Latin 方阵和二维量子漫步相结合的图像加密

蒋建伟[1]，张 田[1]，陈祯羽[2]，马鸿洋[2*]

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

【摘要】针对数字图像在网络传输过程中容易受到攻击导致信息泄漏的问题，在 Arnold 置乱变换的基础上引入量子漫步和 Latin 方阵，设计了一种新型的彩色图像加密方案。首先把彩色图像的三通道分离，用 Arnold 变换来对图像像素点置乱，量子漫步和 Latin 方阵被用来处理置乱后图像的像素值，然后对处理之后的图像使用加取模扩散算法进一步改变图像的像素值，最后合并三通道加密图像得到彩色加密图像。量子漫步的作用是为该文的加密算法提供随机序列。该文对加密算法进行了实验仿真，在直方图、相关性、信息熵、噪声攻击、裁剪攻击等多个方面对实验结果进行了性能分析。仿真结果显示：加密图像的直方图均匀分布，像素点之间的相关性趋近于 0，信息熵为 7.999 3，接近于 8，说明该算法具有较不错的抵抗统计分析的能力；经过噪声攻击和裁剪攻击之后的加密图像经过解密之后，仍然可以看到原图像信息，表明该算法的鲁棒性是良好的；该加密算法的密钥空间足够大为10^{60}且密钥敏感性良好，NPCR 值接近于 99.61%，UACI 值接近于 33.45%，证明该算法拥有抵抗差分攻击的能力。

关 键 词 Arnold 变换； 图像加密； Latin 方阵； 量子漫步

中图分类号 TP391.9 **文献标志码** A doi:10.12178/1001-0548.2022076

Color Image Encryption Combining Latin Matrix and Two-Dimensional Quantum Random Walk

JIANG Jianwei[1], ZHANG Tian[1], CHEN Zhenyu[2], and MA Hongyang[2*]

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

Abstract Aiming at the problem that digital images are vulnerable to attacks during network transmission and cause information leakage. This paper introduces quantum walk and Latin square matrix on the basis of Arnold scrambling, and designs a new type of color image encryption scheme. In the new scheme, the three channels of the color image are separated at first and the Arnold transform is used to scramble the pixel points of the image. Then quantum walk and Latin square matrix are used to process the pixel values of the scrambled image, the modulus diffusion algorithm is used on the processed image to further change the pixel value of the image. Finally, the color encrypted image is obtained by merging the three-channels encrypted images. Quantum walk, as an excellent random sequence generation tool, provides random sequences for algorithms. We conducted experimental simulations on the encryption algorithm, and analyzed the experimental results in the histogram, correlation, information entropy, noise attack, cropping attack and other aspects. The results show that the histogram of the encrypted image is distributed evenly, the correlation between pixels is close to 0, and the information entropy is 7.999 3, close to 8, indicating that the algorithm has a relatively good ability to resist statistical analysis. After decrypting the encrypted image after noise attack and cropping attack, the original image information can still be seen, indicating that the robustness of the algorithm is good. The key space of the encryption algorithm is large enough and the key sensitivity is good. The NPCR(normalized pixel contrast ratio) value is close to 99.61%, and the UACI(unified average changing intensity) value is 33.45%. It has the ability to resist differential attacks.

Key words arnold transformation; image encryption; Latin square matrix; quantum walk

收稿日期：2022－03－15；修回日期：2022－05－29

基金项目：国家自然科学基金 (11975132)；山东省自然科学基金面上项目 (ZR2021MF049)；山东省自然科学基金 (ZR2019YQ01)；山东省高等教育科技计划 (J18KZ012)；山东省自然科学基金联合基金 (ZR202108020011)

作者简介：蒋建伟 (1997－)，男，主要从事数字图像处理、量子计算等方面的研究.

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

随着互联网与多媒体技术的快速发展，信息的安全性问题日益凸显。数字图像作为信息传输的主要载体之一，如何有效地保护图像的信息不被窃取是当今的一个热门研究课题。保护图像信息安全的方法主要分为两类：图像加密[1-5]和图像水印[6-9]。图像加密的原理是针对图像的像素点的位置和像素值按照特定的方式做出改变，从而在变换之后的图像上无法获取原图像的数据信息；图像水印是通过把图像嵌入载体图像以此来达到隐藏图像信息的效果。如今的图像加密技术已经发展得比较成熟，其中主流的加密方法有：DNA 编码加密[10-12]、混沌系统加密[13-15]、魔方置乱加密[16-18]、Arnold 置乱变换[19-22]等。

Arnold 置乱变换是在研究遍历理论时提出的一种变换方法。由于 Arnold 置乱变换最初的实验对象是猫的图片，所以 Arnold 置乱变换也叫作“猫脸变换”。Arnold 置乱变换是一种在有限区域内进行反复折叠和拉伸变换的置乱方法，凭借其置乱直观、具有周期性等多种优点，经常与混沌系统相结合被用于图像加密。文献 [23] 在 Arnold 置乱变换和混沌系统的基础上，设计了一种以彩色图像为载体的抵抗几何攻击的数字水印方案。该算法可以有效地解决图像质量和鲁棒性之间的冲突问题。文献 [24] 提出了一种基于 Arnold 置乱变换和 Hardmard 单像素的彩色图像加密算法。该加密算法只需要一个桶形探测器就可以对彩色图像实现成像质量好、安全性能高的加密效果。

近年来，量子计算与量子通信飞速发展，为许多经典算法难以有效解决的难题提供了新的思路以及发展方向。量子随机行走是经典随机行走与量子计算相结合而生成的。量子随机行走已与多种经典算法相结合，存在于许多加密以及搜索算法中[25-28]。量子随机行走相比于经典随机行走主要有两方面的优势：1) 量子随机行走具有量子计算的并行性特点，因此它有着更快的运行速度；2) 量子随机行走有着更大的密钥空间，如果把量子随机行走应用于加密算法中，能使加密算法中的随机序列有更强的随机性，加密图像从而可以更好地抵御暴力攻击。文献 [29] 设计了一种基于量子漫步和离散余弦变换的彩色图像加密方案，利用量子漫步的控制参数替代随机掩膜来作为加密过程中的密钥，有利于密钥的管理与传输。文献 [30] 将量子漫步与双随机相位编码技术相结合，提出了一种新型图像加密技术，量子漫步被用来在双随机相位编码的过程中生成随机掩码。

