Artificial Intelligence and Robotics Research 人工智能与机器人研究, 2026, 15(3), 760-775
Published Online May 2026 in Hans. https://www.hanspub.org/journal/airr
https://doi.org/10.12677/airr.2026.153072

基于新型二维超混沌映射与动态DNA编码的卫星图像加密算法

徐雨豪[1]，陈初侠[1*]，邵　倩[1]，李雨霏[1]，王金杭[2]

[1]巢湖学院集成电路学院，安徽　巢湖
[2]巢湖学院电子信息工程学院，安徽　巢湖

收稿日期：2026年3月30日；录用日期：2026年4月30日；发布日期：2026年5月14日

摘　要

针对卫星遥感图像数据量大、空间相关性强且实时传输安全性要求高的特点，提出一种基于新型二维超混沌映射与动态DNA编码的加密算法。首先，构造一种具有双正李雅普诺夫指数和全区域混沌特性的新型二维超混沌指数耦合迭代映射(2D-HEICM)，并利用SHA-256生成与明文深度关联的初始密钥；其次，通过混沌序列驱动行列循环移位实现空间置乱；最后，设计一种极速动态DNA扩散策略，利用位运算和矩阵寻址实现DNA规则的动态切换与并行扩散，克服了传统DNA加密逐像素处理的效率瓶颈。实验分析表明，该算法密文信息熵逼近理论极限8，相邻像素相关系数降至10^{-2}量级。在保持极高安全强度的同时，算法处理512 × 512图像耗时仅需约0.08秒，能够满足卫星图像实时安全传输的需求。

关键词

图像加密，超混沌映射，DNA编码，卫星图像，向量化运算

Satellite Image Encryption Algorithm Based on Novel Two-Dimensional Hyperchaotic Mapping and Dynamic DNA Coding

Yuhao Xu[1], Chuxia Chen[1*], Qian Shao[1], Yufei Li[1], Jinhang Wang[2]

[1]School of Integrated Circuits, Chaohu University, Chaohu Anhui
[2]School of Electronic and Information Engineering, Chaohu University, Chaohu Anhui

[*]通讯作者。

文章引用: 徐雨豪, 陈初侠, 邵倩, 李雨霏, 王金杭. 基于新型二维超混沌映射与动态 DNA 编码的卫星图像加密算法[J]. 人工智能与机器人研究, 2026, 15(3): 760-775. DOI: 10.12677/airr.2026.153072

Received: March 30, 2026; accepted: April 30, 2026; published: May 14, 2026

Abstract

Aiming at the characteristics of large data volume, strong spatial correlation, and high real-time security requirements for satellite remote sensing images, a satellite image encryption algorithm based on a novel 2nd-order hyperchaotic map and dynamic DNA coding is proposed. Firstly, a novel 2-Dimensional Hyperchaotic Exponentially-Coupled Iterative Map (2D-HEICM) with double positive Lyapunov exponents and full-mapping chaotic properties is constructed, and an initial secret key deeply associated with the plaintext is generated using the SHA-256 algorithm. Secondly, row-column circular shifting driven by chaotic sequences is utilized to achieve spatial confusion. Finally, a high-speed dynamic DNA diffusion strategy is designed. By leveraging bit-wise operations and matrix indexing, dynamic switching of DNA rules and parallel diffusion are achieved, effectively overcoming the efficiency bottleneck of pixel-by-pixel string conversion in traditional DNA encryption schemes. Experimental analysis shows that the information entropy of the ciphertext generated by the proposed algorithm approaches the theoretical limit of 8, and the correlation coefficients between adjacent pixels are reduced to the magnitude of 10^{-2}. While maintaining extremely high security strength, the algorithm requires only approximately 0.08 seconds to encrypt a 512 × 512 image, which can well meet the real-time secure transmission requirements of satellite observation data.

Keywords

Image Encryption, Hyperchaotic Map, DNA Coding, Satellite Images, Vectorized Operations

1. 引言

随着遥感卫星技术的飞速发展，高分辨率卫星图像在军事侦察、地理测绘、气象监测等领域得到了广泛应用[1]。然而，卫星图像在无线传输过程中面临着严重的截获与篡改风险。卫星图像通常具有海量数据、强空间相关性和高冗余度的物理特性，使得传统的 DES、AES 等文本加密方案难以满足实时处理与安全性要求[2]。

混沌映射因其初值敏感性、伪随机性和非周期性，成为图像加密领域的理想工具[3]。然而，传统的一维或低维混沌映射存在密钥空间窄、动力学区间有限且易受相空间重构攻击等缺陷[4]。同时，DNA 编码技术虽具备极强的非线性和抗预测能力，但传统的 DNA 扩散过程多依赖逐像素的字符串转换，导致算法在处理大尺寸遥感图像时效率低下[5]。

针对上述问题，本文的主要贡献如下：第一，构造了一种新型的二维超混沌指数耦合迭代映射(2D-HEICM)，其最大李雅普诺夫指数显著优于现有主流映射，确保了极高的统计复杂度；第二，引入 SHA-256 哈希函数实现明文关联，增强了算法抵御差分攻击与选择明文攻击的能力；第三，提出了向量化的动态 DNA 扩散机制，通过底层位运算彻底解决了 DNA 加密的性能瓶颈。本文工作为高分辨率卫星观测数据的实时安全保护提供了有效的技术方案。

2. 新型二维超混沌映射

2.1. 系统数学模型构建

在图像加密领域，一个高性能的混沌系统是保证密文安全性的核心。针对卫星遥感图像数据量巨大、空间相关性极高的物理特性，本文设计并构造了一种新型的二维超混沌指数耦合迭代映射(2-Dimensional Hyperchaotic Exponentially-Coupled Iterative Map, 2D-HEICM)。该映射通过有机整合线性反馈扩张、高频正弦调制及指数非线性耦合机制，旨在克服传统低维混沌映射存在的密钥空间狭窄、动力学区间有限等缺陷。

本文提出的 2D-HEICM 系统的数学表达式如式(1)所示：

$$\begin{cases} x_{n+1} = \mathrm{mod}\left(a x_n + \sin\left(\dfrac{b}{x_n + \varepsilon} \right) \mathrm{e}^{x_n} + c \cdot \sin\left(\pi y_n \right), 1 \right) \\ y_{n+1} = \mathrm{mod}\left(a y_n + \sin\left(\dfrac{b}{y_n + \varepsilon} \right) \mathrm{e}^{y_n} + c \cdot \sin\left(\pi x_n \right), 1 \right) \end{cases} \tag{1}$$

其中，a, b, c 为系统的控制参数，其取值均为正实数。$x_n, y_n \in (0,1)$ 是系统在第 n 次迭代时的状态值。mod(·, 1)函数用于将系统状态限制在单位区间[0, 1]内。ε 是一个极小的正数(本文取 1×10^{-10})，用于防止分母为零，增强数值计算的稳定性。

该系统的结构设计包含以下核心逻辑：

(1) 线性反馈扩张项(ax_n, ay_n)：当控制参数 $a > 1$ 时，该项为系统提供了基础的拉伸动力，能够有效消除混沌映射中常见的周期窗口，确保系统在宽参数范围内维持混沌状态。

