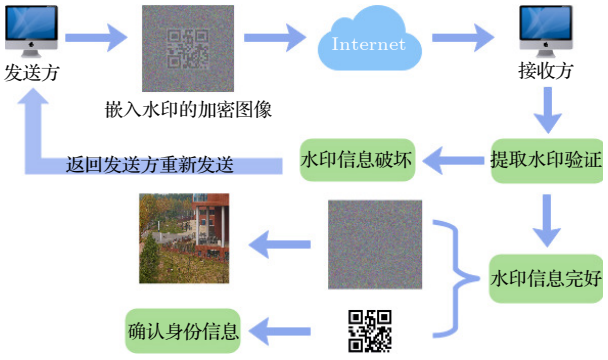

图 7 水印嵌入与提取

Fig. 7. Watermark embedding and extraction.

首先对得到混沌加密后的图像进行读取, 作为载体图像 (G), 将 RGB 转换为 YUV 格式的图像

数据表示, 并实现三通道分离, 然后将图像分成互不重叠的 8 × 8 小分块, 如果图像整体长宽大小不是偶数, 则扩充边缘, 设置边框, 添加的边界框像素值 0, 也就是补上白边. 对每一个小分块做二维 DCT 变换, 得到分块的 DCT 系数矩阵 $B_{ij}(i,j=0,1,2,\cdots,N)$, 其左上方为低频数据的大数值 (称为直流分量), 右下方为高频数据的小数值 (称为交流分量), 按照 ZigZag 排序, 取出变换后每一块矩阵的低频系数 $B_{ij}(0,0)$. 然后对每一块 $B_{ij}(0,0)$构成的矩阵 Array 进行奇异值分解, 得到 Array $=\boldsymbol{USV}^{\mathrm{T}}$. 其中, $\boldsymbol{U}$ 为左正交矩阵, $\boldsymbol{V}$ 为右正交矩阵, $\boldsymbol{S}$ 为对角矩阵. 为实现盲提取, 即无需再提取图像的参数就可提取水印, 本文采用求模量化方式将二值水印图像 (W) 嵌入到低频系数的奇异值矩阵中. 通过以下嵌入公式:

$$z = S(1,1) \bmod q, \tag{26}$$

$$S(1,1) = S(1,1) - z + q/4, \ (w=0), \tag{27}$$

$$S(1,1) = S(1,1) - z + 3q/4, \ (w=1), \tag{28}$$

其中 q 代表数字水印嵌入强度, 此时得到新的 $\boldsymbol{S}_1$ 矩阵, 然后利用 SVD 反变换得到 Array$'=\boldsymbol{US}_1\boldsymbol{V}^{\mathrm{T}}$, 把 Array$'$ 中相应的元素替换为 B_{ij} 里的低频系数, 根据公式 (24) 做逆 DCT 变换, 就得到了嵌入水印信息 W的合成图像 G'. 此时的水印较好地实现了不可见性.

3.7 盲水印的提取

接收方收到发送方的图像后首先进行水印提取, 以验证图像在传输过程中有无受到攻击, 对图像 G 依旧分割为 8 × 8 的小块做 DCT 变换, 取出每块中的低频系数矩阵 Array*, 对其做 SVD 变换得到对角矩阵 $\boldsymbol{S}^*=\boldsymbol{U}^*\boldsymbol{S}^*\boldsymbol{V}^{\mathrm{T}*}$, 根据嵌入公式 (26)—(28) 式可以得出, 此时嵌入后的图像矩阵 $\boldsymbol{D}=\boldsymbol{U}_1\boldsymbol{S}^*\boldsymbol{V}_1^{\mathrm{T}}$, 将 $S^*(1,1)$与嵌入系数 q 相比, 若大于 $q/2$则提取水印矩阵 $\boldsymbol{W}^*=1$, 否则 $\boldsymbol{W}^*=0$, 最后得到可能发生变化的水印图像, 然后分离出原始水印和载体图像.

4 实验仿真与性能分析

4.1 实验结果

实验测试来自作者相机拍摄的校园真实图像. 图像像素大小为 2048 × 2048, 分割为 4 幅像素大小为 512 × 512 的图像, 量子随机行走选取(N_{step}, P, λ_1, λ_2) = (400, 512, π/2, π/6), Lorenz 混沌模型设定参数$(x_0,y_0,z_0,\sigma,\rho,\mu,T)$为 (–16, –20, 36, 10, 29, 9/4, 8000), 加密-水印流程如图 8 所示, 加密仿真结果如图 9 所示, 加密算法如图 10 所示.

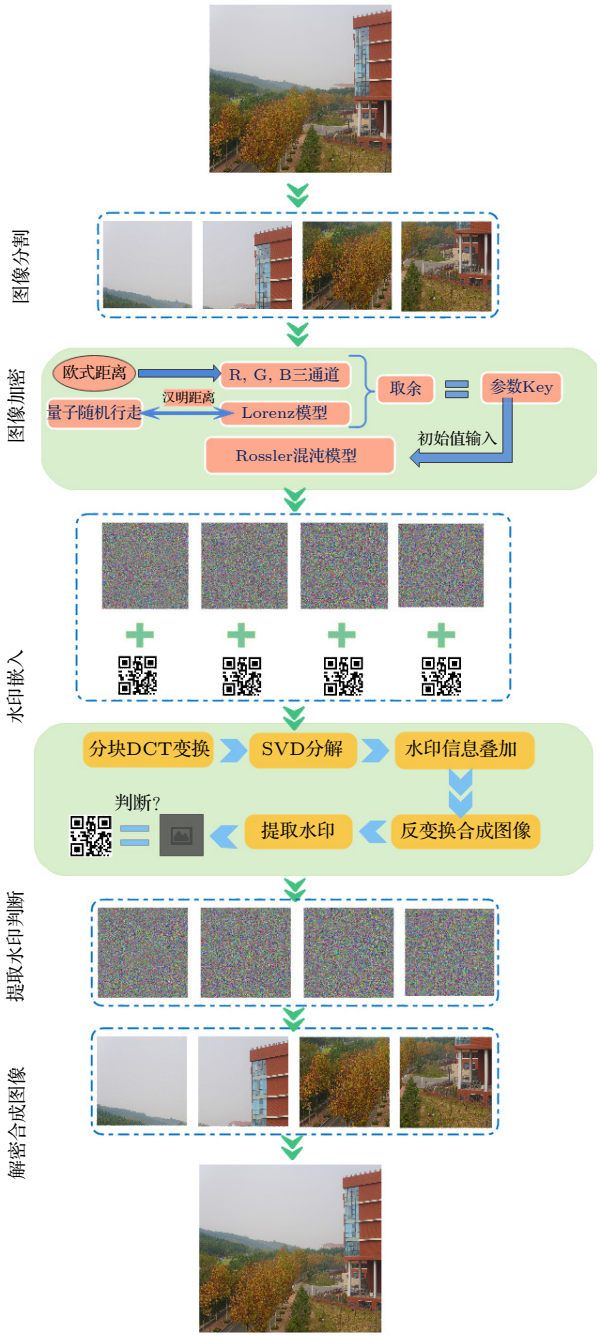

图 8 加密-水印算法流程图

Fig. 8. Encryption watermark algorithm flow chart.