Latin 方阵是一种特殊的方阵，它的每一行或每一列中的元素各不相同，但是每一行以及每一列中的元素种类是相同的。Latin 方阵具有直方图均匀、密钥空间大等诸多优点，在图像加密方面有很大优势[31-33]。文献 [34] 将 Latin 方阵与混沌系统相结合研究出了一种图像加密方案，该加密算法利用 Latin 方阵与混沌系统的同质性使得方案本身具有更好的混淆和扩散效果。文献 [35] 设计了一种新型的图像加密方案：首先利用混沌系统生成随机序列，再利用两个随机序列生成 Latin 方阵，然后用 Latin 方阵以及随机矩阵完成像素值替代，从而完成图像加密。

本文将 Arnold 变换与 Latin 方阵、量子漫步相结合，设计了一种新型的图像加密方式。其中 Arnold 变换和 Latin 方阵用来对图像进行处理，然后对置乱之后的图像使用加取模扩散方法进行像素值的变换。解密过程为加密过程的逆过程。

1 相关工作

1.1 Arnold 置乱变换

Arnold 置乱变换被定义为：

$$\begin{bmatrix} \alpha_{n+1} \\ \beta_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & x \\ y & xy+1 \end{bmatrix} \begin{bmatrix} \alpha_n \\ \beta_n \end{bmatrix} \bmod N \tag{1}$$

式中，α_n, β_n表示变换前图像中的像素点坐标；α_{n+1}和β_{n+1}表示经过变换之后图像的像素点坐标；N表示图像的长度；n表示当前所变换的次数；x, y为参数 (本文采用$x=y=1$)。在图像解密时，可以用 Arnold 反变换 (这里$\alpha=\beta=1$)，反变换的公式为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} \alpha\beta+1 & -\beta \\ -\alpha & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{2}$$

Arnold 置乱变换的原理如图 1 所示。

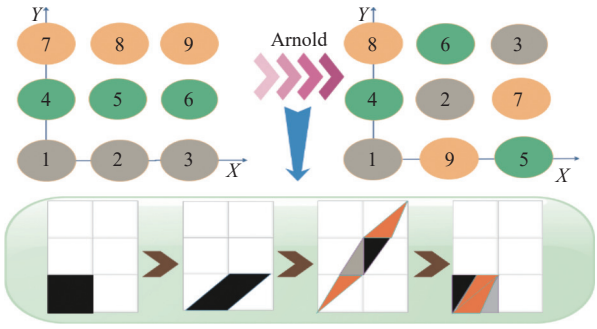


图 1 Arnold 变换原理图

1.2　量子漫步

量子漫步是量子计算中的一个重要模型。如今量子漫步有连续量子漫步和离散量子漫步两种计算模型，本算法利用的是离散时间量子漫步。离散量子漫步是经典漫步与量子计算结合而来的。离散量子漫步在经典漫步的基础上引入了硬币态的概念，它的每步行走由硬币态控制操作和偏移操作共同决定。首先进行硬币态操作，再由硬币态的输出来决定下一步如何移动。而量子漫步的希尔伯特空间由粒子的位置空间与硬币空间张量而成，故量子漫步的动态演化可以看作是一个酉算符反复作用到叠加态上，其中酉算符可以表示为：$U=SC$，其中，S为偏移算子，C是硬币算符。

本文采用 Hardmard 算子作为硬币算符，S作为偏移算子。当硬币态为 0 时，位置态将前进一步；反之当硬币态为 1 时，位置态将后退一步：

$$S=|0\rangle\langle 0|\otimes\sum_i|i+1\rangle\langle i|+|1\rangle\langle 1|\otimes\sum_i|i-1\rangle\langle i| \tag{3}$$

在二维空间内的交替量子漫步中，如图 2 所示，偏移算子可看作两部分组成：X 轴方向上的偏移算子和 Y 轴上的偏移算子：

$$S_x=\sum|i+1,j,0\rangle\langle i,j,0|+\sum|i-1,j,1\rangle\langle i,j,1| \tag{4}$$

$$S_y=\sum|i,j+1,0\rangle\langle i,j,0|+\sum|i,j-1,1\rangle\langle i,j,1| \tag{5}$$

假定交替量子漫步的初始态为$|\psi_0\rangle$，则在 N 步行走之后的叠加态为：$|\psi_N\rangle=U^N|\psi_0\rangle$。

根据漫步在位置 (x,y) 的概率大小得到概率矩阵：

$$P(x,y,N)=\left|\langle x,y,0|U^N|\psi_0\rangle\right|^2+\left|\langle x,y,1|U^N|\psi_0\rangle\right|^2 \tag{6}$$

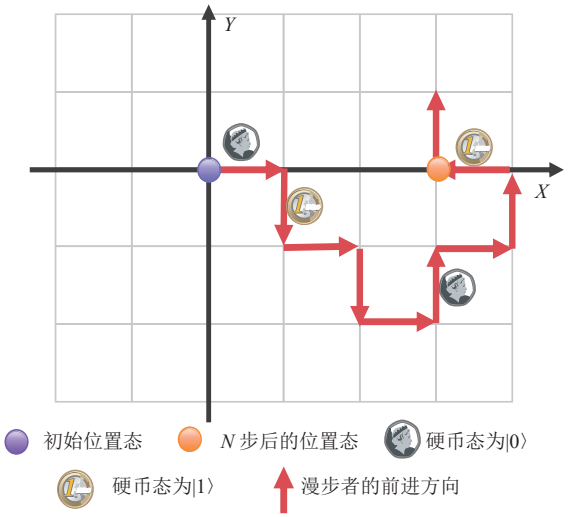


图 2　量子漫步原理图

1.3　Latin 方阵

对于一个 n 阶方阵$\boldsymbol{A}=(a_{i,j})_{n\times n}$，如果该方阵正好有 n 种不同的元素，并且每一种元素在同一行或同一列里只出现一次，那么这种方阵称作 Latin 方阵。Latin 方阵在图像加密中具有促进像素值的均匀分布，平衡图像矩阵中的像素值的作用。图 3a～图 3d 分别对应 3～6 阶 Latin 方阵。

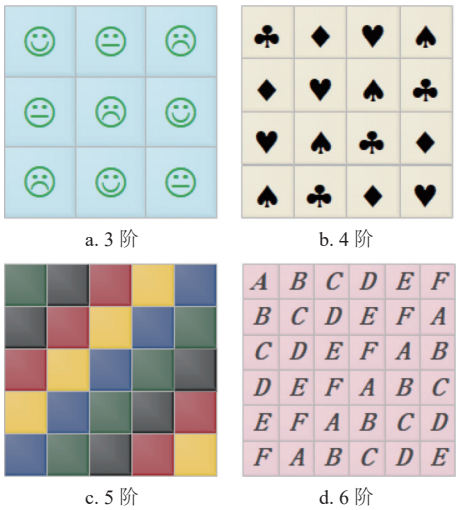


图 3　Latin 方阵

2　算法流程

该算法的加密过程分为 4 个过程：1) Arnold 变换；2) 利用量子漫步生成随机序列从而生成 Latin 方阵；3) 由 Latin 方阵和两个随机矩阵生成与图像矩阵做异或操作的密钥矩阵；4) 对图像进行加取模扩散处理。如图 4 所示。

