Statistics and Application 统计学与应用, 2026, 15(5), 74-87
Published Online May 2026 in Hans. https://www.hanspub.org/journal/sa
https://doi.org/10.12677/sa.2026.155108

Hans汉斯

基于Moore扫描曲线和DNA编码的混沌图像加密算法

陈　星，郑枭宇，赵　妍，王可心，叶瑞松*

汕头大学数学系，广东　汕头

收稿日期：2026年4月12日；录用日期：2026年5月4日；发布日期：2026年5月14日

摘　要

本文结合混沌系统，Moore扫描曲线与DNA编码的技术，提出一种新型灰度图像加密算法。该算法以二维Arnold混沌映射为核心，利用明文图像SHA-256哈希值动态修正映射参数与初始值，实现密钥与明文的高度关联；基于混沌序列驱动Moore扫描曲线生成自适应置乱索引，对图像像素完成空间位置置乱，有效打破像素间的空间邻域相关性；引入动态DNA编码运算规则，利用混沌序列随机确定DNA加法、减法、异或及同或运算的组合模式，对置乱图像实施扩散操作，实现像素灰度值的深度混淆。通过卡方检验、相关系数、信息熵、差分攻击等指标对算法性能进行详细分析验证，实验结果表明，该算法的密文图像灰度分布均匀，相邻像素相关系数、信息熵以及密钥与明文敏感性指标均很接近理论值，算法能有效抵御统计分析攻击、暴力攻击与差分攻击等。

关键词

图像加密，Arnold混沌映射，Moore扫描曲线，DNA编码

Chaotic Image Encryption Algorithm Based on Moore Scanning Curve and DNA Encoding

Xing Chen, Xiaoyu Zheng, Yan Zhao, Kexin Wang, Ruisong Ye*

Department of Mathematics, Shantou University, Shantou Guangdong

Received: April 12, 2026; accepted: May 4, 2026; published: May 14, 2026

Abstract

This paper integrates techniques of chaotic system, Moore scanning curve, and DNA encoding to

*通讯作者。

文章引用: 陈星, 郑枭宇, 赵妍, 王可心, 叶瑞松. 基于 Moore 扫描曲线和 DNA 编码的混沌图像加密算法[J]. 统计学与应用, 2026, 15(5): 74-87. DOI: 10.12677/sa.2026.155108

propose a novel grayscale image encryption algorithm. The algorithm takes the two-dimensional Arnold chaotic map as its core, utilizing the SHA-256 hash value of the plain image to dynamically adjust the map's parameters and initial values, thereby achieving a high degree of association between the key and the plain image. Based on chaotic sequences driving the Moore scanning curve, adaptive scrambling indices are generated to permute the spatial positions of image pixels, effectively disrupting the spatial neighborhood correlations among pixels. Dynamic DNA encoding and operation rules are introduced, where chaotic sequences randomly determine the combination modes of DNA addition, subtraction, XOR, and XNOR operations to perform diffusion operation on the scrambled image, achieving deep confusion of pixel gray values. The algorithm's performance is thoroughly analyzed and validated through metrics such as chi-square test, correlation coefficient, information entropy, and differential attack and so on. Experimental results show that the cipher image produced by the encryption algorithm exhibits uniform grayscale distribution, with adjacent pixel correlation coefficients, information entropy, and key/plaintext sensitivity indices all closely approximating theoretical values. The algorithm effectively resists statistical analysis attacks, brute-force attacks, and differential attacks, etc.

Keywords

İmage Encryption, Arnold Chaotic Map, Moore Scanning Curve, DNA Encoding

1. 引言

进入数字化时代，图像已经成为网络信息传递与交流的主要载体，广泛应用于医疗诊断、军事通信、商业通信及个人隐私信息等诸多保密场景。与此同时，网络传输中的图像信息极易受到非法信息窃取和恶意篡改等安全威胁，保障图像信息传输与储存的安全性、完整性已成为各界关注的热点问题。由于图像数据相邻像素间相关性强、数据量大等固有特点，传统数据加密算法 DES、RSA 等不再适合图像加密的实际应用，寻找适合图像信息的加密算法日益成为研究热点[1]。混沌系统具有高度的初值和参数敏感性、生成的序列具有很好的伪随机性和遍历性，其动力学行为与密码学所要求的混淆与扩散原则高度契合，因此基于混沌系统的图像加密算法备受青睐，日益凸显其卓越性能与广阔应用前景[2]-[5]。

空间扫描曲线可以快速遍历扫描图像的每一个像素并进行重排，达到破坏明文图像的像素空间位置次序，因而被广泛应用于图像置乱，比如只能实现方形图像置乱的标准Zigzag扫描[6]，V形扫描[7]，适用于任何大小的图像置乱的改进Zigzag扫描[8] [9]。分形几何理论表明，迭代函数系统可以便捷生成空间填充曲线，该类曲线具有分形的自相似结构特性，可用于扫描图像的所有像素并置乱图像。文献中最常用的分形填充曲线是Hilbert曲线[10]-[12]，本文利用文[13]构造的迭代函数系统生成另一类空间填充曲线，即Moore扫描曲线，并用于设计加密算法的置乱过程。Moore扫描曲线作为Hilbert扫描曲线的一种变体，具有优秀的局部保持性和全局遍历性，能够将二维图像像素映射为一维向量，且保持部分空间邻近关系。为了提高利用Moore扫描曲线置乱图像的效率，本文改进了固定模式的扫描路径，设计了一种与明文内容相关的自适应扫描策略，获得了“一图一密”的加密效果。

随着图像加密技术的发展，基于混沌系统与其他技术相结合的图像加密算法日益成为研究热点。DNA编码运算技术是分子生物学和计算机科学相结合的产物，通过二进制互补与碱基互补的映射关系以及四种DNA运算规则进行仿生运算，具有并行计算性能高、储存密度高和耗能低等特性，使其在图像加密领

域拥有巨大发展前景，结合混沌系统和DNA编码运算的图像加密算法取得了优良的加密性能[14]-[17]。文[14]提出了一种结合DNA编码运算与混沌系统的图像加密算法。该方法利用SHA-3 算法生成明文图像的哈希值动态改变超混沌系统的初始参数，从而增强算法对明文的敏感性；通过混沌系统生成的伪随机序列所得到的S盒和图像转换的DNA序列进行运算以及图像置乱操作，从而进一步提升了加密算法的密钥敏感性，能有效抵御穷举攻击、统计攻击及差分攻击。文[15]提出超混沌序列驱动的动态协同模式，通过高维混沌序列调控DNA编码与运算规则切换，增强了加密算法的安全性能。文[16]结合混沌系统和DNA技术，提出了一种彩色混沌图像加密算法。该加密算法首先计算明文图像的DNA编码矩阵的汉明距离与圆距离，并应用到控制混沌系统所生成的密钥流。加密过程通过DNA异或等运算实现，取得了较高的安全性，能够有效抵抗明文攻击、差分攻击及统计分析攻击等多种威胁。文[17]通过复合分段线性映射与正弦映射，构建了一个增强混沌特性的新系统，并结合DNA编码运算技术设计一个性能良好的图像加密方案。