(2) 高频非线性振荡项($\sin\left(b/\left(x_n+\varepsilon\right)\right)\mathrm{e}^{x_n}$)：结合了分式正弦调制与指数增长特性。由于 $\sin\left(b/\left(x_n+\varepsilon\right)\right)$ 在 $x_n \to 0$ 附近具有无限密集的振荡频率，配合指数项 e^{x_n} 的非线性放大作用，使系统具备极强的初值敏感性和极高的随机性。

(3) 正弦交叉耦合项($c\sin(\pi y_n)$, $c\sin(\pi x_n)$)：实现了 x 轴与 y 轴分量之间的深度非线性耦合。通过正弦函数的调制，增强了两个变量之间的协同演化复杂度。这是该系统产生两个正的李雅普诺夫指数(具有超混沌特性)的关键因素。

此外，从非线性动力学理论的角度，可以通过雅可比矩阵进一步严谨证明该系统的混沌发散特性。2D-HEICM 系统的雅可比矩阵 J 定义为：

$$J = \begin{bmatrix} \dfrac{\partial x_{n+1}}{\partial x_n} & \dfrac{\partial x_{n+1}}{\partial y_n} \\ \dfrac{\partial y_{n+1}}{\partial x_n} & \dfrac{\partial y_{n+1}}{\partial y_n} \end{bmatrix} = \begin{bmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{bmatrix} \tag{2}$$

其中，对角线元素为：

$$J_{11} = a + \cos\left(\frac{b}{x_n + \varepsilon} \right) \cdot \left(\frac{-b}{\left(x_n + \varepsilon \right)^2} \right) \cdot \mathrm{e}^{x_n} + \sin\left(\frac{b}{x_n + \varepsilon} \right) \cdot \mathrm{e}^{x_n} \tag{3}$$

由于系统设计中包含了指数放大项 e^{x_n} 以及大于 1 的线性反馈项 a，使得矩阵 J 的迹和行列式在状态空间内迅速膨胀。根据动力学稳定性判定定理，这意味着雅可比矩阵的特征值绝对值 $|\lambda_i| \gg 1$。因此，2D-HEICM 系统在工作参数区间内的所有平衡点均是局部不稳定的。这种本质上的局部不稳定性，结合 mod(1)运算提供的全局折叠机制，从严格的数学理论层面保证了系统相空间轨道的持续拉伸与折叠，从而不可避免地演化为具有遍历性的超混沌状态。

2.2. 动力学特性分析

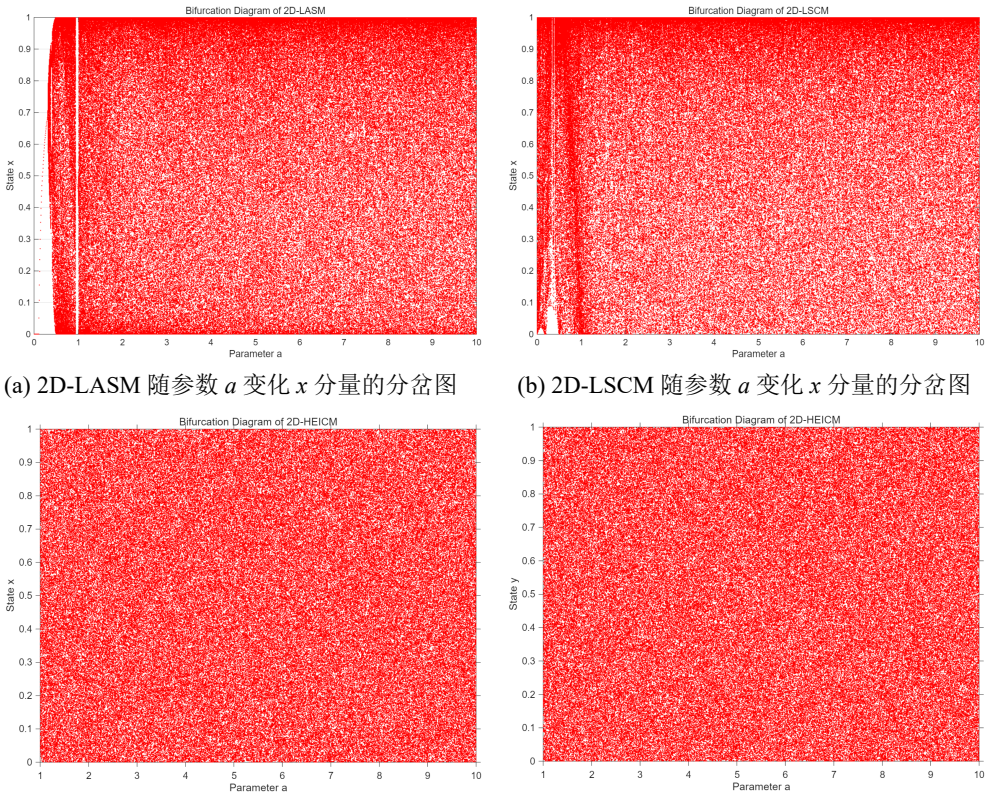
为了科学地评价本文所提出的 2D-HEICM 系统的复杂性与随机性能，本节通过数值仿真手段对其分岔特性、李雅普诺夫指数、相轨迹、相关性及初值敏感性进行深入分析。

2.2.1. 分岔图分析

分岔图能够直观地反映动力学系统随控制参数变化的演化行为，是评估混沌系统遍历性、混沌区间广度以及是否存在周期窗口的关键指标[6]。本节首先考察两种主流的二维混沌映射——2D-LASM [7]和2D-LSCM [8]的分岔特性，并将其与本文提出的 2D-HEICM 系统进行对比分析。

图 1(a)和图 1(b)分别展示了 2D-LASM 与 2D-LSCM 系统随控制参数 a 变化的分岔演化过程。可以观察到，2D-LASM 在参数 a 较小的范围内混沌特性并不稳定，且在多个参数点处存在明显的周期窗口(表现为图中的空白纵条)，这意味着系统在这些特定参数下会退化为固定点或周期轨道，极大地削弱了加密算法的安全性。2D-LSCM 虽然在混沌区间上有所改善，但在高频波动下其状态点的分布密度仍存在不均匀性，且其有效的混沌参数范围相对受限。

相比之下，图 1(c)和图 1(d)分别展示了本文提出的 2D-HEICM 系统的 x 分量与 y 分量的分岔特性。实验结果表明，在极宽的参数范围(例如 $a \in [1,10]$)内，2D-HEICM 系统的两个维度均展现出极其稳定且致密的混沌特性。状态点始终能够均匀地填充在完整的$[0, 1]$映射空间内，且未出现任何周期窗口。这说明 2D-HEICM 在两个维度上均具备完美的遍历性与满射特性。这种跨越极宽参数范围的全区域混沌分布，不仅为卫星图像加密提供了更广阔的密钥选择空间，也使得算法能够有效抵抗基于相空间重构的参数识别攻击。