4.2 加密性能分析

本节对加密图像进行了直方图、相关性、GVD、峰值信噪比等多方面的性能分析, 加密后的图像峰

图 9 加密仿真结果

Fig. 9. Encryption simulation results.

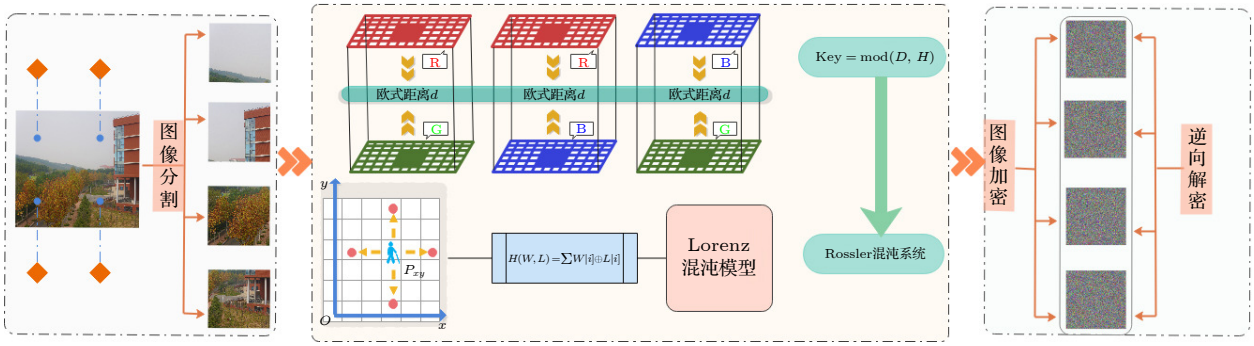

图 10 加密算法

Fig. 10. Encryption algorithm.

值信噪比稳定在 7—9 之间加密效果较好, GVD 评分接近 1 说明加密后图像与加密前图像基本不同, 加密图像的相关性均匀分布, 其相关性系数接近 0, 且加密后的直方图分布均匀, 实验结果表明本算法具有较高的抵御统计分析攻击的能力.

4.2.1 直方图

图像中各个灰度值的分布情况通过图像的直方图显示, 恶意的第三方可针对密文图像的直方图表现出明显的统计规律来获取图像的信息. 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, 图像加密方案就越安全.

3D 直方图以及原始图和加密图像的直方图如图 11—图 18 所示, 可以看出原始图像及其 RGB 三通道的直方图分布极其不均匀, 而经过加密后的图像及其 RGB 三通道的直方图像素分布均匀, 方差小无较大波动, 图像显示的统计信息就越少, 这表明加密图像抵抗统计攻击的效果较好, 图像加密方案就越安全.

4.2.2 像素相关性

图像的相关性分析是指对图像相邻像素之间进行分析, 从而衡量像素之间的相关密切程度. 一个像素往往会泄漏其周边像素的信息, 攻击者往往根据某个像素点来预测出下一个像素值, 实现对整个明文图像的恢复. 数字图像中的相邻像素具有很强的相关性, 这些强相关性必须被打破, 以避免统计攻击. 相关系数的计算公式如下:

$$E_{xy}=\frac{\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{i=1}^{N}x_i\right)\left(y_i-\frac{1}{N}\sum_{i=1}^{N}\mathrm{y}_i\right)}{\sqrt{B(x)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\sum_{i=1}^{N}x_i\right)^2}\sqrt{B(y)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(y_i-\frac{1}{N}\sum_{i=1}^{N}\mathrm{y}_i\right)^2}}. \tag{29}$$

由图 19—图 22 可以清晰地看出原始图像的像素分布集中不均匀, 但经过加密后的图像像素分布均匀. 根据表 1—表 4 得到加密后图像的 Horizontal, Vertical, Diagonald 的值接近 0, 这充分表明, 我们的加密算法对图像加密以后打破原图像的强相关性, 能有效地抵抗像素相关性分析的能力.

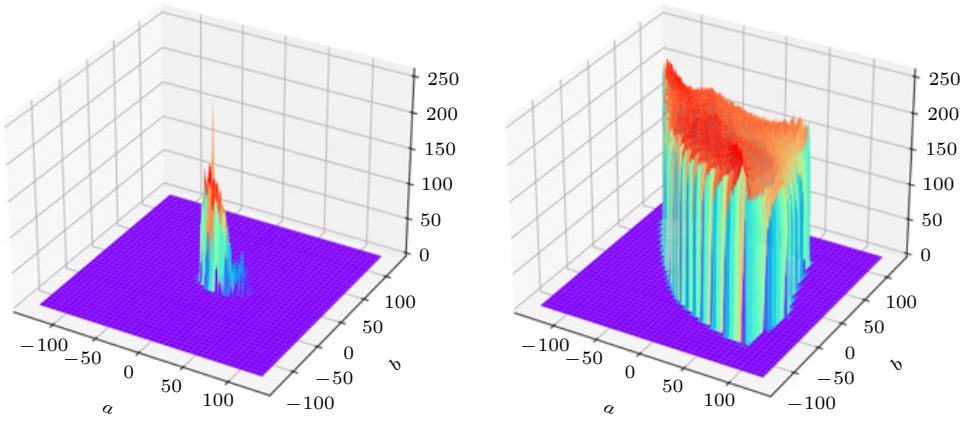

图 11 原始图像 1 和加密图像 1 的 3D 直方图

Fig. 11. 3D histogram of original image 1 and encrypted image 1.