本文将自适应 Moore 扫描曲线的像素位置置乱，DNA 编码运算的像素灰度值扩散以及二维 Arnold 混沌系统的优良伪随机性相结合，提出一种新型混沌图像加密算法。针对现有混沌加密方法中密钥与明文弱关联易受已知明文攻击、传统置乱路径固定难以彻底打破空间相关性以及单一扩散操作非线性不足等问题，本文算法的创新之处包括：1) 构建密钥–明文强耦合机制：利用明文哈希值动态修正 Arnold 映射的参数与初始值，生成与明文高度相关的混沌序列。2) 设计自适应置乱策略：设计了与明文相关的 Moore 扫描曲线，构造自适应的像素位置置乱方案。3) 提出动态 DNA 扩散增强机制：引入动态 DNA 编码与运算规则，对置乱后的像素值进行扩散，进一步提升加密算法的安全性能。

2. 相关知识

2.1. 二维 Arnold 混沌映射

经典的 Arnold 映射(又称猫脸映射)是一种定义在二维单位环面 $\boldsymbol{T}^2=[0,1)\times[0,1)$ 上的混沌系统[18]，其标准形式见公式(1)：

$$\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}x_n\\ y_n\end{pmatrix}\bmod 1, n=0,1,2,\cdots. \tag{1}$$

该映射是保面积的混沌映射，其离散化可以用于数字图像的像素位置置乱，但是该映射安全性极低，无法实际应用。为了提升其安全性，将其推广到更一般的情况，通过引入两个独立的实参数 a 和 b 来扩大系统的参数空间，并使得映射对初值具有更高的敏感性，推广的二维 Arnold 映射见公式(2)：

$$\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & a\\ b & 1+ab\end{pmatrix}\begin{pmatrix}x_n\\ y_n\end{pmatrix}\bmod 1, n=0,1,2,\cdots \tag{2}$$

其中初值 $x_0,y_0\in(0,1)$，参数 $a,b\in R$。该映射的行列式 $\det(A)=1$，同样是保面积的。该映射呈现强烈的混沌行为，生成的序列 $\{x_n,y_n\}$ 具有优良的伪随机性、对初始值和参数的高度敏感性，很适合用于生成伪随机序列并设计图像加密算法[4]。在加密算法中，该映射的初始值 x_0,y_0 和系统参数 a,b 可作为外部密钥。为了增强算法与明文的相关性，利用明文图像的 SHA-256 哈希值对外部密钥进行修正，生成“一图一密”的动态密钥，从而显著提升算法抵抗差分攻击和已知/选择明文攻击的能力。

2.2. Moore 扫描曲线

Moore 扫描曲线是 1900 年由数学家 Moore 提出的一种连续、无交叉的二维空间填充曲线，属于 Hilbert 扫描曲线的同构变种，其计算机实现能在有限区域内通过单一连续路径无遗漏地覆盖所有离散网格点，

因此可以用于扫描图像的所有像素。Hilbert 扫描曲线可通过简单的迭代算法实现，而 Moore 扫描曲线可由 Hilbert 扫描曲线进行变换得到。将 n 级分辨率的 Moore 扫描曲线的位置索引矩阵记为 M_{2^n}，则 M_{2^n} 可通过变换 $n-1$ 级分辨率的 Hilbert 扫描曲线的位置索引矩阵 $H_{2^{n-1}}$ 得到，其矩阵迭代算法见公式(3)~(4) [13]。

Step 1. 迭代公式(3)，得到 $n-1$ 级 Hilbert 扫描矩阵 $H_{2^{n-1}}$，

$$H_2=\begin{bmatrix}2 & 3\\ 1 & 4\end{bmatrix}, H_{2^{k+1}}=\begin{bmatrix}H_{2^k}+4^k & H_{2^k}+2\times 4^k\\ rot90\left(fliplr\left(H_{2^k}\right),3\right) & H_{2^k}^{\mathrm{T}}+3\times 4^k\end{bmatrix}, k=1,2,\cdots,n-2. \tag{3}$$

其中 $rot90(H,r)$ 为将矩阵 H 逆时针旋转 $r\times 90^\circ$，$fliplr(H)$ 实现矩阵 H 的左右翻转。

Step 2. 通过公式(4)得到 n 级 Moore 扫描矩阵 M_{2^n}，对应 1~4 级分辨率的 Moore 扫描曲线分别如图 1(a)~(d)。

$$M_{2^n}=\begin{bmatrix}rot90\left(H_{2^{n-1}},1\right)+4^{n-1} & rot90\left(H_{2^{n-1}},3\right)+2\times 4^{n-1}\\ rot90\left(H_{2^{n-1}},1\right) & rot90\left(H_{2^{n-1}},3\right)+3\times 4^{n-1}\end{bmatrix}. \tag{4}$$

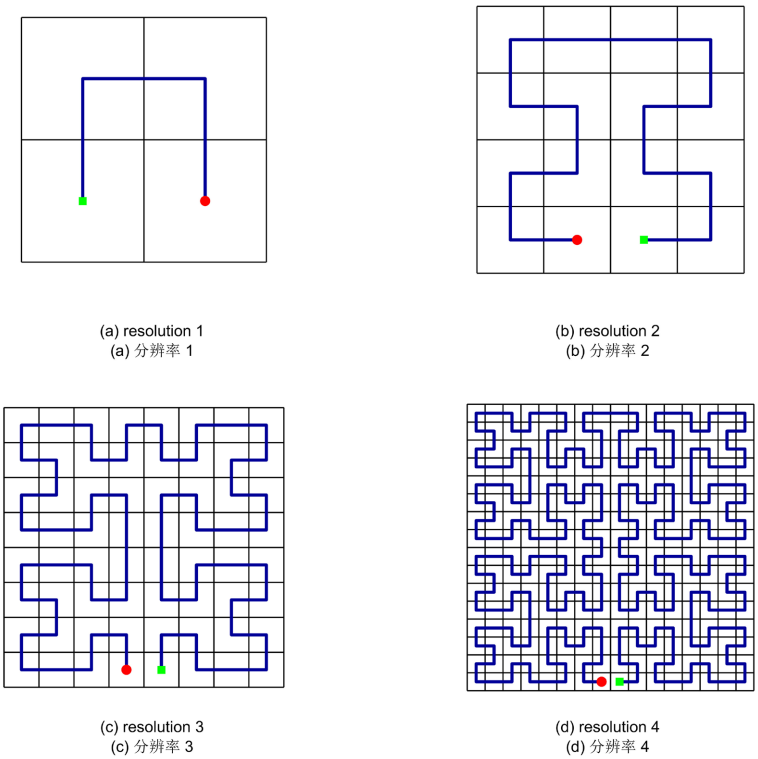


Figure 1. Moore scanning curves
图 1. Moore 扫描曲线

2.3. DNA 编码与运算

2.3.1. DNA 编码规则

DNA 的四种碱基为 A (腺嘌呤)、T (胸腺嘧啶)、G (鸟嘌呤)和 C (保胞嘧啶)。DNA 编码通过将二进制数或十进制数与四种碱基对应，将二进制数 00，01，10 和 11 (或十进制数 0，1，2，3)对应到四种碱基进行编码。根据 Watson-Crick 互补规则，DNA 碱基有 8 种可以实施的编码、解码规则，见表 1 [19]。