(a) 2D-LASM 随参数 a 变化 x 分量的分岔图　(b) 2D-LSCM 随参数 a 变化 x 分量的分岔图

(c) 2D-HEICM 随参数 a 变化 x 分量的分岔图　(d) 2D-HEICM 随参数 a 变化 y 分量的分岔图

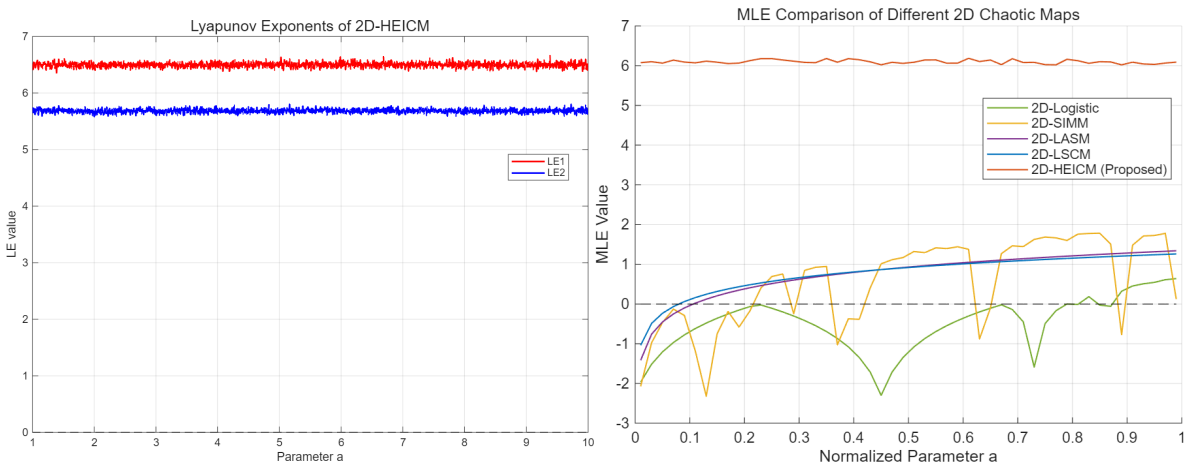
Figure 1. Comparison of bifurcation diagrams of the 2D-HEICM system with other systems
图 1. 2D-HEICM 系统与其他系统的分岔图对比

2.2.2. 李雅普诺夫指数分析

李雅普诺夫指数(Lyapunov Exponents, LE)通过量化相空间中轨道分离的指数速率，是评估动力系统混沌特性与安全强度的核心指标[9]。对于二维离散系统，若存在两个正的李雅普诺夫指数(即 LE1 > 0，LE2 > 0)，则该系统处于超混沌状态，具备比普通混沌更复杂的动力学行为和更强的抗预测能力。

图 2(a)展示了提出的 2D-HEICM 系统在参数 $a \in [1,10]$ 范围内的 LE 演化特性。实验结果显示，该系统的两个李雅普诺夫指数 LE1 和 LE2 在整个测试区间内均稳定地保持在零轴上方。具体而言，LE1 始终维持在 6.5 左右，而 LE2 也保持在 5.5 以上。这种“双高位正指数”特征不仅严谨地证明了系统的超混沌属性，更反映出其相空间轨道具有极速的指数级分离特性，能够产生极高质量的伪随机序列。

为进一步量化算法的先进性，图 2(b)将 2D-HEICM 的最大李雅普诺夫指数(Maximum Lyapunov Exponent, MLE)与经典及近年高性能映射进行了横向对比。可见，传统 2D-Logistic [10]与 2D-SIMM [11]映射的 MLE 指数较低且波动剧烈；2D-LASM 与 2D-LSCM 映射虽然具备较好的混沌性能，但其 MLE 值通常在 2.0 以下。相比之下，本文提出的 2D-HEICM 展现出了压倒性的性能优势，其 MLE 指数约为对比映射的 3 至 4 倍。这种卓越的动力学复杂度为卫星图像的安全加密提供了坚实的物理基础。



(a) 2D-HEICM 系统随参数 a 变化的李雅普诺夫指数　(b) 五种二维混沌映射的最大李雅普诺夫指数横向对比

Figure 2. Lyapunov exponents analysis and complexity comparison of the 2D-HEICM system
图 2. 2D-HEICM 系统的李雅普诺夫指数分析及其复杂度对比

2.2.3. 统计特性验证

为进一步验证 2D-HEICM 系统的伪随机性能与遍历性，本节对其相轨迹、相关特性及初值敏感性进行统计测试。

首先，图 3 展示了系统的二维相轨迹图。可见，系统状态点均匀、致密地填满了整个$[0, 1] \times [0, 1]$平面，不存在任何明显的拓扑空洞或确定性的吸引子。这证明了该系统具备卓越的遍历性与满射特性，能够确保生成的加密序列在统计上高度均匀。

其次，图 4 给出了混沌序列的自相关分析结果。实验表明，序列的自相关系数仅在延迟 $k=0$ 时呈现为 1，在其他偏移位置均迅速跌落至 0 附近波动。这种类脉冲 δ 的自相关特性表明序列各元素间具有极强独立性，证明了 2D-HEICM 序列具有极高的不确定性与类噪声特征。

最后，图 5 测试了系统的初值敏感性。当初始值存在仅为 10^{-15} 的极微小扰动时，两条混沌轨道在经过短暂的演化后迅速发生剧烈偏离。这种显著的“蝴蝶效应”确保了算法具备极大的有效密钥空间，能够从物理层面彻底免疫穷举攻击与非线性预测攻击。

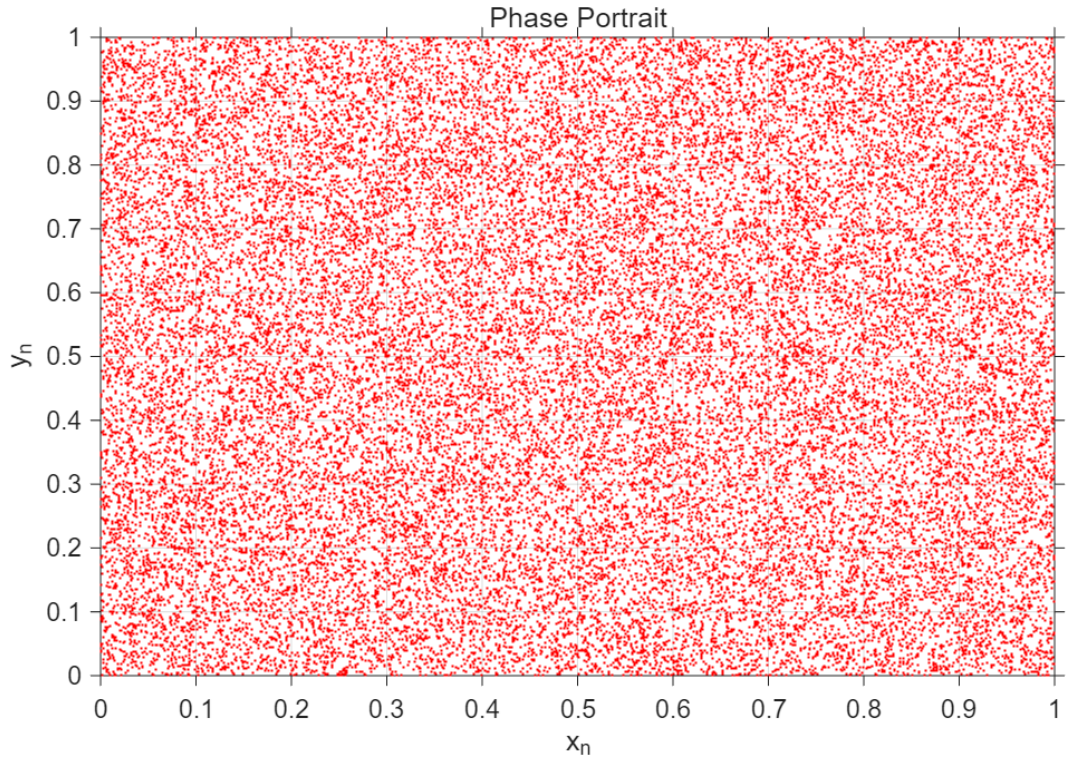


Figure 3. The two-dimensional phase trajectory diagram of the 2D-HEICM system
图 3. 2D-HEICM 系统的二维相轨迹图