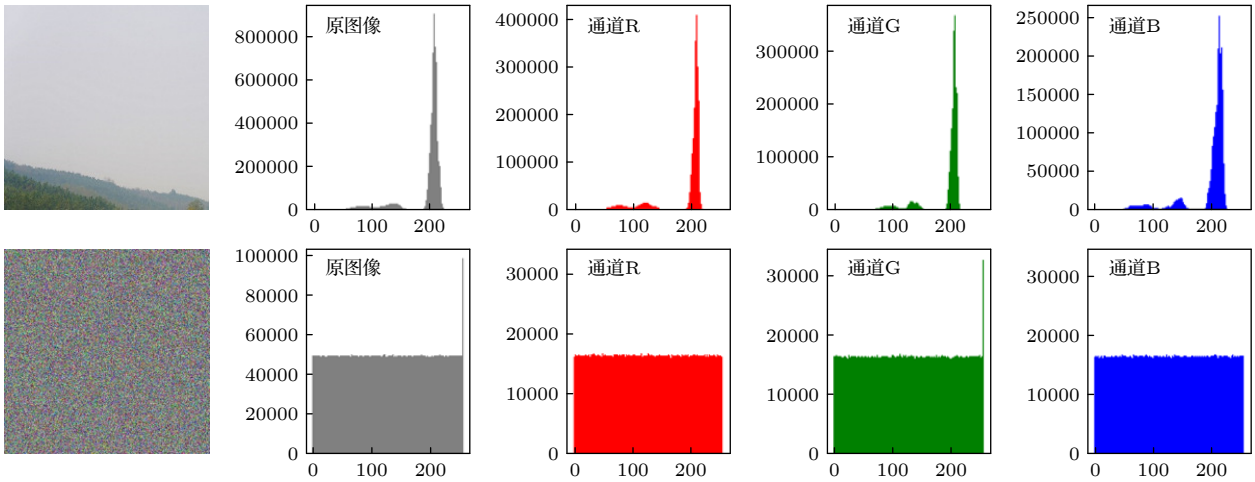

图 12 原始图像 1 和加密图像 1 的性能分析直方图

Fig. 12. Performance analysis histogram of original image 1 and encrypted image 1.

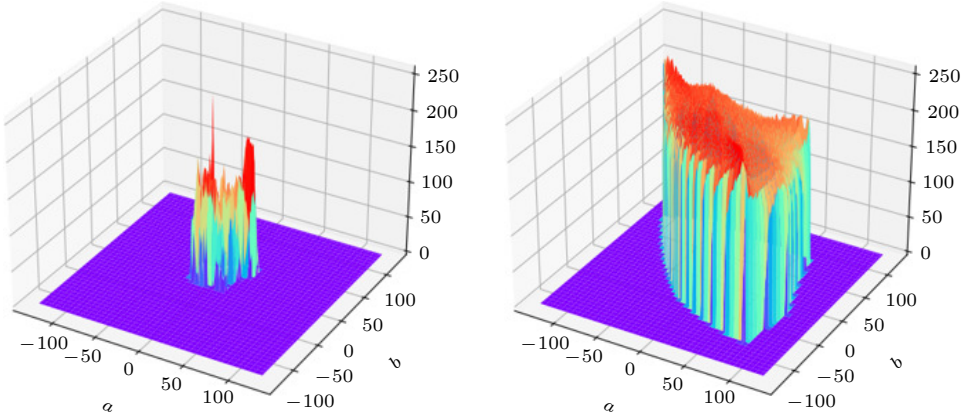

图 13 原始图像 2 和加密图像 2 的 3D 直方图

Fig. 13. 3D histogram of original image 2 and encrypted image 2.

4.2.3 灰度差分析

灰度差分析 (GVD) 是比较原始图像和加密图像的随机性的另一种统计度量, 可由下式定义:

$$\mathrm{GN}(x,y)=\frac{1}{4}\sum\left[G(x,y)-G(x',y')\right]^2, \tag{30}$$

其中

$$(x',y')=\{(x-1,y),(x+1,y),(x,y+1),(x,y-1)\}, \tag{31}$$

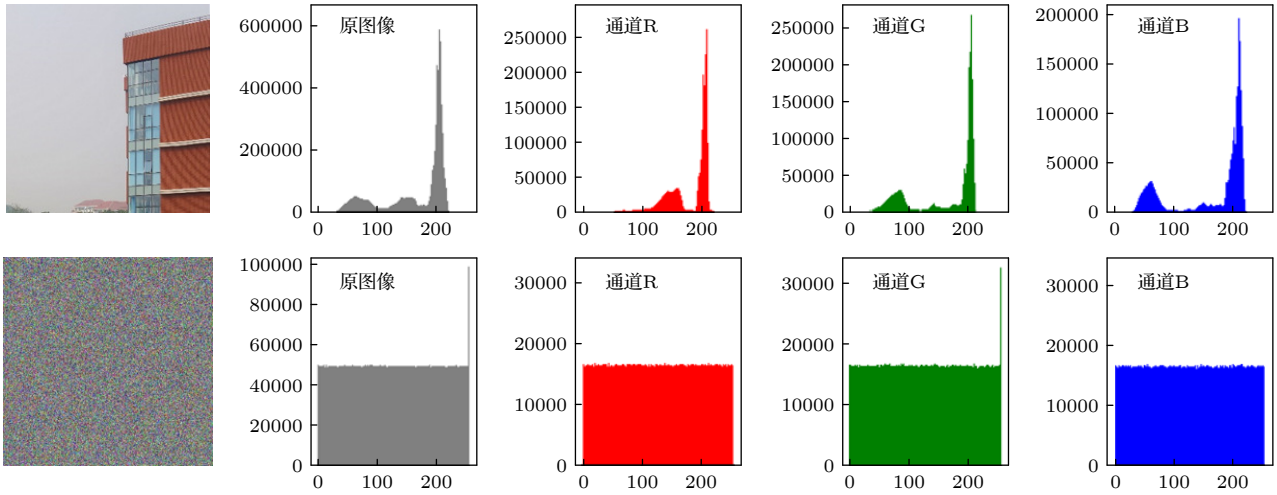

图 14 原始图像 2 和加密图像 2 的性能分析直方图

Fig. 14. Performance analysis histogram of original image 2 and encrypted image 2.