2.1　加密步骤

1) 输入待加密的大小为$M\times N$的彩色图像I，将图像分别按行、列进行位置置乱得到初步置乱图像I_o，然后把初步置乱图像I_o分解成 3 个单通道图像R_1,G_1,B_1：

$$R_1=I_o(0,0,1) \tag{7}$$

$$G_1=I_o(0,0,2) \tag{8}$$

$$B_1=I_o(0,0,3) \tag{9}$$

2) 对分离后的 3 个单通道图像R_1,G_1,B_1分别进行 Arnold 置乱，得到单通道像素点置乱图像R_2,G_2,B_2。Arnold 置乱变换的公式如下：

$$\begin{bmatrix}\alpha_{n+1}\\ \beta_{n+1}\end{bmatrix}=\begin{bmatrix}1&1\\1&2\end{bmatrix}\begin{bmatrix}\alpha_n\\ \beta_n\end{bmatrix}\bmod N \tag{10}$$

3) 通过离散量子漫步生成一个长度为 512 的随机序列P_1，然后把该随机序列平均分成两个长度为 256 的随机序列P_2和P_3，并对两个随机序列利用文献 [32] 中的方法生成 Latin 方阵$\boldsymbol{L}_S$：

$$P_1(x_1,y_1,N)=\left|\left\langle x_1,y_1,0\left|U^N\right|\psi_0\right\rangle\right|^2+\left|\left\langle x_1,y_1,1\left|U^N\right|\psi_0\right\rangle\right|^2 \tag{11}$$

4) 利用量子漫步生成两个长度为$M\times N$的随机序列P_4和P_5，通过如下的方法将随机序列的各个数据转化为大小在 0～255 的序列S_1和S_2，然后把S_1和S_2转化为大小为$M\times N$的矩阵$\boldsymbol{Q}_1$和$\boldsymbol{Q}_2$：

$$P_4(x_2,y_2,N)=\left|\left\langle x_2,y_2,0\left|U^N\right|\psi_0\right\rangle\right|^2+\left|\left\langle x_2,y_2,1\left|U^N\right|\psi_0\right\rangle\right|^2 \tag{12}$$

$$P_5(x_3,y_3,N)=\left|\left\langle x_3,y_3,0\left|U^N\right|\psi_0\right\rangle\right|^2+\left|\left\langle x_3,y_3,1\left|U^N\right|\psi_0\right\rangle\right|^2 \tag{13}$$

$$S_1=\mathrm{fix}(P_4(i)\times 10^8)\bmod 256 \tag{14}$$

$$S_2=\mathrm{fix}(P_5(i)\times 10^8)\bmod 256 \tag{15}$$

$$\boldsymbol{Q}_1=\mathrm{reshape}(S_1,M,N) \tag{16}$$

$$\boldsymbol{Q}_2=\mathrm{reshape}(S_2,M,N) \tag{17}$$

5) 利用 Latin 方阵$\boldsymbol{L}_S$、$\boldsymbol{Q}_1$和$\boldsymbol{Q}_2$生成新的密钥矩阵$\boldsymbol{Q}_3$。其中将$\boldsymbol{L}_S$作为参考矩阵，$\boldsymbol{Q}_1$和$\boldsymbol{Q}_2$分别控制查找行、列：

$$Q_3(i,j)=L_S(Q_1(i,j),Q_2(i,j)) \tag{18}$$

6) 将三通道图像R_2,G_2,B_2分别与得到的密钥矩阵$\boldsymbol{Q}_3$按位异或得到图像R_3,G_3,B_3，即：

$$R_3(i,j)=R_2(i,j)\oplus Q_3(i,j) \tag{19}$$

$$G_3(i,j)=G_2(i,j)\oplus Q_3(i,j) \tag{20}$$

$$B_3(i,j)=B_2(i,j)\oplus Q_3(i,j) \tag{21}$$

7) 对图像R_3,G_3,B_3进行加取模正向、逆向扩散处理得到单通道加密图像R_4,G_4,B_4，加取模扩散算法的正向以及逆向公式为：

$$\text{正向：}\ C_i=(C_{i-1}+S_i+P_i)\bmod 256 \tag{22}$$

$$\text{逆向：}\ D_i=(D_{i+1}+S_i+C_i)\bmod 256 \tag{23}$$

式中，C_i代表 R,G,B 这 3 个单通道加密图像；P_i代表R_3,G_3,B_3；S_i代表随机序列；D_i代表经过加取模扩散得到的单通道加密图像R_4,G_4,B_4。

8) 将 3 个单通道加密图像合并得到最终加密彩色图像I_e。

$$I_e(0,0,1)=R_4(0,0,1) \tag{24}$$

$$I_e(0,0,2)=G_4(0,0,1) \tag{25}$$

$$I_e(0,0,3)=B_4(0,0,1) \tag{26}$$

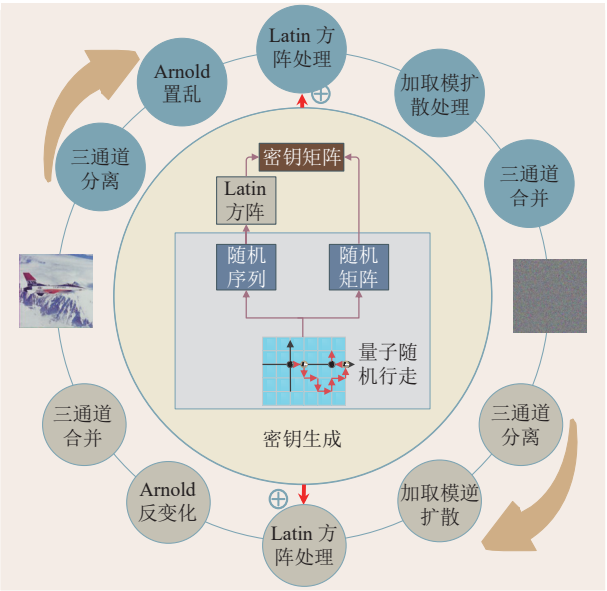


图 4 算法流程图

2.2 解密步骤

1) 将加密图像I_e的 R,G,B 三通道分离，得到 3 个单通道加密图像R_4,G_4,B_4：

$$R_4=I_e(0,0,1) \tag{27}$$

$$G_4=I_e(0,0,2) \tag{28}$$

$$B_4=I_e(0,0,3) \tag{29}$$

2) 对单通道加密图像R_4,G_4,B_4进行加取模逆向、正向逆扩散处理得到图像R_3,G_3,B_3。加取模扩散算法的正向以及逆向公式为：

$$\text{逆向：}\ C_i=(512+D_i-D_{i+1}-S_i)\bmod 256 \tag{30}$$

$$\text{正向：}\ P_i=(512+C_i-C_{i+1}-S_i)\bmod 256 \tag{31}$$

3) 将R_3,G_3,B_3这 3 幅单通道图像分别与加密阶段量子漫步产生的密钥矩阵$\boldsymbol{Q}_3$进行按位异或操作，得到图像R_2,G_2,B_2：