Table 1. DNA encoding and decoding rules
表 1. DNA 编码和解码规则

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

2.3.2. DNA 运算规则

DNA 运算包括加法、减法、异或和同或运算法则，见表 2、表 3。加密算法中 DNA 运算符号统一记为 Δ_r，根据 r 值获取对应的运算规则，定义如公式(5)所示。运算采用查表法，提高运算效率。

$$\Delta_r = \begin{cases} +, r = 1 \\ -, r = 2 \\ \oplus, r = 3 \\ \odot, r = 4 \end{cases} \tag{5}$$

Table 2. DNA addition and subtraction operation
表 2. DNA 加法和减法运算

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

Table 3. DNA XOR and XNOR operation
表 3. DNA 异或、同或运算

⊕	A	T	G	C	⊙	A	T	G	C
A	T	T	G	C	A	T	A	C	G
T	A	A	C	G	T	A	T	G	C
G	G	C	A	T	G	C	G	T	A
C	C	G	T	A	C	G	C	A	T

2.3.3. 动态 DNA 运算

在加密过程中，明文图像的像素动态选取由混沌系统生成的 DNA 编码、解码以及运算规则，则可以增强加密算法的复杂性，提升加密算法的安全性。本文的 DNA 编码解码采用统一的某一个规则号(可随机选取规则 1~8)，运算规则采用动态运算规则，实现对明文的每一个 DNA 编码采用随机的运算规则。

3. 加密算法

本文的加密算法包含置乱与扩散两个核心环节，置乱旨在对像素的空间位置进行随机化置换；扩散则致力于通过修改像素的灰度值或颜色分量，实现明密文统计特性的高度分散。利用自适应 Moore 扫描

曲线对图像实施空间置乱；借助二维 Arnold 混沌映射生成密钥流与 DNA 运算规则序列，并引入 DNA 编码运算对置乱图像进行扩散操作，最终得到密文图像。加密的流程图如图 2 所示，具体步骤包括 Step 1~Step 7。

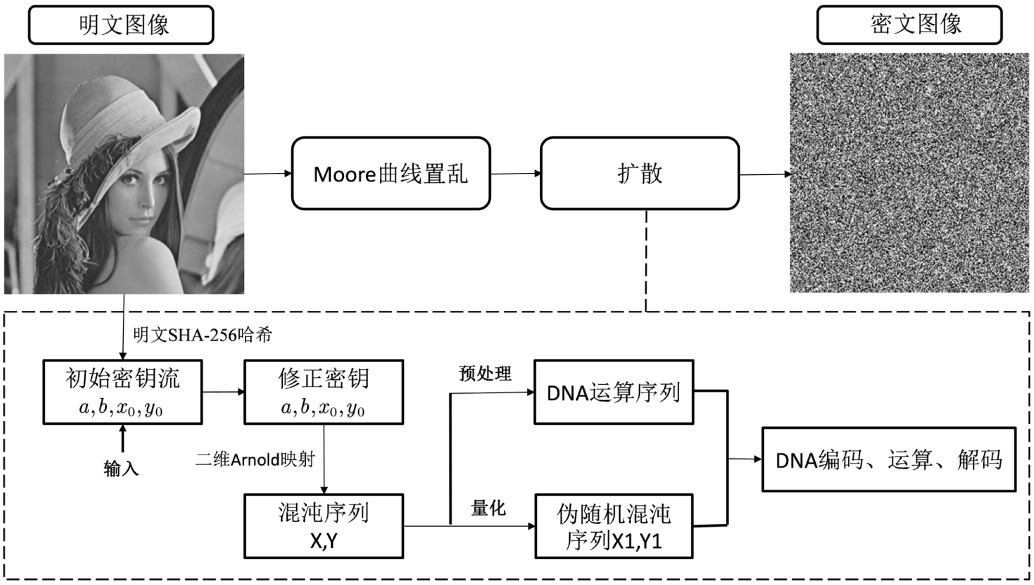


Figure 2. Flow diagram
图 2. 流程图

Step 1. 读入灰度图像 P (大小为 $L=M\times N$)，用函数 reshape 转化 P 为向量 V，长度为 L。通过公式(6)计算 T 值。

$$T=\mathrm{mod}\left(sum\left(V\right),139\right)+111 \tag{6}$$

T 将用于设计基于 Moore 曲线扫描的置乱算法，使得图像像素位置的置乱依赖于明文信息，也将用于扔掉混沌序列的前面过渡态点数，使得用于加密的混沌序列性能更好。

Step 2. 通过 2.2 节的方法生成 Moore 扫描曲线的矩阵 S，大小为 $2^n\times 2^n$，其中 n 为满足 $2^n\times 2^n\geq L$ 的最小正整数，即 $n=\mathrm{ceil}\left(\log_4 L\right)$，函数 $\mathrm{ceil}\left(x\right)$ 返回不小于 x 的最小整数。用 T 改变扫描的起始位置，并自适应地实现任意大小的图像的位置置乱。将 S 转化为一维向量 SV，将 SV 中大于 L 的元素丢弃，剩下的 L 个元素按原有的先后顺序排列，得到 $1,2,\cdots,L$ 的一个置换，记为 ind，用以置乱图像像素。

为了使得置乱具有自适应性，希望明文图像的微小差异可以导致置乱效果差异巨大，用 Moore 扫描曲线设计置乱算法时，将向量 V 的前面 T 个值砍断，搬至尾部，得到新向量 $V1$。然后根据位置索引 ind，从 $V1$ 中随机获取元素，得到的向量记为 $V2$，见公式(7)：

$$V2\left(i\right)=V1\left(ind\left(i\right)\right),i=1,2,\cdots,L \tag{7}$$

Step 3. 采用二维 Arnold 混沌映射(8)来生成混沌序列。

$$\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix}=\begin{pmatrix}1 & a\\ b & 1+ab\end{pmatrix}\begin{pmatrix}x_n\\ y_n\end{pmatrix}\mathrm{mod}1 \tag{8}$$