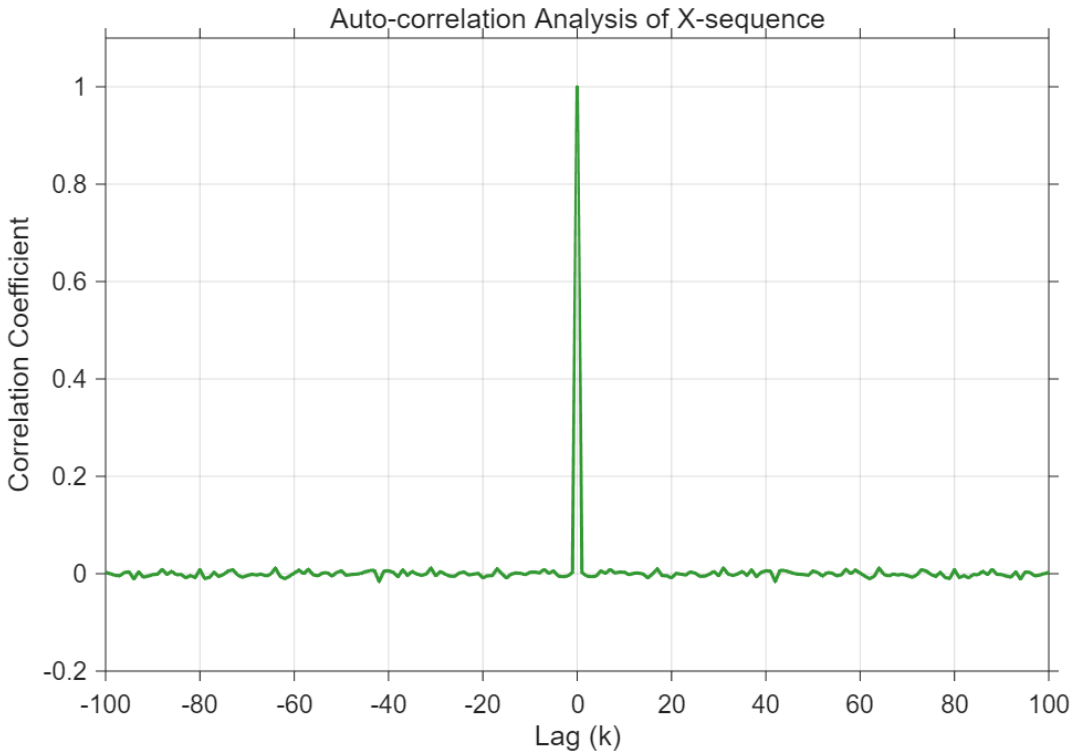


Figure 4. The autocorrelation analysis results of the 2D-HEICM system
图 4. 2D-HEICM 系统的自相关分析结果

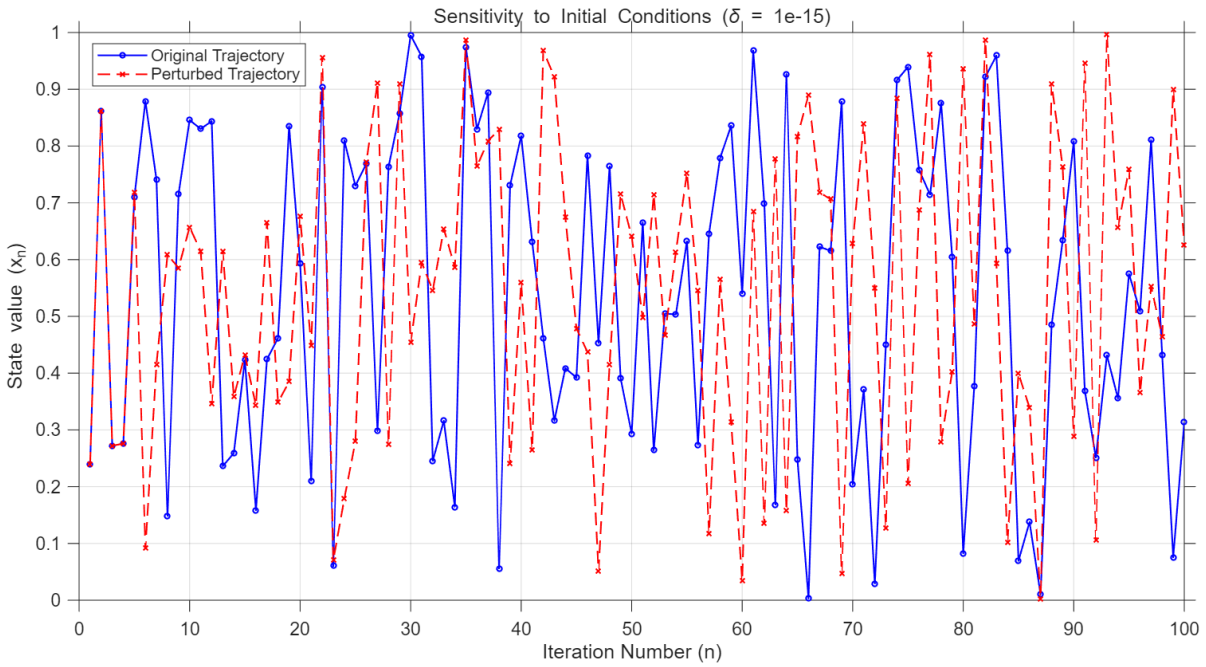


Figure 5. Initial value sensitivity test of the 2D-HEICM system
图 5. 2D-HEICM 系统的初值敏感性测试

3. 提出的卫星图像加密算法

针对卫星图像数据量巨大且空间相关性极强的特点，本章设计并实现了一种结合明文哈希关联、行列置乱及动态 DNA 扩散的对称加密方案。该算法通过多层级的混淆与扩散机制，旨在提供卓越的安全强度与实时处理性能。

3.1. 密钥生成与明文关联

根据柯克霍夫原则，密码系统的安全性应完全依赖于密钥的复杂性。为了使加密系统能够有效抵抗已知明文攻击和选择明文攻击，本文引入了 SHA-256 (Secure Hash Algorithm 256)算法。通过将明文图像的特征信息与混沌系统的初始状态进行深度绑定，实现了“一图一密”的安全特性。具体的密钥生成与数值映射逻辑如下：

步骤 1：明文指纹提取

设输入的原始灰度卫星图像为 P，其尺寸为 $M \times N$。首先将图像像素矩阵按行优先顺序转化为一维字节流，并利用 SHA-256 算法计算其哈希值 H。该哈希值是一个长度为 256 位的二进制序列，在计算逻辑中通常表示为由 64 个十六进制字符组成的字符串：

$$H = \{k_1, k_2, k_3, \cdots, k_{64}\}, \quad k_i \in \{0,1,\cdots,9,\mathrm{A},\cdots,\mathrm{F}\} \tag{4}$$