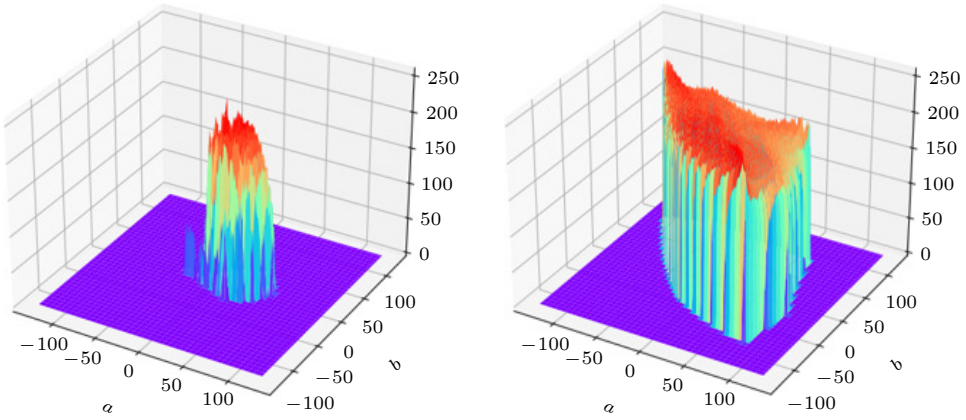

图 15 原始图像 3 和加密图像 3 的 3D 直方图

Fig. 15. 3D histogram of original image 3 and encrypted image 3.

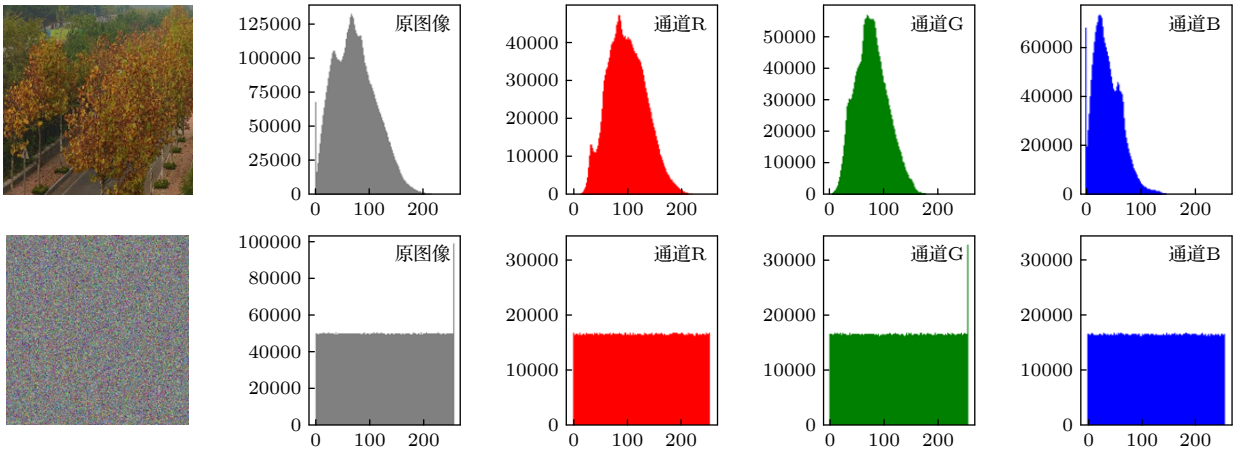

图 16 原始图像 3 和加密图像 3 的性能分析直方图

Fig. 16. Performance analysis histogram of original image 3 and encrypted image 3.

其中 $G(x,y)$ 表示位置 (x,y) 处的灰度值. 整幅图像的平均邻域灰度差用下式计算:

$$\mathrm{GVD}=\frac{\mathrm{AN}'[\mathrm{GN}(x,y)]-\mathrm{AN}[\mathrm{GN}(x,y)]}{\mathrm{AN}'[\mathrm{GN}(x,y)]+\mathrm{AN}[\mathrm{GN}(x,y)]}, \tag{32}$$

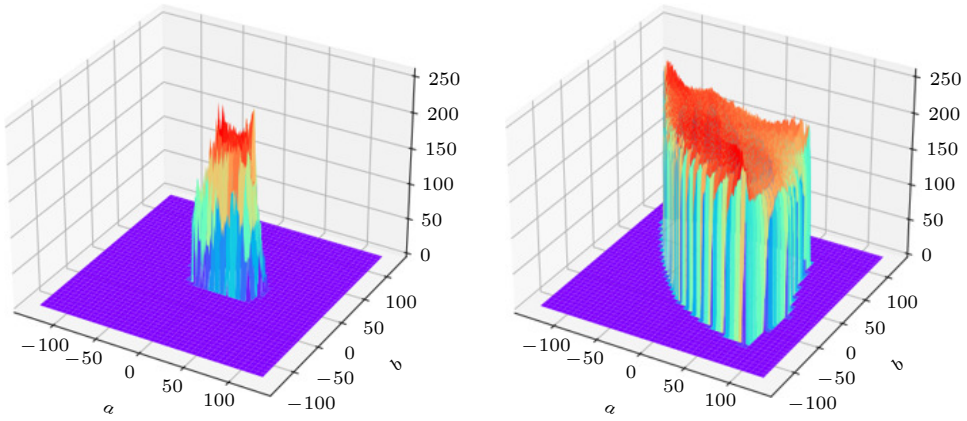

图 17 原始图像 4 和加密图像 4 的 3D 直方图

Fig. 17. 3D histogram of original image 4 and encrypted image 4.

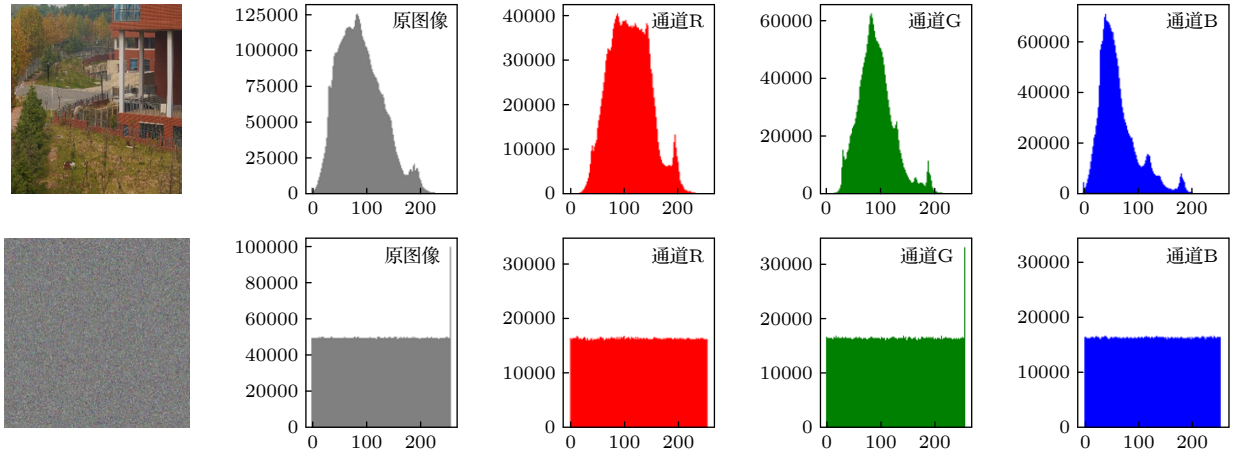

图 18 原始图像 4 和加密图像 4 的性能分析直方图

Fig. 18. Performance analysis histogram of original image 4 and encrypted image 4.