设定的外部密钥为 $a=3.31,b=19.17,x_0=0.5,y_0=0.5$。首先，通过 SHA-256 哈希函数作用于明文图像，得到 64 个 16-进制的哈希值序列 $K_1,K_2,\cdots,K_{64}$，利用公式(9)生成 k_1,k_2,k_3,k_4，进一步通过公式(10)对

外部密钥进行修正，得到与明文相关的密钥 a,b,x_0,y_0。

$$k_i=\frac{\sum_{j=1}^{64}K_{16\times(i-1)+j}+t_0}{100},t_0=\frac{1}{64}\sum_{j=1}^{64}K_j,i=1,2,3,4, \tag{9}$$

$$\begin{cases}a=a+k_1,\\ b=b+k_2,\\ x_0=\mathrm{mod}\left(x_0+k_3,1\right),\\ y_0=\mathrm{mod}\left(y_0+k_4,1\right).\end{cases} \tag{10}$$

Step 4. 用混沌映射(8)生成混沌序列 $\{x_k,y_k:k=0,1,\cdots,T,\cdots,L+T-1\}$，用于控制加密算法的伪随机灰度值序列和 DNA 序列，参与灰度值的扩散过程。扔掉前面 T 个值，将剩余 L 个值构成的向量记为 $X=\{x_T,...,x_{L+T-1}\},Y=\{y_T,...,y_{L+T-1}\}$。通过公式(11)量化 X,Y 为伪随机灰度值序列得到序列 $X1,Y1$，再将序列 $X1,V2$ 进行比特异或操作得到序列 $V3$：$V3=\mathrm{bitxor}\left(X1,V2\right)$。

$$X1=\mathrm{mod}\left(floor\left(X\times10^{14}\right),256\right),Y1=\mathrm{mod}\left(floor\left(Y\times10^{14}\right),256\right) \tag{11}$$

Step 5. 通过公式(12)对混沌序列 X,Y 进行预处理得到 DNA 运算规则序列 E，长度为 $4L$：

$$\begin{cases}E\left(1:L\right)=\mathrm{mod}\left(floor\left(X\left(1:L\right)\times10^{12}\right),4\right)+1,\\ E\left(L+1:2L\right)=\mathrm{mod}\left(floor\left(Y\left(1:L\right)\times10^{12}\right),4\right)+1,\\ E\left(2L+1:3L\right)=\mathrm{mod}\left(floor\left(X\left(1:L\right)\times10^{10}\right),4\right)+1,\\ E\left(3+1:4L\right)=\mathrm{mod}\left(floor\left(Y\left(1:L\right)\times10^{10}\right),4\right)+1.\end{cases} \tag{12}$$

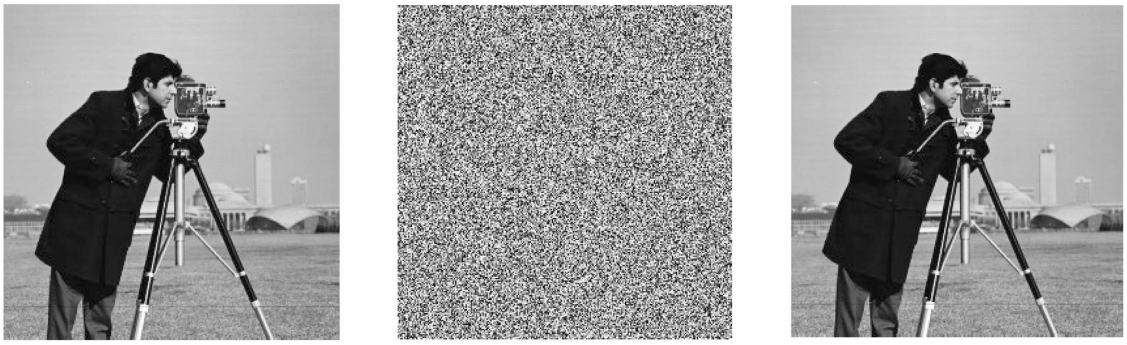
Step 6. 使用 DNA 编码规则 1 对 $V3$ 进行编码，得到 MN 行 4 列的 DNA 编码矩阵 $V4$，并按列优先原则重新转化为 $4M$ 行 N 列的编码矩阵 $P1$。将密钥流 $Y1$ 作相同的 DNA 编码，得到 $4M$ 行 N 列的编码矩阵 $Y2$。将向量 E 重新排列成 $4M$ 行 N 列的矩阵 $E1$，由 DNA 运算规则和公式(13)对编码矩阵 $P1$ 和 $Y2$ 实施动态 DNA 运算，得到 DNA 矩阵 Q。

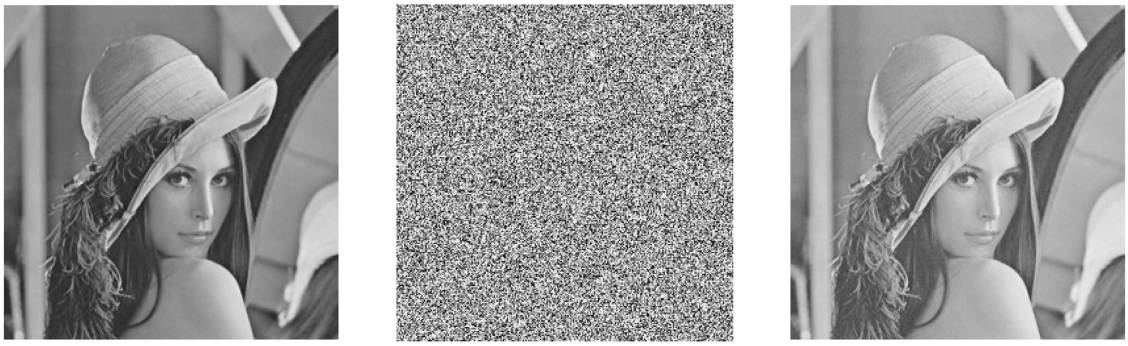
$$\begin{cases}Q\left(1,1\right)=P1\left(1,1\right)\Delta_{E1(1,1)}Y2\left(1,1\right),\\ Q\left(1,j\right)=P1\left(1,j\right)\Delta_{E1(1,j)}Y2\left(1,j\right)\Delta_{E1(1,j)}Q\left(1,j-1\right),j=2:N,\\ Q\left(i,1\right)=P1\left(i,1\right)\Delta_{E1(i,1)}Y2\left(i,1\right)\Delta_{E1(i,1)}Q\left(i-1,1\right),i=2:4M,\\ Q\left(i,j\right)=P1\left(i,j\right)\Delta_{E1(i,1)}Y2\left(i,j\right)\Delta_{E1(i,1)}Q\left(i,j-1\right),j=2:M,i=2:4M.\end{cases} \tag{13}$$