其中，k_i 代表哈希字符串中的第 i 个十六进制字符。基于 SHA-256 的雪崩效应，原始图像中哪怕仅有一个 bit 的改变，都会导致这 64 个字符发生剧烈变化。

步骤 2：哈希序列的数值转换与归一化

为了将哈希字符串 H 转化为混沌系统的连续控制变量，将其均匀切分为 8 个子块，每个子块包含 8 个十六进制字符。定义第 i 个子块对应的归一化十进制数值为 h_i，其计算公式为：

$$h_i = \frac{\mathrm{hex2dec}\left(k_{8i-7}k_{8i-6}\cdots k_{8i}\right)}{2^{32}}, \quad i = 1,2,\cdots,8 \tag{5}$$

在该式中，hex2dec ( )函数用于执行十六进制字符串到十进制数值的转换。由于 8 位十六进制数的最大值为 $2^{32}-1$，通过除以 2^{32} 进行归一化运算，每一个分量 h_i 均被精确映射到半开区间[0, 1)内。

步骤 3：混沌系统初值与控制参数的计算

利用得到的归一化数值序列 $\{h_1,h_2,\cdots,h_8\}$，通过线性映射方法生成 2D-HEICM 系统的初始迭代状态变量(x_0, y_0)及三个核心控制参数 a, b, c。计算公式如下：

$$\begin{cases} x_0=(h_1+h_2+h_3)\bmod 1 \\ y_0=(h_4+h_5+h_6)\bmod 1 \\ a=a_{\min}+(h_1\times 10^{10})\bmod(a_{\max}-a_{\min}) \\ b=b_{\min}+(h_4\times 10^{10})\bmod(b_{\max}-b_{\min}) \\ c=c_{\min}+(h_7\times 10^{10})\bmod(c_{\max}-c_{\min}) \end{cases} \tag{6}$$

式中，mod 表示取余运算。为了确保 2D-HEICM 系统在加密过程中始终运行在高性能的超混沌区域，本文设定参数的映射取值范围为：$a\in[2,5]$，$b\in[50,100]$，$c\in[10,20]$。

通过上述精密设计的密钥生成机制，每一张待加密的卫星图像都会生成一组与之内容深度绑定的专属混沌演化轨迹。这种设计从算法底层确保了极高的密钥敏感性和抗差分攻击能力。

3.2. 图像行列置乱设计

卫星图像通常包含大面积的相似地形(如海洋、森林等)，导致相邻像素间存在极高的空间相关性。置乱阶段的核心目标是打破这种空间强相关性。传统的基于 Arnold 映射或全局排序的置乱算法在处理高分辨率卫星图像时，往往面临周期性缺陷或时间复杂度过高的问题[12]。为此，本文设计了一种基于 2D-HEICM 混沌序列驱动的行列循环移位置乱方案，在保证打乱效果的同时，大幅提升了置乱效率。

具体置乱流程如下：

步骤 1：混沌序列的预处理与截取

利用 3.1 节生成的初始密钥(x_0, y_0, a, b, c)作为 2D-HEICM 系统的初始条件，迭代生成两条长度为 $L=M+N+N_0$ 的混沌实数序列 X 和 Y。为消除系统初始的瞬态效应，增强序列的伪随机性，首先舍弃前 N_0(本文取 $N_0=1000$)个迭代值。随后，从序列 X 中截取前 M 个元素构成行控制序列 S_R，从序列 Y 中截取前 N 个元素构成列控制序列 S_C：

$$\begin{cases} S_R(i)=X(i+N_0), & i=1,2,\cdots,M \\ S_C(j)=Y(j+N_0), & j=1,2,\cdots,N \end{cases} \tag{7}$$

步骤 2：行循环移位

将连续的混沌序列 S_R 映射为整数步长向量 V_R，用于控制图像每一行的位移量。第 i 行的循环移位步长 v_{ri} 计算如下：

$$v_{ri}=\left\lfloor S_R(i)\times 10^{14}\right\rfloor \bmod N \tag{8}$$

式中，$\lfloor\ \rfloor$表示向下取整函数，10^{14} 用于提取双精度浮点数的小数部分以放大混沌扰动。设原始明文图像为 P，经过行移位后的中间图像矩阵记为 P'，则其位移规则可表示为：

$$P'(i,:)=\mathrm{CircShift}(P(i,:),v_{ri}),\quad i=1,2,\cdots,M \tag{9}$$

其中，CircShift(·, v_{ri})表示将一维行向量向右循环移动 v_{ri} 个位置。

步骤 3：列循环移位

同理，将混沌序列 S_C 映射为整数步长向量 V_C。第 j 列的循环移位步长 v_{cj} 计算如下：

$$v_{cj} = \left\lfloor S_C(j) \times 10^{14} \right\rfloor \bmod M \tag{10}$$

在中间图像 P'的基础上，对其每一列进行向下循环移位操作，得到最终的置乱图像矩阵 P''：

$$P''(:, j) = \mathrm{CircShift}\left(P'(:, j), v_{cj}\right), \quad j = 1, 2, \cdots, N \tag{11}$$

该操作表示将一维列向量向下循环移动 v_{cj} 个位置。

经过上述基于超混沌序列的正交双向循环移位，原始卫星图像中像素的绝对坐标被完全打乱。相比于像素级的全局索引排序，该行列置乱方案仅需进行 $M + N$ 次移位操作，极大地降低了算法的时间复杂度，非常适用于处理对实时性要求较高的大尺度卫星观测数据。

3.3. 极速动态 DNA 扩散设计

置乱层虽然有效打破了像素间的空间相关性，但并未改变图像的直方图统计分布。为了抵御统计分析攻击，必须引入扩散机制，使得明文的微小改变能够迅速“雪崩”至全局。传统的 DNA 图像加密算法通常采用全局单一的编码规则，且依赖逐像素的字符串转换，在处理海量数据的卫星图像时存在安全性不足与时间复杂度过高的双重瓶颈。为此，本文提出了一种基于位运算的极速动态 DNA 扩散策略。

3.3.1. DNA 编码与运算规则

在生物学中，DNA 序列由腺嘌呤(A)、胞嘧啶(C)、鸟嘌呤(G)和胸腺嘧啶(T)四种碱基组成，且遵循 A 与 T 配对、C 与 G 配对的互补原则[6]。在灰度图像中，每个像素值范围为 0~255，可表示为 8 位的二进制序列。若将 2 位二进制数(00, 01, 10, 11)映射为一个 DNA 碱基，则满足互补配对原则的合法编码规则共有 8 种，如表 1 所示。

Table 1. Eight legal DNA coding rules
表 1. 8 种合法的 DNA 编码规则

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

类似于二进制的布尔运算，DNA 碱基之间也可以定义代数运算。本文选用能够有效改变像素值的 DNA 异或(XOR, ⊕)运算，其运算规则如表 2 所示。

Table 2. The rules of DNA XOR (⊕) operation
表 2. DNA 异或(⊕)运算规则

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

3.3.2. 向量化动态扩散流程

为了实现“极速”与“动态”，本文摒弃了耗时的逐像素循环处理，将置乱后的图像矩阵 P'' 直接进行位平面分解，并利用 2D-HEICM 混沌序列生成动态索引矩阵，通过矩阵级并行寻址完成扩散。具体步骤如下：