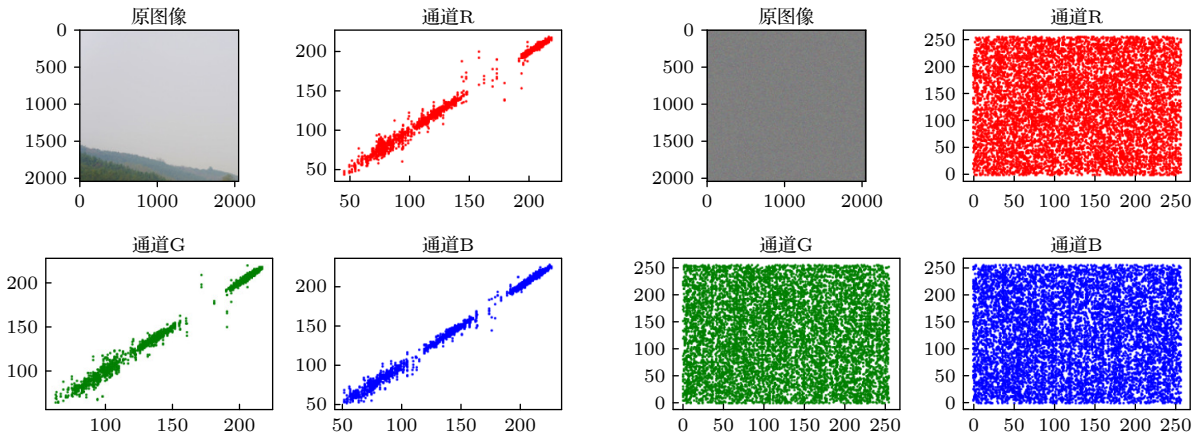

图 19 原始图像 1 和加密图像 1 的相关性

Fig. 19. Correlation between original image 1 and encrypted image 1.

$$\mathrm{AN}[\mathrm{GN}(x,y)]=\frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1}\mathrm{GN}(x,y)}{(M-2)(N-2)},\qquad(33)$$

式中, AN 和 AN′代表平均邻域灰度值, 但前者表示加密前, 后者表示加密后. 上述方程的最终结果称为 GVD 评分, 如果两幅图像完全相同, 则 GVD 评分为 0, 否则为 1, 实验结果如表 5 所示.

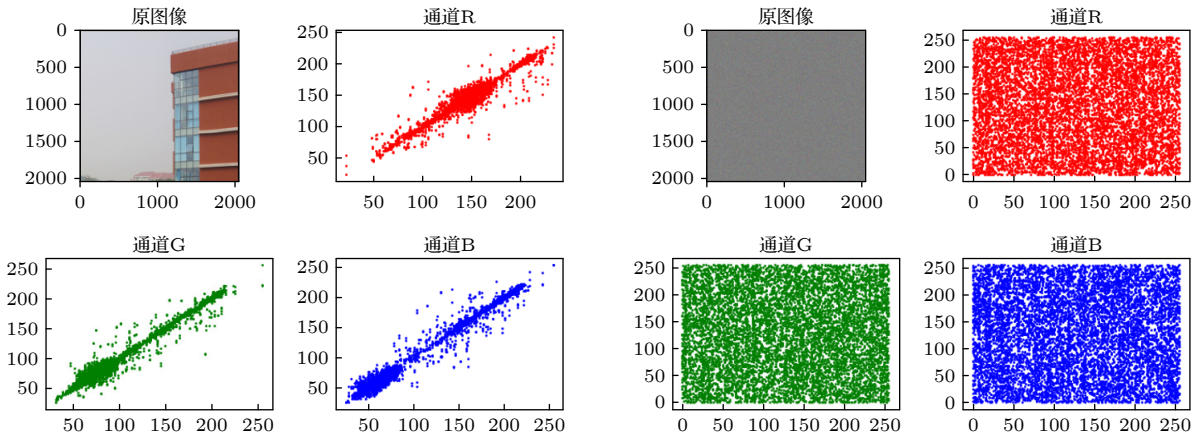

图 20 原始图像 2 和加密图像 2 的相关性

Fig. 20. Correlation between original image 2 and encrypted image 2.

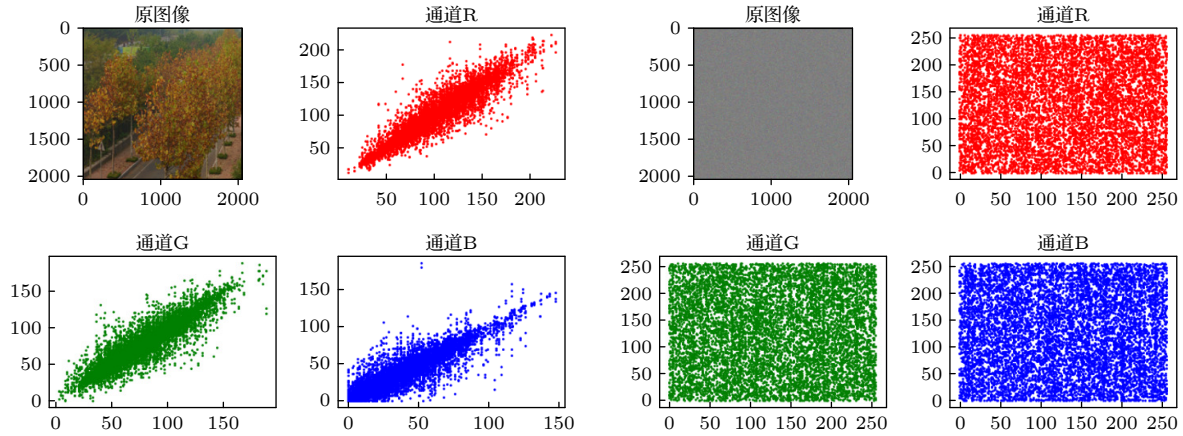

图 21 原始图像 3 和加密图像 3 的相关性

Fig. 21. Correlation between original image 3 and encrypted image 3.