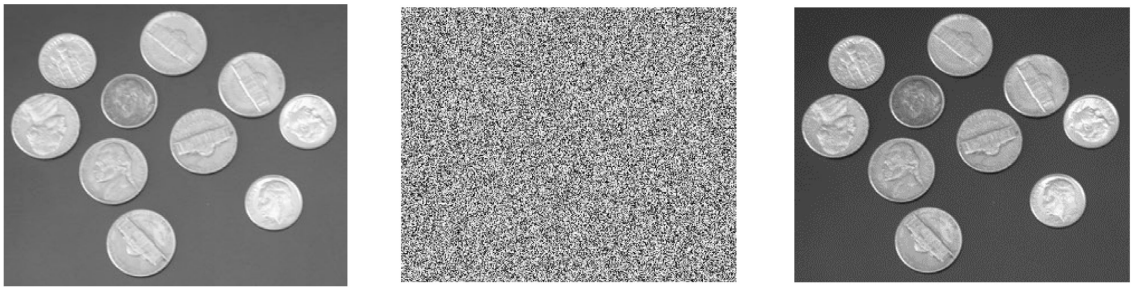
Step 7. 将 DNA 编码矩阵 Q 重新排列为 MN 行 4 列的矩阵 $Q1$，用 DNA 解码规则 3 进行解码，然后每 4 碱基合并转化为 0~255 之间的 10-进制数，得到 MN 列的向量 $Q2$，最后按列优先原则转化为 M 行 N 列的密文图像 C。

4. 仿真结果与性能分析

实验使用的计算机配置为 Windows 11，在 MATLAB R2023a 平台上进行图像加密算法的仿真实验。选取灰度等长图像 Lena、Bridge、Cameraman，及非等长图像 Tire、Pout、Coins 作为明文图像，解密和解密结果如图 3 所示。明文图像如图 3(a)~(d)，密文图像如图 3(e)~(h)，解密图像如图 3(i)~(l)，经验证，解密图像与明文图像完全一致，可知加密后的图像均类似随机噪声，较好地隐藏了明文图像的信息，加密效果良好，算法无失真解密。


(a) cameraman 原图像 (e) cameraman 加密图像 (i) cameraman 解密图像


(b) Lena 原图像 (f) Lena 加密图像 (j) Lena 解密图像


(c) coins 原图像 (g) coins 加密图像 (k) coins 解密图像

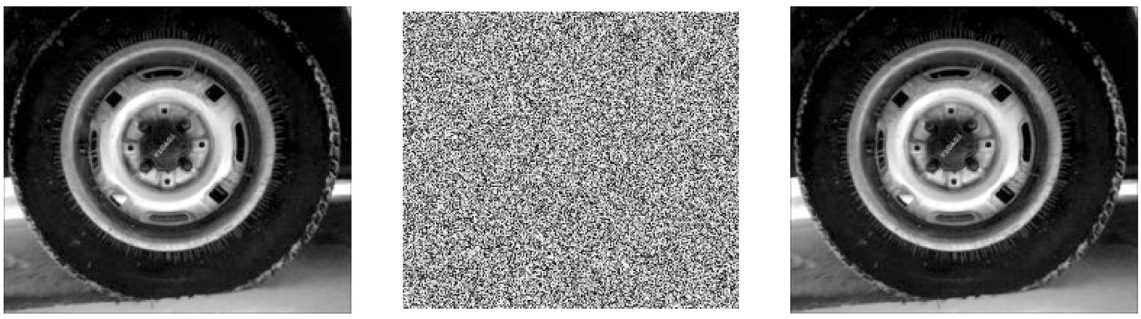
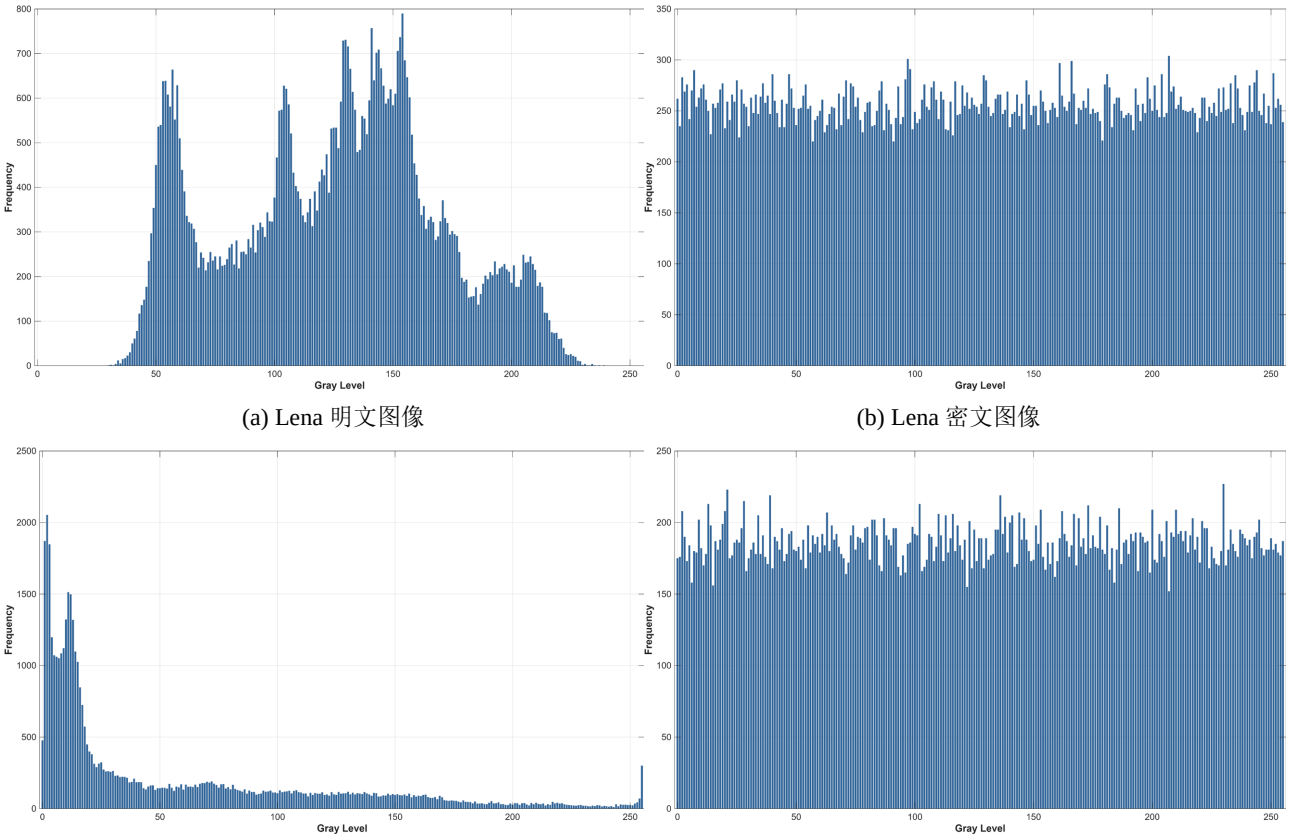