步骤 1：动态规则与掩码矩阵生成

继续迭代 2D-HEICM 系统，截取末尾的 $M \times N$ 个状态值重塑为动态控制矩阵 R_{seq} 与混沌掩码矩阵 M_{mask}。利用公式(10)计算每个像素点对应的动态 DNA 编码规则索引矩阵 R (取值 1~8)及掩码像素矩阵 K (取值 0~255)：

$$\begin{cases} R(i,j) = \left\lfloor R_{seq}(i,j) \times 10^{10} \right\rfloor \bmod 8 + 1 \\ K(i,j) = \left\lfloor M_{mask}(i,j) \times 255 \right\rfloor \end{cases} \tag{12}$$

其中，$i \in [1, M]$，$j \in [1, N]$。这意味着图像中每一个像素点都将采用独立且随机的 DNA 编码规则，极大提升了算法的非线性与抗破解能力。

步骤 2：基于位运算的像素极速拆分

利用位与和位移操作，将置乱图像 P'' 与混沌掩码 K 拆分为 4 个双比特层矩阵。以图像矩阵分解为例：

$$\begin{cases} L_1 = (P'' \text{ bitand } 192) \gg 6 \\ L_2 = (P'' \text{ bitand } 48) \gg 4 \\ L_3 = (P'' \text{ bitand } 12) \gg 2 \\ L_4 = (P'' \text{ bitand } 3) \end{cases} \tag{13}$$

同理，将掩码 K 拆分为 K_1~K_4。此操作在底层矩阵维度完成，彻底避免了将十进制转为二进制字符串所带来的算力消耗。

步骤 3：动态 DNA 并行异或与解码

根据动态规则矩阵 R，将拆分后的数值矩阵映射为 DNA 碱基矩阵，并查表(表 2)进行并行异或运算。设经过动态编码、异或及动态解码后得到的 4 个双比特结果层矩阵为 D_1, D_2, D_3, D_4，则最终的密文图像矩阵 C 可通过位重组极速合成：

$$C = (D_1 \ll 6) + (D_2 \ll 4) + (D_3 \ll 2) + D_4 \tag{14}$$

通过引入混沌掩码并动态切换编码规则，任何明文像素的微小改变都会在动态映射下引发不同的碱基运算结果。结合矩阵级别的向量化操作，该算法在实现完美雪崩效应与直方图平坦化的同时，展现出了对卫星大图像的卓越处理效率。

4. 实验仿真与安全性能评价

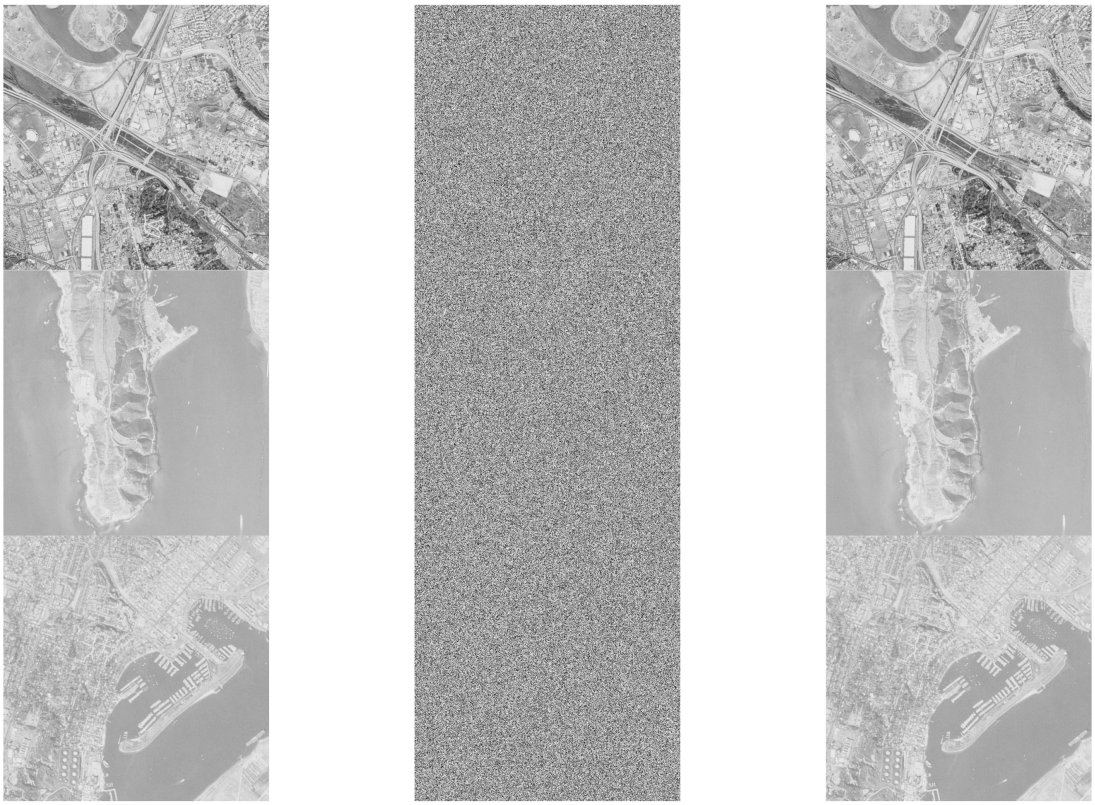
为全面评估本文提出的基于新型 2D-HEICM 与动态 DNA 编码的卫星图像加密算法的有效性与安全性，本章在 MATLAB R2025a 软件平台下进行了详尽的仿真实验。实验硬件环境配置为 Intel (R) Core (TM) Ultra 9 275HX (2.70 GHz)处理器，32 GB 内存，Windows 11 操作系统。

为了验证算法对不同纹理特征遥感数据的普适性，测试图像集均选取自国际权威的 USC-SIPI 图像数据库中的高分辨率航空/卫星图像集。本文从中挑选了三幅具有代表性的 512 × 512 灰度图像进行测试，分别命名为 Image1 (复杂立交桥)、Image2 (岛屿)和 Image3 (港口)。

4.1. 仿真实验与视觉安全性分析

一个成熟的图像加密系统必须具备两个最基本的视觉特征[13]：一是将包含高价值特征信息的明文图像转换为毫无规律的类噪声密文，使攻击者无法通过人类视觉系统或图像识别算法获取任何有用的先验知识；二是能够在接收端凭借正确的密钥实现密文图像的零误差还原。

图 6 展示了本文算法对三幅不同卫星图像进行加解密测试的视觉效果对比。



(a) 原始图像　(b) 加密图像　(c) 解密图像

Figure 6. Comparison of visual effects of encryption and decryption of three different satellite images
图 6. 三幅不同卫星图像的加解密视觉效果对比

从图 6 的第一列可以看出，原始的卫星图像包含了极其丰富的空间几何结构和强烈的相邻像素相关性，这些特征是军事侦察或地理信息提取的关键。

经过本文算法中基于 2D-HEICM 的行列置乱与极速动态 DNA 扩散处理后，观察图 6 第二列的加密结果可知，三幅密文图像在视觉上均呈现出极其均匀的“雪花状”白噪声纹理。无论是建筑物的边缘轮

廓，还是山脉、海洋的大面积平滑区域，其原始的纹理和结构信息均被彻底掩盖。这种高度的视觉混乱状态表明，本文提出的动态 DNA 编码策略能够有效地打破原始卫星图像的空间相关性，实现了从视觉层面的完美信息隐藏，具备极强的视觉安全性。