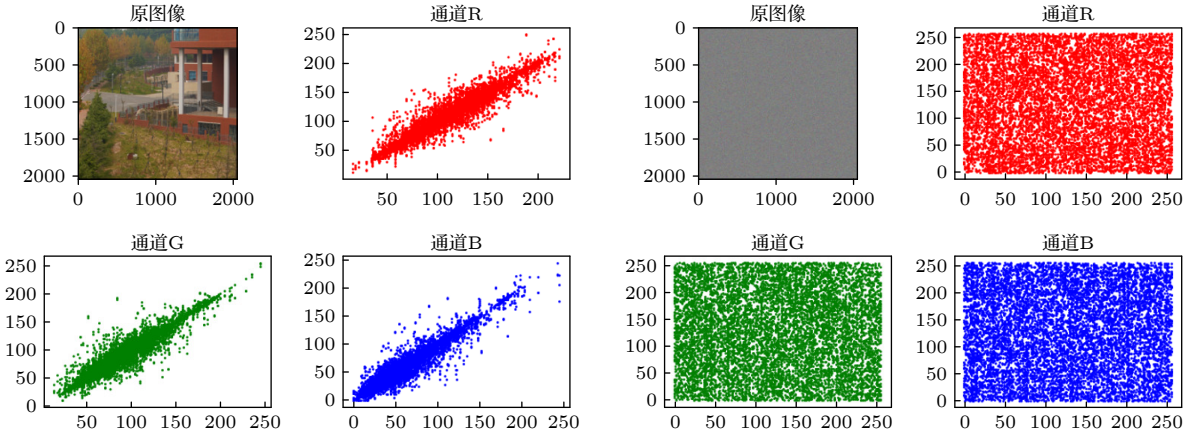

图 22 原始图像 4 和加密图像 4 的相关性

Fig. 22. Correlation between original image 4 and encrypted image 4.

4.2.4 密钥敏感度分析

检测加密方案安全性的方法之一是密钥敏感度分析, 本文通过实验对密钥生成序列中的某个比特值进行改变得到了完全不同的加密效果, 并对前后两张加密图像的像素数变化率 (NPCR) 和统一平均变化强度 (UACI) 进行分析, 实验结果如表 6 所示,

表 1 原始图像 1 和加密图像 1 的相关性数值分析
Table 1. Numerical analysis of correlation between original image 1 and encrypted image 1.

图像	通道	Horizontal	Vertical	Diagonal
图像1	R	0.9985	0.9990	0.9976
	G	0.9980	0.9988	0.9973
	B	0.9980	0.9991	0.9975
加密图像1	R	–0.0136	–0.0325	–0.0304
	G	0.0304	0.0014	0.0251
	B	–0.0234	0.0221	0.0051

表 2 原始图像 2 和加密图像 2 的相关性数值分析
Table 2. Numerical analysis of correlation between original image 2 and encrypted image 2.

图像	通道	Horizontal	Vertical	Diagonal
图像2	R	0.9910	0.9858	0.9752
	G	0.9954	0.9941	0.9883
	B	0.9969	0.9962	0.9930
加密图像2	R	–0.0136	–0.0325	–0.0304
	G	0.0304	0.0014	0.0251
	B	–0.0234	0.0221	0.0051

表 3 原始图像 3 和加密图像 3 的相关性数值分析
Table 3. Numerical analysis of correlation between original image 3 and encrypted image 3.

图像	通道	Horizontal	Vertical	Diagonal
图像3	R	0.9293	0.9631	0.8961
	G	0.9077	0.9522	0.8648
	B	0.9011	0.9379	0.8484
加密图像3	R	–0.0069	–0.0081	–0.0218
	G	–0.0070	0.0065	–0.0245
	B	–0.0117	0.0249	–0.0134

表明其接近理想值 NPCR = 99.6094%, UACI = 33.4635%,计算公式如下:

$$\mathrm{NPCR} = \frac{\sum_{i,j} E(i,j)}{M_{\mathrm{width}} \cdot N} \times 100\%, \tag{34}$$

式中, M_{width} 和 N 分别为两幅随机图像的宽度和高度, 定义 $E(i,j)$ 为

$$E(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j), \\ 0, \text{ otherwise}. \end{cases} \tag{35}$$

相应地, UACI 可以用来测量颜色分量对比度强度的平均值, 计算公式如下:

$$\mathrm{UACI} = \frac{1}{M_{\mathrm{width}} \cdot N} \frac{\sum (C_1(i,j) - C_2(i,j))}{255} \times 100\%. \tag{36}$$

表 4 原始图像 4 和加密图像 4 的相关性数值分析
Table 4. Numerical analysis of correlation between original image 4 and encrypted image 4.

图像	通道	Horizontal	Vertical	Diagonal
图像4	R	0.9568	0.9750	0.9379
	G	0.9449	0.9665	0.9170
	B	0.9540	0.9746	0.9346
加密图像4	R	–0.0162	–0.0055	0.0147
	G	0.0006	0.0003	–0.0060
	B	0.0207	–0.0291	0.0017

表 5 GVD
Table 5. GVD.

GVD	原始-加密图像1	原始-加密图像2	原始-加密图像3	原始-加密图像4
R	0.9993	0.995	0.9755	0.9809
G	0.9993	0.9947	0.9763	0.9815
B	0.9993	0.995	0.9804	0.9826

表 6 密钥敏感性分析
Table 6. Key sensitivity analysis.

图像	通道	NPCR/%	UACI/%
图像1	R	99.5687	33.4381
	G	99.6098	33.4594
	B	99.6180	33.4347
图像2	R	99.5690	33.4386
	G	99.6100	33.4598
	B	99.6186	33.4350
图像3	R	99.5684	33.4378
	G	99.6094	33.4588
	B	99.6174	33.4437
图像4	R	99.5688	33.4376
	G	99.6088	33.4590
	B	99.6170	33.4347

4.2.5 峰值信噪比

峰值信噪比 (peak signal to noise ratio, PSNR) 主要考察对应像素点之间的误差. 给定大小为 $M \times N$ 的加密图像 X 和原图像 Y, PSNR 计算如下:

$$\mathrm{PSNR} = 10 \lg \frac{M_{\mathrm{width}} \times N(2^n - 1)^2}{\sum_{i=1}^{M_{\mathrm{width}}} \sum_{j=1}^{M_{\mathrm{width}}} (X(i,j) - Y(i,j))^2}, \tag{37}$$

其中, M_{width} 和 N 分别表示图像的宽高, n 为像素位数; PSNR 值越大, 表示失真越小, 两张图片差距越小, 加密效果越差.