(d) tire 原图像 (h) tire 加密图像 (l) tire 解密图像

Figure 3. The simulation experiment results
图 3. 仿真实验结果

4.1. 直方图分析

直方图是图像中每个灰度级(通常为 0~255)的像素数量统计图，用于反映图像中灰度值的分布特征。

当直方图分布趋于均匀时，图像灰度信息的统计特征更加随机，不确定性显著增加，从而能够有效抵御基于直方图的统计分析攻击。图 4 中展示了 Lena 与 Tire 在加密前后直方图分布。在图中可以清晰地观察到，Lena 和 Tire 的明文图像灰度值分布波动较大，具有明显的集中峰谷特征；而密文图像的灰度值分布则较为均匀，直方图曲线整体趋于平坦。这一对比表明，该加密方案生成的密文图像灰度直方图更加均匀，能有效地掩盖原始图像的统计特征，从而更好地保护图像信息的安全。为进一步定量刻画明文图像与密文图像在统计分布上的差异，本文采用 Pearson χ^2 检验对两者的差别进行数值上的分析。



(a) Lena 明文图像　(b) Lena 密文图像

(c) Tire 明文图像　(d) Tire 密文图像

Figure 4. Histograms
图 4. 直方图

卡方值是定量评估图像灰度分布均匀性与随机性的指标，可用于验证加密算法对明文统计特性的破坏程度。理想的加密算法所得的密文图像应呈现均匀的灰度分布特征，通过计算卡方值可定量衡量密文图像对明文原始统计规律的破坏程度。设定检验显著性水平 $\alpha = 0.05$，作原假设 H_0：图像灰度级(0~255)的实际分布符合均匀分布；备择假设 H_1：图像灰度级(0~255)的实际分布不符合均匀分布。若计算得到的卡方值小于临界值 $\chi^2_{0.05}255 = 293.247$，则接受原假设，认为图像灰度分布符合均匀分布；反之则拒绝原假设[20]。

对明文图像进行加密，生成对应的密文图像，分别统计明文与密文图像中各灰度级 0~255 的实际出现频数 $p_0, p_1, \cdots, p_{255}$，以均匀分布下的理论频数 e 为基准，按照公式(14)计算的卡方值 χ^2。

$$e = \frac{M \times N}{256}, \chi^2 = \sum_{i=0}^{255} \frac{(p_i - e)^2}{e}. \tag{14}$$

由测试图像的明文图像与密文图像卡方值对比表 4 可知，6 幅测试图像的明文卡方值均处于 10^4~10^6 量级，远高于临界值 $\chi^2_{0.05}255=293.247$，反映出明文图像灰度分布具有明显的的非均匀性。而加密后的密文图像卡方值稳定在 230~260 区间，均小于临界值 $\chi^2_{0.05}255$，因此接受原假设 H_0，即密文图像灰度分布符合均匀分布，说明本文算法能够彻底破坏明文图像的灰度统计规律，具备抗统计分析攻击能力，可有效抵御基于灰度频数分布的密码分析手段。

Table 4. Comparison of Chi-square values between plain image and cipher image
表 4. 明文与密文图像卡方值对比

		Lena	Bridge	Cameraman	Tire	Pout	Coins
卡方值	明文图像	4.9144e+04	1.1856e+06	1.3752e+05	1.3752e+05	3.3687e+05	3.4804e+05
	密文图像	256.1016	236.9238	230.8616	230.8616	259.5959	230.0245

4.2. 相关系数分析

图像抵御统计攻击能力与相邻像素值相关性成反比，即相邻像素值相关性越小，加密算法抗统计攻击能力越强。明文图像在水平、垂直、正对角和反对角方向上的相邻像素灰度值通常存在强相关性，相关系数绝对值接近 1；理想的加密算法通过置乱、扩散等操作使密文图像相邻像素呈现伪随机性，相关系数近似于 0。相关系数的计算见公式(15)：

$$\begin{cases} r=\dfrac{Cov(x,y)}{\sigma_x\sigma_y}, \\ Cov(x,y)=\dfrac{1}{T}\sum_{i=1}^{T}(x_i-u_x)(y_i-u_y), \\ u_x=\dfrac{1}{T}\sum_{i=1}^{T}x_i, u_y=\dfrac{1}{T}\sum_{i=1}^{T}y_i, \\ \sigma_x=\sqrt{\dfrac{1}{T}\sum_{i=1}^{T}(x_i-u_x)^2}, \sigma_y=\sqrt{\dfrac{1}{T}\sum_{i=1}^{T}(y_i-u_y)^2}. \end{cases} \tag{15}$$

其中 $x=(x_1,\cdots,x_T), y=(y_1,\cdots,y_T)$ 表示相邻位置的像素值，r 为相邻位置像素的相关性系数，T 表示相邻位置像素对的数目，u_x, u_y 分别为 x 和 y 的均值。

Table 5. Correlation coefficients of adjacent pixels from plain images and cipher images
表 5. 明文图像和密文图像的相邻像素相关系数

图像相关系数		水平	垂直	对角	反对角
Lena	明文图像	0.9716	0.9410	0.9182	0.9446
	密文图像	−0.0215	−0.0003	0.0070	0.0029
Bridge	明文图像	0.9324	0.9419	0.9007	0.9023
	密文图像	0.0066	0.0005	0.0044	−0.0315
Cameraman	明文图像	0.9590	0.9380	0.9189	0.9187
	密文图像	0.0252	0.02919	0.0170	0.0077

以 Lena、Bridge、Cameraman 图像为例，为避免样本偏差，在图像有效区域随机生成 5000 个不重复的像素点，以每个像素点为中心取其右方 $(x+1,y)$、下方 $(x,y+1)$、右下方 $(x+1,y+1)$、右上方 $(x+1,y-1)$

的像素点，作为水平、垂直、对角、反对角四个方向的相邻像素；将随即像素点的灰度值作为数据集 X，各方向相邻像素灰度值依次作为数据集 Y，相关系数。根据表 5 的实验数据对比分析可知，原始明文图像在水平、垂直及对角方向上的相关系数趋近 1，相邻像素间均呈现出显著的相关性特征。密文图像在相应方向的相关系数均近似理想值 0。这一结果表明，该加密算法能削弱图像相邻像素相关性，有效增强抗统计攻击能力。