进一步地，观察图 6 第三列的解密结果。在输入完全正确的 SHA-256 关联密钥和 2D-HEICM 初始参数后，解密算法成功地从杂乱无章的密文噪声中无损地恢复出了原始的卫星图像。解密后的图像在视觉质量上与原图不存在任何肉眼可见的失真或伪影，这不仅验证了算法的对称可逆性，也证明了其在实际高精度遥感数据传输应用中的可靠性。综合以上多组测试图像的实验表现，本文算法展现出了优异的普适性和强大的加密能力。

4.2. 安全性能与效率评估

一个优秀的图像加密算法不仅需要在视觉上完美掩盖明文信息，还必须能够经受住密码学界严苛的量化指标测试。本节将从密钥空间、信息熵、像素相关性以及执行效率四个维度，对本文提出的加密算法进行全面的量化评估。

4.2.1. 密钥空间分析

密钥空间是指密码系统中所有合法密钥的集合规模。为了有效抵御现代计算机的穷举攻击，密码学界普遍要求安全算法的密钥空间必须大于 2^{128}。

本文算法的密钥包含 2D-HEICM 系统的初始状态参数。具体而言，算法的密钥由 5 个混沌系统参数构成，在 IEEE 754 双精度浮点数标准下，计算机对实数的运算精度约为 10^{-15}。因此，混沌系统参数所能提供的密钥空间为$(10^{15})^5 = 10^{75}$，约为 2^{249}。这不仅远超 2^{128} 的理论安全阈值，也优于绝大多数现有的二维混沌加密方案，从物理层面彻底阻断了穷举破解的可能性。

4.2.2. 信息熵分析

密钥空间是指密码系统中所有合法密钥的集合规模。为了有效抵御现代计算机的穷举攻击，密码学界普遍要求安全算法的密钥空间必须大于 2^{128}。

信息熵是信息论中用于衡量系统混乱程度与随机性的核心指标。对于一幅灰度等级为 $L=256$ 的 8 比特图像，其信息熵 $H(m)$的计算公式如式(13)所示：

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \tag{15}$$

其中，$P(m_i)$表示灰度值为 m_i 的像素在整幅图像中出现的概率。当图像表现为绝对随机的理想白噪声时，每个灰度级出现的概率均为 1/256，此时信息熵达到理论最大值 8。密文图像的信息熵越接近 8，说明加密算法的随机性越好，信息泄露的风险越低。

本文计算了三幅测试图像加密前后的信息熵，结果如表 3 所示。

Table 3. Comparison of information entropy of different satellite images before and after encryption
表 3. 不同卫星图像加密前后的信息熵对比

测试图像(512 × 512)	原图信息熵	密文信息熵	理想值
Image1 (复杂立交桥)	7.3526	7.9993	8
Image2 (岛屿)	6.0193	7.9993	8
Image3 (港口)	6.5022	7.9993	8

从表 3 的统计数据可以看出，原始卫星图像由于存在大面积相似区域，其信息熵普遍偏低。而在加

密后，三幅密文图像的信息熵均达到了 7.999 以上，极其逼近理论极限值 8。这定量地证明了本文设计的动态 DNA 编码策略能够产生具有极高不确定性的密文数据，有效抵御了香农理论下的信息熵攻击。

4.2.3. 相邻像素相关性分析

自然图像(尤其是高分辨率的卫星图像)在空间上存在极强的数据冗余，即相邻像素点之间的灰度值通常非常接近，其相关系数往往趋近于 1。攻击者常利用这种强相关性进行统计预测攻击。一个安全的图像加密算法必须彻底打破这种空间相关性，使密文图像的相邻像素呈现出零相关的随机白噪声特性。

为了量化评估本文算法对空间相关性的消除效果，从图像中随机抽取 N 对(本文取 $N = 8000$)相邻像素点，分别在水平(Horizontal)、垂直(Vertical)和对角线(Diagonal)三个方向上计算相关系数 r_{xy}。其数学计算公式如下：

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{16}$$

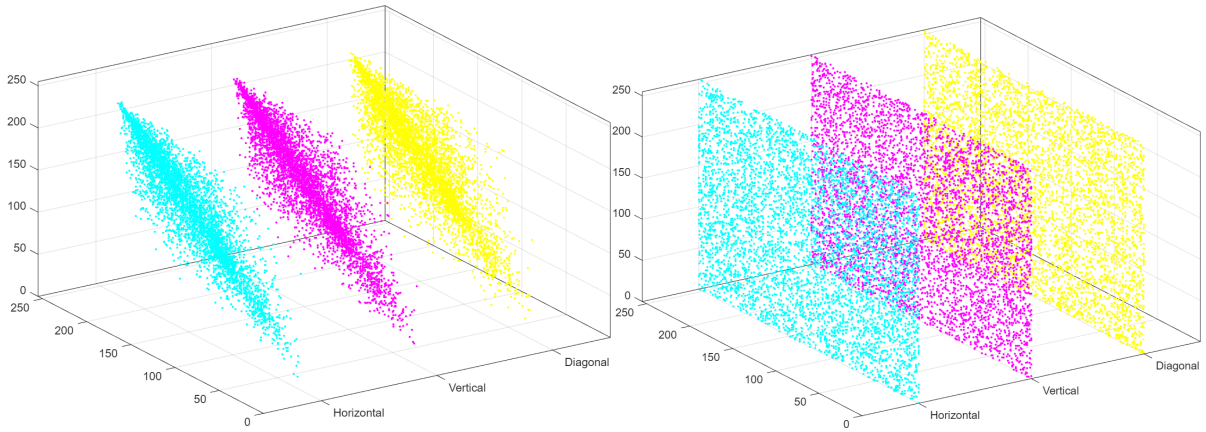
$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{17}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)\left(y_i-E(y)\right) \tag{18}$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{19}$$

式中，x 和 y 分别表示相邻两个像素的灰度值；$E(x)$为均值；$D(x)$为方差；$\operatorname{cov}(x,y)$为协方差。

图 7 直观地展示了以 Image1 (复杂立交桥)为例，在加密前后随机选取的 8000 对相邻像素在三个方向上的散点分布情况。



(a) 原始图像相邻像素相关性散点图　　(b) 加密图像相邻像素相关性散点图

Figure 7. Comparison of scatter plots of adjacent pixel correlation before and after encryption of Image1 satellite image
图 7. Image1 卫星图像加密前后的相邻像素相关性散点图对比

从图 7(a)可以清晰地观察到，原始卫星图像的相邻像素点紧密地聚集在主对角线 $y=x$ 附近，表明相邻像素的灰度值高度一致，存在强烈的线性相关性。然而，经过本文的行列置乱与动态 DNA 扩散加密后，图 7(b)中密文图像的散点如同满屏的“雪花”般，均匀且杂乱地分布在整个 256×256 的坐标空间中，没有任何聚集趋势。这从视觉上直观地证明了像素间的强相关性已被彻底打破。

为了提供更精确的定量评价，表 4 统计了三幅不同测试卫星图像在加密前后的相关系数具体数值。

Table 4. Comparison of the correlation coefficients of adjacent pixels before and after encryption of different test satellite images
表 4. 不同测试卫星图像加密前后的相邻像素相关系数对比