$$R_2(i,j)=R_3(i,j)\oplus Q_3(i,j) \tag{32}$$

$$G_2(i,j)=G_3(i,j)\oplus Q_3(i,j) \tag{33}$$

$$B_2(i,j)=B_3(i,j)\oplus Q_3(i,j) \tag{34}$$

4) 对得到的R_2,G_2,B_2这 3 幅单通道图像分别进行 Arnold 反变换，得到图像R_1,G_1,B_1。Arnold 反变换公式如下：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} \alpha\beta+1 & -\beta \\ -\alpha & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{35}$$

5) 将R_1,G_1,B_1三通道图像合并，并对其进行行列置乱逆变换，得到解密图像。

3　实验结果及性能分析

为验证加密算法的可靠性与安全性，本文主要对 Plane、Boat、Milk 和 Lena 4 幅大小为512×512的彩色图像进行仿真实验以及结果分析。本文量子漫步选用参数 (400, 801, π/3, π/2)。下面对图像的直方图、信息熵、相关性、抗攻击性、密钥空间及密钥敏感性多性能进行分析。

3.1　仿真结果

为证明该加密算法的可行性，本文对 4 幅彩色图像进行了仿真实验，实验结果如图 5 所示。由图 5 可见，在加密后的图像上无法获得任何原图像的视觉信息，而解密后的效果与原图视觉感上是一致的。

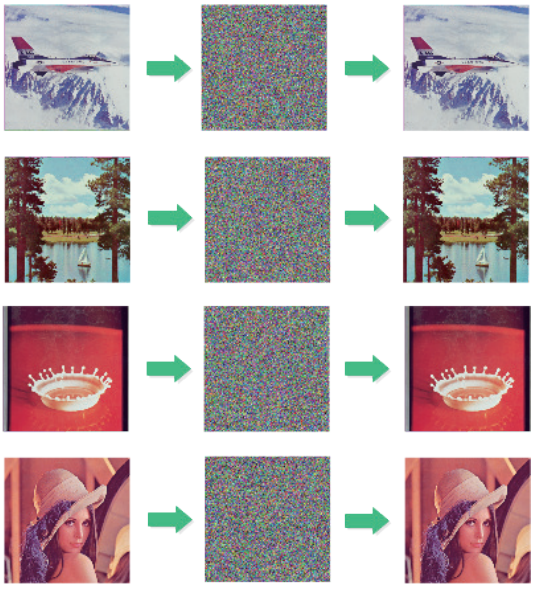
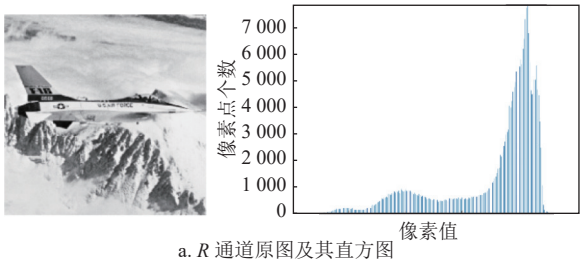


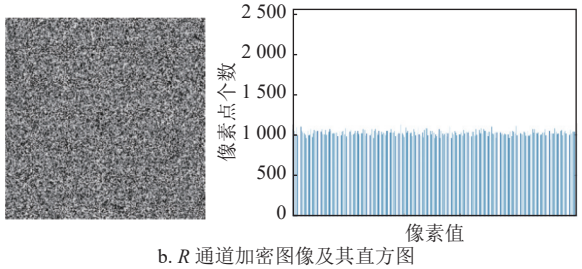
图 5　加密和解密图像

3.2　直方图分析

直方图由一系列垂直的条纹组成，用以表示数据的分布情况：横轴为像素值，代表 0～255 的色阶；纵轴表示图像中此像素值的像素点个数。本文对图像的原图及其加密图像的 *R*,*G*,*B* 三通道分别进行了直方图测试，测试结果如图 6～图 8 所示。