4.3. 信息熵分析

信息熵用于衡量图像信息的不确定性，熵值越大，图像像素灰度值分布越均匀，即加密算法抗统计攻击能力更强，其计算见公式(16)：

$$H = -\sum_{i=0}^{L-1} p_i \log_2 p_i \tag{16}$$

其中 p_i 表示灰度图像中灰度值 i 出现的概率，图像的灰度级数为 $L = 256$，信息熵的最大值为 8。表 6 显示图像加密前后的信息熵值，密文图像的信息熵皆接近于 8，表示密文图像的像素混乱程度已接近极限值，本文加密算法能有效抵御信息熵的统计攻击。

Table 6. Information entropies of plain images and cipher images
表 6. 明文图像和密文图像的信息熵

指标		Lena	Bridge	Cameraman	Tire	Pout	Coins
信息熵	明文图像	7.3497	5.7055	6.9265	5.7598	7.0097	7.0097
	密文图像	7.9971	7.9993	7.9965	7.9973	7.9973	7.9973

为方便将本文算法与现有文献进行比较，采用大小为 256 × 256 的 Lena 图像进行对比实验，其结果如表 7 所示。实验结果表明，本文算法的信息熵为 7.9971，与文献[21]-[27]相比，信息熵更接近于理想信息熵值 8。因此，本文提出的算法在抵御统计攻击方面具有更优越的性能。

Table 7. Comparison of information entropy among different algorithms
表 7. 不同算法信息熵对比

算法	本文算法	文献[21]	文献[22]	文献[23]	文献[24]	文献[25]	文献[26]	文献[27]
信息熵	7.9971	7.9970	7.9971	7.9967	7.9969	7.9655	7.9935	7.9896

4.4. 密钥敏感性

密钥敏感性是衡量图像加密算法抵御密钥篡改、暴力穷举等攻击的核心指标，要求密钥的微小扰动能引发密文图像的剧烈变化，体现混沌系统与加密流程对密钥的高度依赖。为验证密钥敏感性，设计如下实验：用密钥 KEY1 以及 KEY1 的微小扰动(本文用 10^{-14})生成 KEY2 分别加密明文图像得到密文图像 C_1 和 C_2，通过像素变化率(NPCR)和归一化平均像素变化强度(UACI)定量评估两组密文图像的差异，NPCR 和 UACI 的计算见公式(17)~(18)，256 级灰度图像的 NPCR 和 UACI 的理论最优值分别为 99.6094%，33.4635% [28]。

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N}, D(i,j) = \begin{cases} 0, C_1(i,j) = C_2(i,j), \\ 1, C_1(i,j) \neq C_2(i,j), \end{cases} \tag{17}$$

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|C_1(i,j)-C_2(i,j)\right|. \tag{18}$$

其中 $C_1(i,j)$ 和 $C_2(i,j)$ 分别表示使用两个微小差异密钥加密后的密文图像在像素 (i,j) 的灰度值。

由表 8 知，6 幅测试图像的密钥敏感性指标 NPCR 值在 99.5865%~99.6398%之间，UACI 值在 33.2722%~33.6498%之间，均与 256 级灰度图像的理论最优值高度吻合，不同图像间指标波动极小，加密算法具有很强的密钥敏感性，可有效地抵御蛮力攻击。

Table 8. The Values of NPCR and UACI for key sensitivity test
表 8. 密钥敏感性测试的 NPCR 与 UACI 值

密钥	指标	Lena	Bridge	Cameraman	Tire	Pout	Coins	理论值
a	NPCR	99.6368	99.6063	99.6170	99.6110	99.5947	99.6016	99.6094
	UACI	33.4280	33.4502	33.4829	33.3922	33.4885	33.3514	33.4635
b	NPCR	99.6200	99.6257	99.6032	99.6215	99.6248	99.6463	99.6094
	UACI	33.5630	33.4847	33.4828	33.4299	33.4859	33.4474	33.4635
x_0	NPCR	99.6398	99.6200	99.5925	99.6215	99.6162	99.6097	99.6094
	UACI	33.6213	33.4528	33.5373	33.3859	33.4781	33.3394	33.4635
y_0	NPCR	99.5758	99.5868	99.6017	99.6257	99.6033	99.6341	99.6094
	UACI	33.5540	33.4170	33.3853	33.6498	33.3446	33.2722	33.4635

4.5. 明文敏感性分析(抗差分攻击)

明文敏感性是图像加密算法抵御差分攻击的核心性能，要求明文图像的微小像素变化能引发密文图像的剧烈全局变化。本文通过单像素灰度值扰动的方式验证算法明文敏感性：随机选取明文图像的像素，灰度值非 255 时加 1，为 255 时减 1，对单一像素改变前后的两幅明文图像分别加密得到密文 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$，通过对比 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 的差异性能指标 NPCR，UACI 来刻画算法性能。实验选取 Lena，Bridge，Cameraman，Tire，Pout，Coins 为测试图像，对每幅图像独立开展 50 次明文敏感性测试，计算 50 次测试的 NPCR 和 UACI 结果，并取平均值。

由表 9 可知，6 幅测试图像的 NPCR 平均值均在 99.6050%~99.6163%之间，UACI 平均值均在 33.4504%~33.5038%之间，均与 256 级灰度图像的理论最优值(NPCR: 99.6094%, UACI: 33.4635%)高度吻合，且不同图像间指标波动极小，性能稳定。本文算法具有极强的明文敏感性，能有效抵御差分攻击，满足图像加密的安全要求。

Table 9. Average values of NPCR and UACI for plaintext sensitivity test
表 9. 明文敏感性测试的 NPCR 与 UACI 平均值

指标	Lena	Bridge	Cameraman	Tire	Pout	Coins
NPCR	99.6158	99.6096	99.6138	99.6163	99.6137	99.6050
UACI	33.5038	33.4563	33.5020	33.4504	33.4885	33.4581

为方便将本文算法与已有文献进行比较，取大小为 256 × 256 的 Lena 图像进行对比实验，其结果如表 10 所示。实验结果表明，本文算法的 NPCR 和 UACI 值分别为 99.6158%，33.5038%，比文献[29]-[31]更接近于理想值 99.6094%和 33.4635%。因此，本文提出的算法在抵御差分攻击方面具有更优越的性能。

Table 10. NPCR and UACI comparison among different algorithms
表 10. 不同算法的 NPCR 和 UACI 对比

算法	本文算法	文献[29]	文献[30]	文献[31]
NPCR	99.6158	99.3700	99.4100	99.6200
UACI	33.5038	31.8500	33.5700	33.4000

5. 结束语

本文结合二维 Arnold 混沌映射，Moore 扫描曲线与动态 DNA 运算规则，提出了一种新型灰度图像加密算法。该算法利用明文 SHA-256 哈希值对 Arnold 映射参数与初始值进行动态修正，使得密钥与明文高度相关，具有极强的密钥敏感性与明文敏感性，可有效抵御选择明文、已知明文与差分攻击。算法采用 Moore 扫描曲线完成自适应像素置乱，打破图像空间相关性，很好地隐藏了明文像素的空间位置信息。为进一步提升密文图像抵御统计攻击的安全性，算法在置乱后引入动态 DNA 编码与多规则 DNA 运算，配合混沌序列完成深度扩散。结果表明，本文所设计的加密算法具有优良的统计特性与安全性能，能够抵御统计分析攻击、暴力攻击、差分攻击与明文攻击等。

基金项目

论文研究资助项目为广东省大学生创新创业项目，广东省基础与应用基础研究基金项目(No. 2023A1515030199)以及广东省教育厅普通高校重点科研项目(2025ZDZX2020)。

参考文献

[1] Schneier, B. (1995) Cryptography: Theory and Practice. CRC Press.