测试图像	状态	水平方向	垂直方向	对角线方向
Image1	原图	0.8074	0.7820	0.7029
	密文	0.0075	0.0022	0.0060
Image2	原图	0.9225	0.9373	0.8980
	密文	−0.0125	0.0453	0.0099
Image3	原图	0.8766	0.8638	0.8097
	密文	0.0191	0.0126	−0.0063

结合表 4 的量化数据可知，三幅原始卫星图像在各个方向上的相关系数均高达 0.7 以上。而加密后的密文图像，其相关系数均发生断崖式下降，极度逼近于理想值 0。这一实验结果充分验证了基于 2D-HEICM 驱动的移位置乱与动态 DNA 扩散层具有卓越的去相关性能，能够有效抵御任何形式的统计分析攻击。

4.2.4. 时间效率分析

对于军事侦察、灾害监测等需要实时传输与处理的应用场景，加密算法的执行效率是衡量其实用价值的关键指标。传统的基于 DNA 编码的图像加密方案，由于普遍依赖逐像素的字符串转换与迭代计算，在处理高分辨率的遥感卫星图像时往往存在耗时过长的问题。

为了验证本文提出的基于位运算的向量化扩散策略的先进性，本节在 4.1 节所述的硬件环境下，对不同尺寸的卫星图像进行了加密时间测试，并与近年来部分经典的图像加密算法进行了横向对比。

表 5 详细记录了本文算法在处理 256 × 256、512 × 512 和 1024 × 1024 三种不同分辨率图像时的各阶段耗时。

Table 5. Encryption time test of the algorithm proposed in this paper under images of different resolutions (unit: seconds)
表 5. 本文算法在不同分辨率图像下的加密时间测试(单位：秒)

图像分辨率	密钥生成	行列置乱	极速 DNA 扩散	总加密时间	总解密时间
256 × 256	0.0092	0.0011	0.0115	0.0218	0.0169
512 × 512	0.0312	0.0022	0.0535	0.0869	0.0800
1024 × 1024	0.1210	0.0119	0.1600	0.2929	0.2736

从表 5 的数据可以清晰看出，本文算法展现出了卓越的实时处理能力。即便在处理百万像素级的 1024 × 1024 图像时，总加密耗时也仅为 0.29 秒左右。特别值得注意的是，算法的核心创新——极速 DNA 扩散层，其耗时随像素数量的增长呈准线性关系，这得益于其底层的矩阵并行化与位运算机制，彻底避免了传统算法中因循环迭代带来的指数级时间膨胀。

为了进一步突显其竞争力，表 6 将本文算法在处理 512 × 512 图像时的总耗时与部分已有文献中的先进加密方案进行了对比。

Table 6. Comparison of time consumption for processing 512 × 512 images by different encryption algorithms (unit: seconds)
表 6. 不同加密算法处理 512 × 512 图像的耗时对比(单位：秒)

加密算法	核心技术	加密时间
文献[7] (2D-LASM)	混沌置乱 + 全局扩散	0.5312
文献[8] (2D-LSCM)	混沌置乱 + DNA	1.9567
本文算法	超混沌 + 向量化 DNA	0.0869

综合表 5 和表 6 的数据，可以得出结论：本文提出的结合新型超混沌映射与极速向量化 DNA 扩散的加密方案，不仅在理论层面具备极高的安全性，更在实践层面展现出了卓越的计算效率。其性能远超众多依赖传统 DNA 运算的算法，特别适用于需要对高分辨率遥感卫星图像进行实时加密与安全传输的关键应用场景。

5. 结论

本文设计并实现了一种结合新型二维超混沌映射 2D-HEICM 与动态 DNA 编码的高效卫星图像加密算法。通过深入的动力学特性分析证明，提出的 2D-HEICM 系统在宽泛的参数范围内具有显著的超混沌行为，其最大李雅普诺夫指数(MLE)远超同类典型映射，为算法提供了坚实的安全性物理基础。

在加密流程设计上，算法利用 SHA-256 建立明文关联机制，增强了抵御已知明文攻击的能力，并通过行列循环移位有效打破了卫星图像的空间相关性。核心创新点在于提出了基于位运算的向量化动态 DNA 扩散策略，利用矩阵并行化处理彻底解决了传统 DNA 加密在大尺度遥感图像上的性能瓶颈。

仿真实验与量化指标评估显示，该算法在处理高分辨率卫星图像时表现卓越：密文图像的信息熵极度逼近理论极限 8，相邻像素相关系数降至 10^{-2} 量级，且单幅 512 × 512 图像的加密耗时仅为约 0.08 秒。综上所述，本文算法在保持极高统计安全性的同时，展现出了显著的计算效率优势，非常适用于对实时性要求较高的大规模卫星遥感数据安全传输与处理。

基金项目

本研究得到了巢湖学院 2025 年度省级大学生创新创业训练计划项目(项目编号：S202510380001)、本研究得到了巢湖学院 2024 年校级教学改革与研究项目(项目编号：x24jyxm02)、企业委托技术开发横向项目“基于混沌与位平面的图像加密算法研究及 FPGA 实现(项目编号：hxkt20240285)”、企业委托技术开发横向项目“基于机器学习的财政资金异常流动智能预警模型研究(项目编号：hxkt2511021)”的支持。

参考文献

[1] 肖嵩, 陈哲, 杨亚涛, 等. 基于混沌理论与 DNA 动态编码的卫星图像加密算法[J]. 电子与信息学报, 2024, 46(3): 1128-1137.

[2] 陈哲. 基于混沌理论的卫星图像加密算法研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2024.

[3] 马浩然, 章庆勇. 基于双混沌系统与 DNA 编码的医学图像加密算法[J]. 科技创新与应用, 2026, 16(6): 135-138.

[4] 秦秋霞. 基于 DNA 编码和位平面循环移位的混沌图像加密算法研究[J]. 信息与电脑, 2026, 38(1): 10-13.

[5] 范素娟, 董孝伟, 左宪禹, 等. 基于混沌系统和动态 DNA 编解码规则的图像加密方法[J]. 河南大学学报(自然科学版), 2025, 55(5): 580-589.

[6] 刘宇平. 基于四维混沌与 DNA 编码的图像加密系统设计与实现[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2025.

[7] Hua, Z. and Zhou, Y. (2016) Image Encryption Using 2D Logistic-Adjusted-Sine Map. *Information Sciences*, **339**, 237-253. https://doi.org/10.1016/j.ins.2016.01.017

[8] Hua, Z., Jin, F., Xu, B. and Huang, H. (2018) 2D Logistic-Sine-Coupling Map for Image Encryption. *Signal Processing*,

149, 148-161. https://doi.org/10.1016/j.sigpro.2018.03.010

[9] 王全余. 基于混沌和 DNA 编码的图像加密算法研究[D]: [博士学位论文]. 北京: 中国矿业大学, 2024.

[10] Liu, S., Liu, P., Liu, J. and Wang, L. (2015) Spatial Chaos on Surface and Its Associated Bifurcation and Feigenbaum Problem. *Nonlinear Dynamics*, **81**, 283-298. https://doi.org/10.1007/s11071-015-1991-7

[11] 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

[12] 陆向艳, 陈泉金. 基于 Arnold 和 Logistic 算法的混沌图像加密方法[J]. 网络安全技术与应用, 2025(6): 39-41.

[13] 赵晶晶. 基于超混沌系统的跨通道图像加密算法研究[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2025.