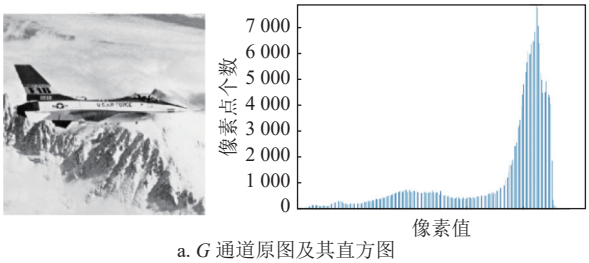


a. *R* 通道原图及其直方图

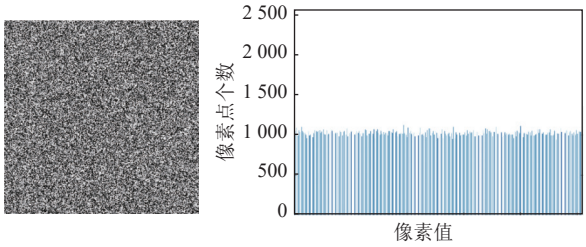


b. *R* 通道加密图像及其直方图

图 6　*R* 通道原图、加密图像及其直方图

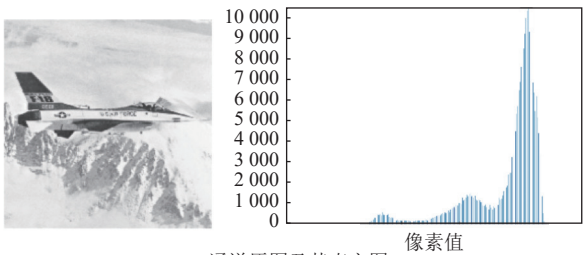


a. *G* 通道原图及其直方图

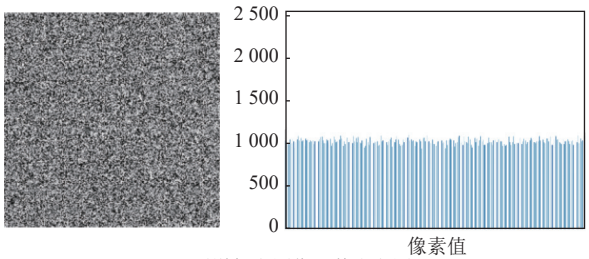


b. *G* 通道加密图像及其直方图

图 7　*G* 通道原图、加密图像及其直方图



a. *B* 通道原图及其直方图



b. *B* 通道加密图像及其直方图

图 8　*B* 通道原图、加密图像及其直方图

原图像的直方图像素分布不均，高低错落易于进行统计学分析，而加密后的图像像素分布均匀，无法据此进行统计学分析，具有良好的加密效果，能有效抵御统计学分析攻击。

3.3 信息熵分析

信息熵在描述图片像素点混乱程度上扮演着重要的角色。信息熵可以由以下公式计算得出：

$$H(p)=\sum_{i=1}^{N}P(p_i)\log_2 P(p_i) \tag{36}$$

式中，p_i代表每个像素值出现的概率；N表示整幅图像像素点的数量总和。加密过程中像素值为[0,255]，加密图像信息熵值越接近8.0，说明图像的加密效果越好。本文测试了4幅加密图像的熵值，信息熵值如表1所示，并将加密的Lena图像与文献[36]及文献[37]中的实验Lena图像作了熵值对比。由本方案得到加密图像的信息熵值约在7.999 2左右，接近于理想值8。因此，本文提出的加密算法具有良好的加密效果。

表1 加密图像信息熵

图像	通道			平均信息熵
	*R*通道	*G*通道	*B*通道	
Plane	7.999 3	7.999 4	7.999 3	7.999 3
Boat	7.999 3	7.999 2	7.999 2	7.999 2
Milk	7.999 2	7.999 1	7.999 3	7.999 2
Lena	7.999 3	7.999 4	7.999 3	7.999 3
文献[36]中的实验Lena图像	7.987 4	7.987 2	7.986 6	7.987 1
文献[37]中的实验Lena图像	7.997 4	7.997 1	7.997 2	7.997 2

3.4 相关性分析

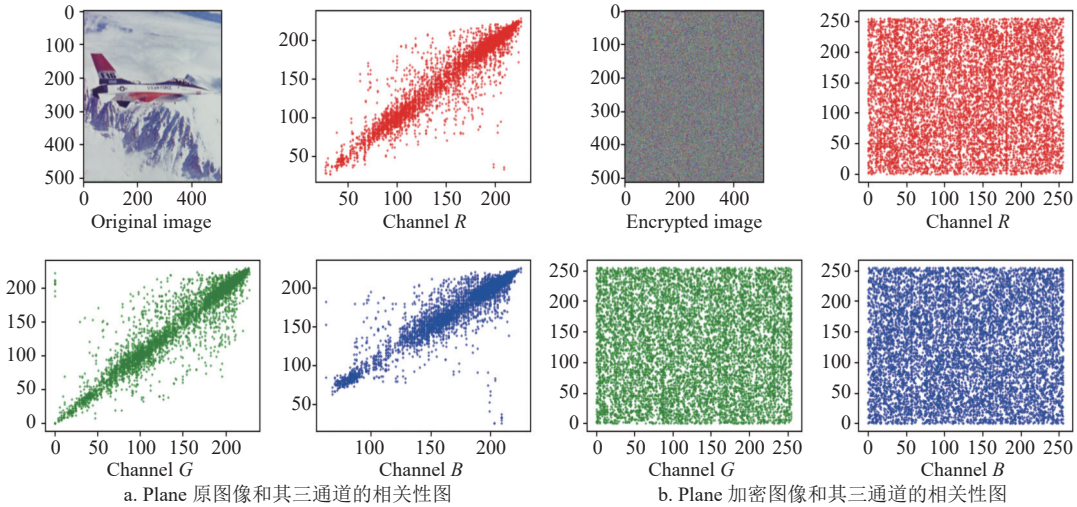
一副完整的图像中相邻像素之间具有很强的相关性，而加密效果好的算法往往能消除像素间的相关性。相邻像素的相关性主要体现在水平、垂直和对角方向上，且一般的彩色图像像素之间的相关性基本近似线性关系且相关系数趋近于1。对每一幅图像随机选择3 000对像素值分别计算各方向的相关系数，计算相关系数的公式为：

$$r_c=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{37}$$

式中，$\operatorname{cov}(x,y)$表示相邻像素点x和y之间的协方差；$D(x)$和$D(y)$分别表示像素点x和y的方差。本方案对Plane、Boat、Milk 3幅彩色图像的加密图像进行了相关性分析，测试结果如表2所示(视觉化效果如图9～图11所示)。从相关性数值来看，各个方向的相关性均趋近于0，从图中看到加密前的图像相关性很强、呈线性关系，而加密后的图像像素之间的关系基本上不存在，像素无序分布，表明算法具有良好的加密效果。通过与其他方法比较，说明该加密算法有较好的加密效果。