[2] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **8**, 1259-1284. https://doi.org/10.1142/s021812749800098x

[3] Wong, K., Kwok, B.S. and Law, W. (2008) A Fast Image Encryption Scheme Based on Chaotic Standard Map. *Physics Letters A*, **372**, 2645-2652. https://doi.org/10.1016/j.physleta.2007.12.026

[4] Ye, R. (2011) A Novel Chaos-Based Image Encryption Scheme with an Efficient Permutation-Diffusion Mechanism. *Optics Communications*, **284**, 5290-5298. https://doi.org/10.1016/j.optcom.2011.07.070

[5] Ye, R. (2014) A Novel Image Encryption Scheme Based on Generalized Multi-Sawtooth Maps. *Fundamenta Informaticae*, **133**, 87-104. https://doi.org/10.3233/fi-2014-1063

[6] Wang, X. and Chen, X. (2021) An Image Encryption Algorithm Based on Dynamic Row Scrambling and Zigzag Transformation. *Chaos, Solitons & Fractals*, **147**, Article 110962. https://doi.org/10.1016/j.chaos.2021.110962

[7] 牛莹, 张勋才. 基于填充曲线和相邻像素比特置乱的图像加密方法[J]. 电子与信息学报, 2022, 44(3): 1137-1146.

[8] 冯炽, 叶桦. 基于改进 Zigzag 变换与混沌序列相结合的数字图像加密算法[J]. 计算机科学与应用, 2017, 7(6): 554-561.

[9] Wang, Q., Zhang, X. and Zhao, X. (2022) Image Encryption Algorithm Based on Improved Zigzag Transformation and Quaternary DNA Coding. *Journal of Information Security and Applications*, **70**, Article 103340. https://doi.org/10.1016/j.jisa.2022.103340

[10] 王笋, 徐小双. Hilbert 曲线扫描矩阵的生成算法及其 MATLAB 程序代码[J]. 中国图象图形学报, 2006, 11(1): 119-122.

[11] Suresh, V. and Madhavan, C. (2012) Image Encryption with Space-Filling Curves. *Defence Science Journal*, **62**, 46-50. https://doi.org/10.14429/dsj.62.1441

[12] 贾连印, 范瑶, 丁家满, 李晓武, 游进国. 高效前缀约简的三维 Hilbert 空间填充曲线编解码算法[J]. 电子与信息学报, 2024, 46(2): 633-642.

[13] Ye, R. and Liu, L. (2015) A Matrix Iterative Approach to Systematically Generate Hilbert-Type Space-Filling Curves. *International Journal of Computers & Technology*, **14**, 6281-6294. https://doi.org/10.24297/ijct.v14i12.1741

[14] 张勋才, 刘奕杉, 崔光照. 基于 DNA 编码和超混沌系统的图像加密算法[J]. 计算机应用研究, 2019, 36(4): 1139-1143.

[15] 朱凯歌, 武相军, 任广龙. 基于 DNA 动态编码和混沌系统的彩色图像无损加密算法[J]. 计算机应用研究, 2020, 37(S2): 230-233.

[16] Zhang, X. and Ye, R. (2020) A Novel RGB Image Encryption Algorithm Based on DNA Sequences and Chaos. *Multimedia Tools and Applications*, **80**, 8809-8833. https://doi.org/10.1007/s11042-020-09465-6

[17] Zhang, S. and Liu, L. (2021) A Novel Image Encryption Algorithm Based on SPWLCM and DNA Coding. *Mathematics and Computers in Simulation*, **190**, 723-744. https://doi.org/10.1016/j.matcom.2021.06.012

[18] Arnold, V. and Avez, A. (1968) Ergodic Problems in Classical Mechanics. Benjamin.

[19] Watson, J.D. and Crick, F.H.C. (1953) Molecular Structure of Nucleic Acids: A Structure for Deoxyribose Nucleic Acid. *Nature*, **171**, 737-738. https://doi.org/10.1038/171737a0

[20] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社, 2016.

[21] Chen, C., Sun, K. and He, S. (2020) An Improved Image Encryption Algorithm with Finite Computing Precision. *Signal Processing*, **168**, Article 107340. https://doi.org/10.1016/j.sigpro.2019.107340

[22] Wang, X., Zhu, X. and Zhang, Y. (2018) An Image Encryption Algorithm Based on Josephus Traversing and Mixed Chaotic Map. *IEEE Access*, **6**, 23733-23746. https://doi.org/10.1109/access.2018.2805847

[23] Sun, S. (2018) A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling. *IEEE Photonics Journal*, **10**, 1-14. https://doi.org/10.1109/jphot.2018.2817550

[24] 赵耿, 李文健, 马英杰. 基于变参数的 logistic 混沌系统图像加密算法[J]. 计算机应用与软件, 2023, 40(12): 325-331.

[25] 周红亮, 刘洪娟. 结合 DNA 编码的快速混沌图像加密算法[J]. 东北大学学报(自然科学版), 2021, 42(10): 1391-1399.

[26] 孙倩, 胡苏. 基于改进 Cat 映射与混沌系统的彩色图像快速加密算法[J]. 计算机应用研究, 2017, 34(1): 233-237, 255.

[27] 谢国波, 邓华军. 二次广义 Cat 映射的混合混沌图像加密算法[J]. 计算机工程与应用, 2018, 54(15): 197-202.

[28] 叶瑞松, 陈月明. 一个迭代函数系统的分形混沌特性及其应用[J]. 汕头大学学报(自然科学版), 2023, 38(2): 3-30+2.

[29] 李付鹏, 刘敬彪, 王康泰. 基于 Tent 映射的图像加密算法及其实验研究[J]. 杭州电子科技大学学报(自然科学版), 2020, 40(3): 38-43.

[30] Liu, W., Sun, K. and Zhu, C. (2016) A Fast Image Encryption Algorithm Based on Chaotic Map. *Optics and Lasers in Engineering*, **84**, 26-36. https://doi.org/10.1016/j.optlaseng.2016.03.019

[31] Li, Y., Wang, C. and Chen, H. (2017) A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation. *Optics and Lasers in Engineering*, **90**, 238-246. https://doi.org/10.1016/j.optlaseng.2016.10.020