由表 7 峰值信噪比看出原始图像与加密图像 1, 原始图像加密图像 2, 原始图像加密图像 3, 原始图像加密图像 4 的 R, G, B 三通道的 PSNR 值

都稳定在 7—9 之间. 可以判断出原始图像与各个加密图像的差距较大, 加密的效果较好.

表 7 峰值信噪比

Table 7. Peak signal to noise ratio.

PSNR	原始-加密图像1	原始-加密图像2	原始-加密图像3	原始-加密图像4
R	7.691	8.376	9.369	9.582
G	7.755	8.132	8.686	9.193
B	7.479	7.747	6.782	7.782

4.3 水印攻击检测

通过对水印嵌入的图像模拟各种攻击来检测水印的鲁棒性, 对图像的攻击同时影响载体图片信息和提取的水印的信息.

4.3.1 嵌入水印的峰值信噪比

峰值信噪比主要考察对应像素点之间的误差. 分别计算 4 幅加密图像和嵌入水印图像的峰值信噪比, 结果如表 8 所列.

表 8 嵌入水印的峰值信噪比

Table 8. Peak signal to noise ratio of embedded watermark.

PSNR	加密-嵌入水印1	加密-嵌入水印2	加密-嵌入水印3	加密-嵌入水印4
R	38.81	38.81	38.8	38.79
G	40.28	40.29	40.26	40.28
B	35.46	35.48	35.47	35.47

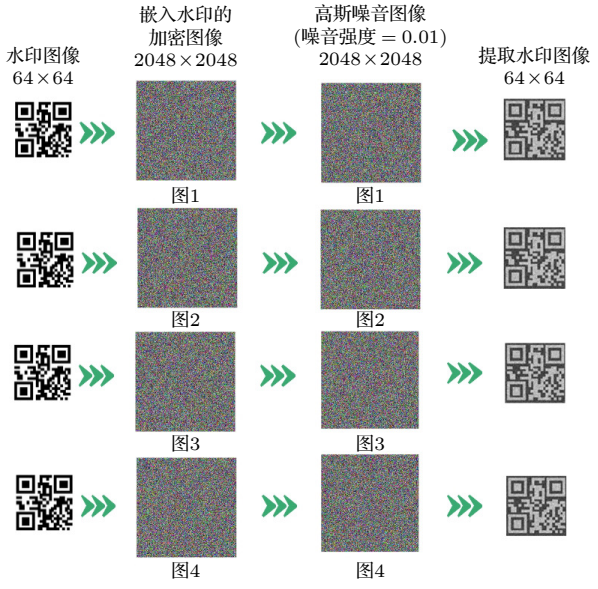

图 23 高斯噪声

Fig. 23. Gaussian noise.

4.3.2 高斯噪声

高斯噪声是指概率密度函数服从高斯分布 (即正态分布) 的一类噪声, 高斯噪声可以表示为

$$C(x,y)=f(x,y)+c(x,y), \tag{38}$$

其中, $C(x,y)$是被添加高斯噪声后的图像, $f(x,y)$是原图像, $c(x,y)$是高斯加性噪声, 如图 23 所示.

$$c(x,y)=\frac{\sum_i^m X_i-m\mu}{\sqrt{m}\sigma}=\frac{\bar{X}-\mu}{\sigma/\sqrt{m}}, \tag{39}$$

其中, μ是区间$[ab]$的均值, 即$\mu=(b+a)/2$, X_m代表从区间$[ab]$上随机取的 m 个数, 当 m 足够大时, $c(x,y)$近似正态分布, $c(x)=\dfrac{1}{\sqrt{2\pi}\sigma}\exp\left[-\dfrac{(x-\mu)^2}{2\sigma^2}\right]$.

5 总 结

本文提出一种新颖的基于量子随机行走和多维混沌的三维图像加密算法, 利用量子计算的优势, 改善了混沌系统的密钥的空间和随机性, 使得密钥的敏感度较高, 难以通过暴力求解的方式推出密钥. 对该方案进行直方图、信息熵、相关性等性能分析, 实验结果表明该算法安全可靠, 能够抵抗统计攻击, 在 RGB 三通道之间进行像素置乱使得很难从一个通道求解另一个通道的解密图像. 并且图像嵌入盲水印信息后, 在传输中对恶意篡改图像起到了监听作用, 一旦对图像攻击, 在提取水印后, 接收方就会知道传输过程中遭受攻击, 进一步提高了图像传输过程中的安全性.

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] Aharonov Y, Davidovich L, Zagury N 1993 *Phys. Rev. A* **48** 1687
[6] Farhi E, Gutmann S 1998 *Phys. Rev. A* **58** 915
[7] Childs A M, Cleve R, Deotto E, Farhi E, Gutmann S, Spielman D A 2003 *STOC'03: Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing* (New York: Association for Computing Machinery) pp59–68
[8] Castagnoli G 2016 *Found. Phys.* **46** 360
[9] Castagnoli G 2016 *Quanta.* **5** 34
[10] Gong L H, Song H C, He C S, Liu Y, Zhou N R 2014 *Phys. Scr.* **89** 035101
[11] Li H H, Gong L H, Zhou N R 2020 *Chin. Phys. B* **29** 110304
[12] Watrous J 2001 *J. Comput. Syst. Sci.* **62** 376