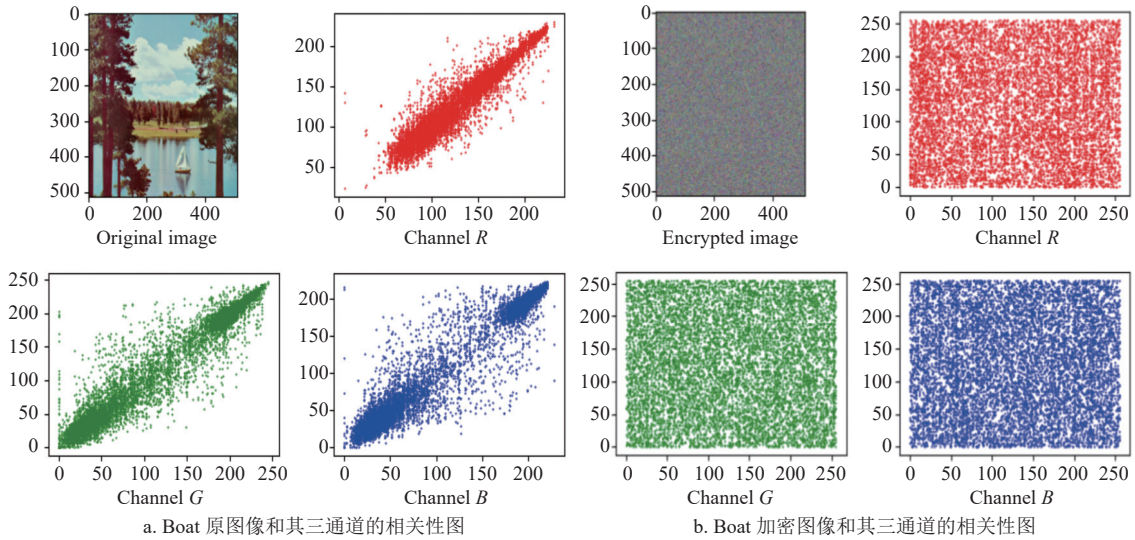
表2 像素相关性分析

图像	方向	加密图像		
		*R*通道	*G*通道	*B*通道
Plane	水平	−0.012 8	0.026 8	−0.008 7
	垂直	−0.003 5	0.009 4	0.016 7
	对角	0.006 2	−0.001 3	−0.013 5
Boat	水平	0.004 9	0.003 3	0.002 3
	垂直	0.001 0	0.009 9	−0.017 2
	对角	−0.026 8	0.006 7	−0.002 1
Milk	水平	0.001 3	0.013 0	0.027 0
	垂直	−0.016 2	−0.009 5	0.007 1
	对角	0.003 5	0.003 7	−0.004 2



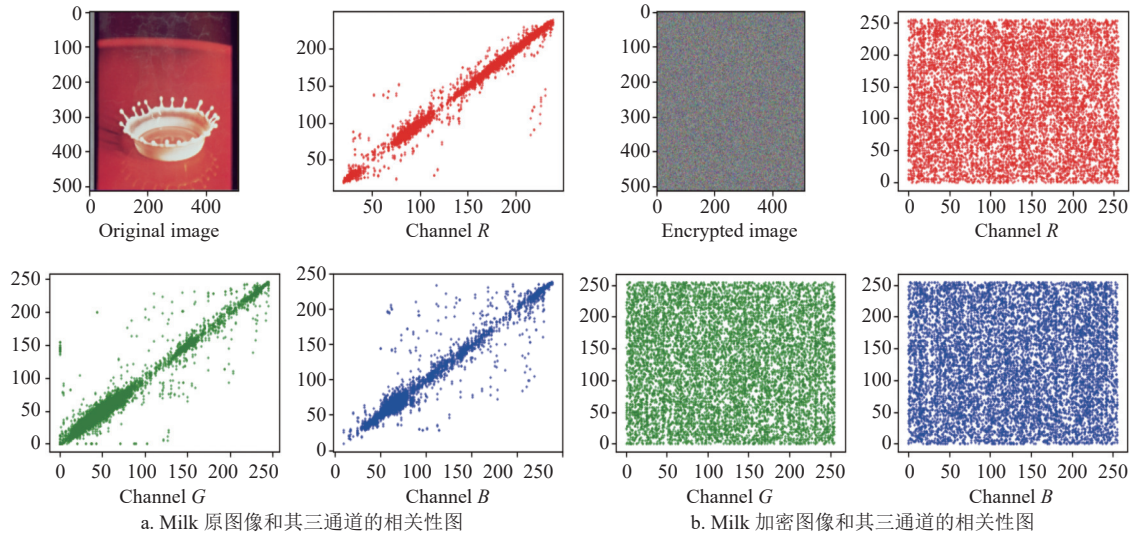
a. Plane 原图像和其三通道的相关性图　　b. Plane 加密图像和其三通道的相关性图

图9 图像Plane和其对应的加密图像的三通道相关性图



a. Boat 原图像和其三通道的相关性图　　b. Boat 加密图像和其三通道的相关性图

图 10　图像 Boat 和对应的加密图像的三通道相关性

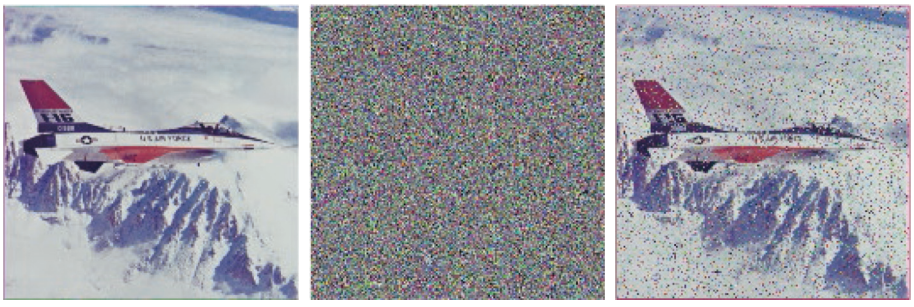


a. Milk 原图像和其三通道的相关性图　　b. Milk 加密图像和其三通道的相关性图

图 11　图像 Milk 和其对应的加密图像的三通道相关性

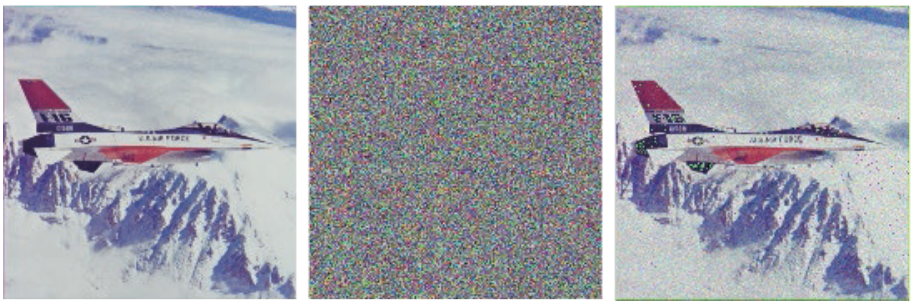
3.5　抗噪声攻击性分析

在加密图像的数据传输过程中，可能会或多或少地掺入噪声，从而影响图像的解密。所以对于加密图像来说，抵抗噪声的能力是评价加密算法的一个重要指标。高斯噪声和椒盐噪声是最为常见的两类噪声，对加密图像 Plane 分别加入强度为 5% 的椒盐噪声和均值为 0、方差为 0.000 5 的高斯噪声，图 12 和图 13 分别为加密图像 Plane 加入椒盐噪声和高斯噪声之后的图像以及其对应的解密后的图像。实验结果表明，该加密算法有着良好的抵抗噪声的能力。



a. 原图像　　b. 加入椒盐噪声的加密图像　　c. 解密后的图像

图 12　加入椒盐噪声的加密图像及对应的解密图像

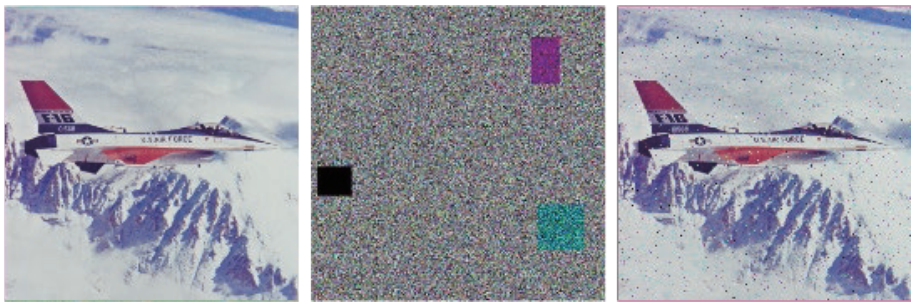


a. 原图像 b. 加入高斯噪声的加密图像 c. 解密后的图像

图 13 加入高斯噪声的加密图像及对应的解密图像

3.6 抗裁剪攻击性分析

加密图像在网络传输中，可能会出现某一块区域的像素点丢失。因此，加密算法必须具有在加密图像缺损情况下解密的能力。如果在加密图像缺损情况下，原始信息在解密之后得以保留，说明该算法可以有效抵抗外界的裁剪攻击。对加密图像 Plane 移除一块80×80像素的红色通道、一块50×80像素的绿色通道和一块60×50像素的全通道，然后对其进行密，裁剪加密图像及其对应的解密之后的图像如图 14 所示。实验结果表明，在加密图像的某一块区域的像素值缺失时，经过解密可以恢复原始图像信息，说明该加密算法具有良好的抵抗裁剪攻击的能力。



a. 原图像 b. 经剪裁后的加密图像 c. 解密后的图像

图 14 裁剪之后的加密图像及对应的解密图像

3.7 密钥空间分析

一个优良的加密算法往往具有一个足够大的密钥空间。密钥空间越大，该算法抵抗外界暴力攻击的能力越强。在本加密算法中使用了交替量子漫步，交替量子漫步提供了无限的密钥空间。密钥空间在理论上达到 2^{100} 时，加密图像就可以有效地抵抗暴力攻击。如果计算精度为10^{-15}，那么该算法的密钥空间为10^{60}，这对保护加密图像的安全性已经足够了，因此该算法可以有效抵抗外部的暴力攻击。

3.8 密钥敏感性分析

差分攻击是破解加密图像的另一种常用手段。差分攻击是外界对原待加密图像的数据信息做微小的变动，然后利用加密算法对改变后的数字图像和原待加密图像分别进行加密，然后把两幅加密后的密文图像进行对比，找出原图像数据与加密图像数据之间的内在联系，利用二者之间的联系来进行破解加密图像。为了应对差分攻击，加密算法应该对密钥足够敏感。即当密钥发生一点变化，产生的加密结果应该是与原加密结果完全不同的。像素改变率 (NPCR) 和统一平均变化强度 (UACI) 是检验加密算法的密钥敏感性的两个重要指标，分别定义为：

$$\begin{cases} \mathrm{NPCR} = \dfrac{\sum_{i,j} Q(i,j)}{MN} \times 100\% \\ \mathrm{UACI} = \dfrac{\sum (P_1(i,j) - (P_2(i,j))}{255MN} \times 100\% \end{cases} \tag{38}$$

式中，P_1和P_2分别代表密钥改变前后生成的两幅加密图像。如果 $P_1(i,j) = P_2(i,j)$，$Q_1(i,j) = 0$，反之 $Q(i,j) = 1$，稍微改变随机行走的一个参数，产生其对应的加密图像，然后计算两幅加密图像的 NPCR 和 UACI，结果如表 3 所示。并将 Lena 图像的测试结果与文献 [38] 及文献 [39] 中的测试结果进行对比。测试结果表明，该加密算法具有良好的密钥敏感性。

表 3　密钥敏感性分析

%

图像	NPCR				UACI			
	R	*G*	*B*	平均	*R*	*G*	*B*	平均
Plane	99.595 6	99.623 9	99.617 0	99.612 2	33.495 2	33.456 9	33.476 4	33.476 2
Boat	99.601 0	99.604 4	99.612 4	99.605 9	33.395 9	33.533 0	33.450 4	33.459 8
Milk	99.623 9	99.634 9	99.602 9	99.620 6	33.441 9	33.399 4	33.416 7	33.419 3
Lena	99.601 7	99.611 3	99.633 4	99.616 1	33.369 2	33.528 3	33.525 6	33.474 4
文献[38]中的实验Lena图像				99.58				33.38
文献[39]中的实验Lena图像				99.629 9				31.834 6

4　结 束 语

本文将 Arnold 变换与 Latin 方阵、量子漫步相结合，设计了一种新型的彩色图像加密方法。首先把彩色图像三通道分离，然后通过 Arnold 变换对三幅单通道图像进行置乱处理。另一方面，利用量子漫步产生 Latin 方阵和随机矩阵对初步置乱图像进一步处理，然后对处理之后的图像使用加取模扩散方法进行像素值的变换，最后把 3 个单通道图像合并得到加密图像。经过实验仿真结果分析，加密图像的相关性非常低，信息熵接近于 8，说明本文提出的算法具有比较良好的抵抗统计分析的能力；经过噪声攻击和裁剪攻击之后的加密图像在经过解密之后仍然可以看到原图像信息，说明本文提出的算法具有较强的鲁棒性；算法的密钥空间足够大且密钥敏感性良好，能够抵抗差分攻击。

参　考　文　献

[1] WANG X, ZHAO J, LIU H. A new image encryption algorithm based on chaos[J]. Optics Communications, 2012, 285(5): 562-566.

[2] DIACONU A V, LOUKHAOUKHA K. An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher[J]. Mathematical Problems in Engineering, 2013(3): 1-10.

[3] WANG Y, WONG K W, LIAO X, et al. A new chaos-based fast image encryption algorithm[J]. Applied Soft Computing, 2011, 11(1): 514-522.

[4] WANG X, FENG L, ZHAO H. Fast image encryption algorithm based on parallel computing system[J]. Information Sciences, 2019, 486: 340-358.

[5] LAIPHRAKPAM D S, KHUMANTHEM M S. Medical image encryption based on improved ElGamal encryption technique[J]. Optik, 2017, 147: 88-102.

[6] SAVAKAR D G, GHULI A. Robust invisible digital image watermarking using hybrid scheme[J]. Arabian Journal for Science and Engineering, 2019, 44(4): 3995-4008.