[13] Abd El-Latif A A, Abd-El-Atty B, Venegas-Andraca S E, Elwahsh H, Piran M J, Bashir A K, Song O Y, Mazurczyk W, 2020 *IEEE Access* **8** 92687
[14] Abd-El-Atty B, Iliyasu A M, Alaskar H, Alaskar H, Abd-El-Latif A A 2020 *Sensors* **20** 3108
[15] Abd El-Latif A A, Abd-El-Atty B, Mazurczyk W, Fung C, Venegas-Andraca S E 2020 *IEEE Trans. Netw. Serv. Manage.* **17** 118
[16] 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
[17] Abd El-Latif A A, Abd-El-Atty B, Amin M, Iliyasu A M 2020 *Sci. Rep.* **10** 1
[18] Abd-El-Atty B, Iliyasu A M, Alanezi A, Abd El-latif AA 2021 *Opt. Lasers Eng.* **138** 106403
[19] Smith J D, Hill A J, Reeder L E, Franke B C, Lehoucp R B, Parekh O, Severa, M, Aimone J B 2022 *Nat. Electron.* **5** 102
[20] Godsil C, Zhan H M 2019 *J. Comb. Theory A* **167** 181
[21] Singh S, Chawla P, Sarkar A, Chandrashekar C M 2021 *Sci. Rep.* **11** 1
[22] Tsafack N, Kengne J, Abd-El-Atty B, Iliyasu A M, Hirota K, Abd EL-Latif A A 2020 *Inf. Sci.* **515** 191
[23] Wang Y N, Song Z Y, Ma Y L, Hua N, Ma H Y 2021 *Acta Phys. Sin.* **70** 10 (in Chinese) [王一诺, 宋昭阳, 马玉林, 华南, 马鸿洋 2021 物理学报 **70** 10]
[24] Kocarev L 2001 *IEEE. Circ. Syst. Mag.* **1** 6
[25] Guan Z H, Huang F J, Guan W J 2005 *Phys. Lett. A* **346** 153
[26] Lian S G, Sun J S, Wang Z Q 2005 *Physica A* **351** 645
[27] Xiao D, Liao X F, Wei P C 2009 *Chaos. Solitons Fractals* **40** 2191
[28] Zhang X P, Zhao Z M, Wang J Y 2014 *Signal Process. Image Commun.* **29** 902
[29] Assad S E, Farajallah M 2016 *Signal Process. Image Commun.* **41** 144
[30] Wang M G, Wang X Y, Zhang Y Q, Zhou S, Zhao T T, Yao N M 2019 *Opt. Lasers Eng.* **121** 479
[31] Kumar V, Girdhar A 2021 *Multimed Tools Appl.* **80** 3749
[32] Huang W, Jiang D H, An Y S, Liu L D, Wang X Y 2021 *IEEE Access* **9** 41704
[33] Rakesh S, Kaller A A, Shadakshari B C, Annappa B 2012 *IJCIS* **2** 49
[34] Huang X L, Ye G D 2014 *Commun. Nonlinear Sci.* **19** 4094
[35] Wang M X, Wang X Y, Zhang Y Q, Zheng G 2018 *Opt. Laser Technol.* **108** 558
[36] Zhou W J, Wang X Y, Wang M X, Li D Y 2022 *Opt. Laser Eng.* **149** 106782

Three dimensional image encryption algorithm based on quantum random walk and multidimensional chaos*

Liu Han-Yang [1)] Hua Nan [1)] Wang Yi-Nuo [2)]

Liang Jun-Qing [1)] Ma Hong-Yang [2)†]

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

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

(Received 15 March 2022; revised manuscript received 14 April 2022)

Abstract

With the development of computer network technology, people's requirements for information security is increasing day by day. However, the classical encryption technology has the defects of small key space and easy crack. The problems of image encryption technology in protecting image information security and private content need solving urgently. As a new type of quantum key generator, quantum random walk has a large key space. Compared with the classical random walk, the computing speed and security are significantly improved. This paper presents a three-dimensional image encryption algorithm that is based on quantum random walk and involves Lorenz and Rossler multidimensional chaos. Firstly, Gaussian pyramid is used to segment the image. Secondly, the Hamming distances of several sub images are calculated by using the random sequence generated by quantum random walk and the random sequence generated by Lorenz chaotic system in multi-dimensional chaos, and then synthesized, and the Euclidean distances between the three RGB channels of the image are calculated. Finally, the sequence value obtained from the remainder of Hamming distance and Euclidean distance, as an initial value is input into the Rossler system in multi-dimensional chaos to generate a random sequence which is used as the key to XOR the RGB channel of the image so as to create an encrypted image. The corresponding decryption scheme is the inverse process of the encryption process. In addition, in terms of transmission security, this paper uses a blind watermark embedding algorithm based on DCT and SVD to embed the watermark information into the encrypted image, so that the receiver can extract the watermark and judge whether the image is damaged by the attack in the transmission process according to the integrity of the watermark information. If it is not attacked maliciously, the image will be decrypted. This operation further improves the protection of image information security.The experimental results show that the peak signal-to-noise ratio of the encrypted image is stable between 7 and 9 and the encryption effect is good, the GVD score is close to 1, the correlation of the encrypted image is uniformly distributed, and the correlation coefficient is close to 0, and the key space is 2^{128} in size and the encrypted histogram is evenly distributed, showing a high ability to resist statistical analysis attacks.

Keywords: quantum walk, chaotic model, image encryption, blind watermarking

PACS: 03.65.–w, 03.67.Ac, 03.67.Dd, 95.10.Fh **DOI:** 10.7498/aps.71.20220466

* 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), the Project of Shandong Province Higher Educational Science and Technology Program of Shandong Province, China (Grant No. J18KZ012), and the Joint Fund of Shandong Natural Science Foundation, China (Grant No. ZR202108020011).

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

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

基于量子随机行走和多维混沌的三维图像加密算法

刘瀚扬　华南　王一诺　梁俊卿　马鸿洋

Three dimensional image encryption algorithm based on quantum random walk and multidimensional chaos

Liu Han-Yang　Hua Nan　Wang Yi-Nuo　Liang Jun-Qing　Ma Hong-Yang

引用信息 Citation: Acta Physica Sinica, 71, 170303 (2022)　DOI: 10.7498/aps.71.20220466
在线阅读 View online: https://doi.org/10.7498/aps.71.20220466
当期内容 View table of contents: http://wulixb.iphy.ac.cn

您可能感兴趣的其他文章
Articles you may be interested in

基于DNA编码与交替量子随机行走的彩色图像加密算法
Color image encryption algorithm based on DNA code and alternating quantum random walk
物理学报. 2021, 70(23): 230302　https://doi.org/10.7498/aps.70.20211255

基于深度学习的新混沌信号及其在图像加密中的应用
A new chaotic signal based on deep learning and its application in image encryption
物理学报. 2021, 70(23): 230502　https://doi.org/10.7498/aps.70.20210561

基于深度学习压缩感知与复合混沌系统的通用图像加密算法
General image encryption algorithm based on deep learning compressed sensing and compound chaotic system
物理学报. 2020, 69(24): 240502　https://doi.org/10.7498/aps.69.20201019

基于新的五维多环多翼超混沌系统的图像加密算法
Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system
物理学报. 2020, 69(4): 040502　https://doi.org/10.7498/aps.69.20191342

一种基于压缩感知和多维混沌系统的多过程图像加密方案
Multi-process image encryption scheme based on compressed sensing and multi-dimensional chaotic system
物理学报. 2019, 68(20): 200501　https://doi.org/10.7498/aps.68.20190553

基于空间角度复用和双随机相位的多图像光学加密方法
Multiple-image encryption method based on spatial angle multiplexing and double random phase encoding
物理学报. 2019, 68(24): 240503　https://doi.org/10.7498/aps.68.20191362