[7] PRAJWALASIMHA S N, MOHAN C S, CHETHAN S S. Digital image watermarking based on sine hyperbolic transformation[C]//2019 IEEE International Conference on Electrical, Computer and Communication Technologies, [S.l.]: IEEE, 2019: 1-6.

[8] BARNI M, PODILCHUK C I, BARTOLINI F, et al. Watermark embedding: Hiding a signal within a cover image[J]. IEEE Communications Magazine, 2001, 39(8): 102-108.

[9] ZHU P, JIA F, ZHANG J. A copyright protection watermarking algorithm for remote sensing image based on binary image watermark[J]. Optik, 2013, 124(20): 4177-4181.

[10] ZHU S, ZHU C. Secure image encryption algorithm based on hyperchaos and dynamic DNA coding[J]. Entropy, 2020, 22(7): 772.

[11] ZHEN P, ZHAO G, MIN L, et al. Chaos-based image encryption scheme combining DNA coding and entropy[J]. Multimedia Tools and Applications, 2016, 75(11): 6303-6319.

[12] 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): 230302.
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): 230302.

[13] LONG Z M, BIN Y U. Chosen plaintext attack for hyper-chaotic system image encryption algorithm[J]. Computer Engineering, 2012, 38(17): 148-151.

[14] XU X J, WANG L H, WANG J Z, et al. A Fast image encryption algorithm based on high-dimension chaotic system[C]//2012 IEEE 14th International Conference on Communication Technology. Chengdu: IEEE, 2012: 829-835.

[15] MIRZAEI O, YAGHOOBI M, IRANI H. A new image encryption method: Parallel sub-image encryption with hyper chaos[J]. Nonlinear Dynamics, 2012, 67(1): 557-566.

[16] PAN P, PAN Y, WANG Z, et al. Provably secure encryption schemes with zero setup and linear speed by using Rubik's cubes[J]. IEEE Access, 2020, 8: 122251-122258.

[17] LOUKHAOUKHA K, CHOUINARD J Y, BERDAI A. A secure image encryption algorithm based on Rubik's cube principle[J]. Journal of Electrical and Computer Engineering, 2012(1): 173931.

[18] ABDULLATIF A A, ABDULLATIF F A, NAJI S A. An enhanced hybrid image encryption algorithm using Rubik's cube and dynamic DNA encoding techniques[J].

Periodicals of Engineering and Natural Sciences, 2019, 7(4): 1607-1617.
[19] LIU X, CAO Y, LU P, et al. Optical image encryption technique based on compressed sensing and Arnold transformation[J]. Optik, 2013, 124(24): 6590-6593.
[20] BATOOL S I, WASEEM H M. A novel image encryption scheme based on Arnold scrambling and Lucas series[J]. Multimedia Tools and Applications, 2019, 78: 27611-27637.
[21] LIU Z, CHEN H, LIU T, et al. Image encryption by using gyrator transform and Arnold transform[J]. Journal of Electronic Imaging, 2011, 20(1): 013020.
[22] DEBNATH D, GHOSH E, BANIK B G. Multiple RGB image steganography using Arnold and discrete cosine Transformation[C]//International Ethical Hacking Conference. Kolkata, India: [s.n.], 2019: 151-161.
[23] BHATTI U A, YUAN L, YU Z, et al. Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption[J]. IEEE Access, 2020, 8: 76386-76398.
[24] QU G, MENG X, YIN Y, et al. Optical color image encryption based on Hadamard single-pixel imaging and Arnold transformation[J]. Optics and Lasers in Engineering, 2021, 137(20): 106392.
[25] DENG G W, WEI D, JOHANSSON J R, et al. Charge number dependence of the dephasing rates of a graphene double quantum dot in a circuit QED architecture[J]. Physical Review Letters, 2015, 115(12): 126804.
[26] LI X Y, CHANG Y, ZHANG S B, et al. Quantum blind signature scheme based on quantum walk[J]. International Journal of Theoretical Physics, 2020, 59(7): 2059-2073.
[27] PATEL A, RAGHUNATHAN K S. Search on a fractal lattice using a quantum random walk[J]. Physical Review A, 2012, 86(1): 012332.
[28] DENG G W, WEI D, LI S X, et al. Coupling two distant double quantum dots with a microwave resonator[J]. Nano Letters, 2015, 15(10): 6620-6625.
[29] MA Y, LI N, ZHANG W, et al. Image encryption scheme based on alternate quantum walks and discrete cosine transform[J]. Optics Express, 2021, 29(18): 28338-28351.
[30] ABD-EL-ATTY B, ILIYASU A M, ALANEZI A, et al. Optical image encryption based on quantum walks[J]. Optics and Lasers in Engineering, 2021, 138: 106403.
[31] WU Y, NOONAN J P, AGAIAN S. Dynamic and implicit latin square doubly stochastic s-boxes with reversibility[C]//2011 IEEE International Conference on Systems, Man, and Cybernetics. [S.l.]: IEEE, 2011: 3358-3364.
[32] HUA Z Y, LI J Y, CHEN Y Y, et al. Design and application of an *S*-box using complete Latin square[J]. Nonlinear Dynamics, 2021, 104(1): 807-825.
[33] WU Y, ZHOU Y, NOONAN J P, et al. Design of image cipher using latin squares[J]. Information Sciences, 2014, 264: 317-339.
[34] MACHKOUR M, SAAIDI A, BENMAATI M L. A novel image encryption algorithm based on the two dimensional logistic map and the Latin square image cipher[J]. 3D Research, 2015, 6(4): 1-18.
[35] ZHANG X, WU T, WANG Y, et al. A novel chaotic image encryption algorithm based on Latin square and random shift[J]. Computational Intelligence and Neuroscience, 2022, 24(11): 1574.
[36] LIU H, WANG X, KADIR A. Color image encryption using Choquet fuzzy integral and hyper chaotic system[J]. Optik-International Journal for Light and Electron Optics, 2013, 124(18): 3527-3533.
[37] YE G, HUANG X. An efficient symmetric image encryption algorithm based on an intertwining logistic map[J]. Neurocomputing, 2017, 251: 45-53.
[38] 赵智鹏, 周双, 王兴元. 基于深度学习的新混沌信号及其在图像加密中的应用[J]. 物理学报, 2021, 70(23): 230502.
ZHAO Z P, ZHOU S, WANG X Y. A new chaotic signal based on deep learning and its application in image encryption[J]. Acta Physica Sinica, 2021, 70(23): 230502.
[39] ÇAVUŞOĞLU Ü, KAÇAR S, PEHLIVAN I, et al. Secure image encryption algorithm design using a novel chaos based S-Box[J]. Chaos, Solitons & Fractals, 2017, 95: 92-101.

编 辑 张 莉