Pure Mathematics 理论数学, 2026, 16(3), 122-134
Published Online March 2026 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2026.163076

Hans汉斯

基于压缩感知和动态DNA编码的图像加密算法

邓一灵，姑丽加玛丽·麦麦提艾力

新疆师范大学数学科学学院，新疆 乌鲁木齐

收稿日期：2026年2月15日；录用日期：2026年3月11日；发布日期：2026年3月18日

摘　要

针对图像在传输过程中面临的安全性问题，提出了一种基于混沌系统、压缩感知与动态DNA编码相结合的图像加密方案。首先，对原始图像进行二维离散余弦变换(DCT)实现稀疏表示，利用Logistic混沌映射生成的测量矩阵完成二维压缩感知测量，在实现数据压缩的同时引入初步加密。随后，采用Zigzag进行全局索引置乱，有效破坏像素间相关性；再经非线性映射完成量化，并结合高维混沌系统生成的混沌序列对其进行扩散。进一步地，引入基于Logistic混沌映射与四维超混沌系统的动态DNA编码机制，对加密图像进行DNA编码、DNA运算及跨块级联扩散，有效增强密钥空间和扩散性能。最后，通过加密的逆过程以及重构算法得到重构图像。实验结果表明，该方案在保证较高压缩效率和良好解密质量的同时，复杂度较高，加密效果好，具有较强的安全性。

关键词

超混沌系统，图像加密，压缩感知，动态DNA编码

An Image Encryption Algorithm Based on Compressed Sensing and Dynamic DNA Coding

Yiling Deng, Gulijiamali Maimaiti Aili

School of Mathematical Sciences, Xinjiang Normal University, Urumqi Xinjiang

Received: February 15, 2026; accepted: March 11, 2026; published: March 18, 2026

Abstract

To address the issues of security and limited bandwidth during image transmission, an image encryption scheme integrating a chaotic system, compressive sensing, and dynamic DNA coding is proposed. First, the original image is sparsely represented using a two-dimensional discrete cosine

文章引用: 邓一灵, 姑丽加玛丽·麦麦提艾力. 基于压缩感知和动态 DNA 编码的图像加密算法[J]. 理论数学, 2026, 16(3): 122-134. DOI: 10.12677/pm.2026.163076

transform (DCT). A measurement matrix generated by the Logistic chaotic map is then employed to perform two-dimensional compressive sensing measurements, achieving data compression while introducing preliminary encryption. Subsequently, a zigzag-based global index scrambling strategy is applied to effectively disrupt inter-pixel correlations. The measured data are then quantized through a nonlinear mapping, followed by diffusion using chaotic sequences generated by a high-dimensional chaotic system. Furthermore, a dynamic DNA coding mechanism based on the Logistic chaotic map and a four-dimensional hyperchaotic system is introduced. The encrypted image undergoes DNA encoding, DNA operations, and inter-block cascading diffusion, significantly enhancing the key space and diffusion performance. Finally, the reconstructed image is obtained through the inverse encryption process combined with a reconstruction algorithm. Experimental results demonstrate that the proposed scheme achieves high compression efficiency and satisfactory decryption quality, while exhibiting strong encryption performance, high computational complexity, and robust security.

Keywords

Hyperchaotic System, Image Encryption, Compressive Sensing, Dynamic DNA Encoding

1. 引言

随着人工智能、互联网及多媒体技术的飞速发展，数字图像已成为人们感知与沟通的重要媒介，广泛应用于军事、医疗、工业、金融、遥感及国家安全等领域[1]。然而，在信息高度共享的网络环境中，图像传输易遭非法截取、篡改，安全与效率面临严峻挑战[2]。因此，图像加密作为有效保护机制备受关注。鉴于图像的高冗余度及像素间强相关性，传统文本加密算法(如 AES、DES、RSA)已不适用，从而催生了大量替代性图像加密算法。这些算法采用多种不同技术实现，例如混沌系统[3] [4]、压缩感知(CS) [5] [6]、DNA 编码[7]-[9]、量子计算[10] [11]、元胞自动机[12] [13]等。这些技术将具有视觉意义的明文图像转化为类噪声或类纹理的密文图像，从而有效防止攻击者获取任何有效的明文图像信息。自 Friedrich 等人[14]于 1998 年提出基于混沌系统的经典置乱－扩散加密架构以来，混沌图像加密技术因其优异的伪随机性、不可预测性、遍历性及对初值的极端敏感性等特性，近年来得到广泛研究。结构简单的一维混沌系统能够快速生成混沌序列：文献[15]采用 Logistic 映射对置乱后的图像进行加密；舒永录等人[16]提出了一种基于置乱与扩散同步操作的图像加密算法，其通过混沌序列控制，在像素级同步完成置乱与扩散。然而，Li 等人[17]通过典型实例证明了基于混沌逻辑映射的图像加密算法存在安全隐患。随着研究深入，具有更复杂动力学行为的高维混沌系统逐渐被应用于图像加密系统。文献[18]提出基于新型五维正弦混沌系统的彩色图像加密方案，该系统产生的混沌数据用于加密过程。此外，Li 等人[19]提出基于 Chen 超混沌系统的快速图像加密方案，通过生成随机序列对明文图像的四个低频分量进行置乱。尽管高维混沌系统具有复杂轨迹和长迭代周期的高安全性，但其时间复杂度和计算耗时均高于一维混沌系统。凭借 DNA 的高并行性和大存储容量特性，结合 DNA 编码与混沌系统的图像加密方案日益增多。例如，Chen 等人[20]提出基于自适应置乱－扩散和 DNA 随机编码的图像加密技术。然而现有研究存在两大安全隐患[21]：其一，多数系统中所有像素点的 DNA 编码/解码规则固定不变，这种与明文无关的固定规则会显著降低方案安全性；其二，大多数 DNA 加密算法采用 DNA 加法、减法、异或和同或运算对 DNA 矩阵进

行扩散，这些基于二进制演算的操作导致 DNA 碱基转换结果可预测，增大了算法被破解的风险。针对图像传输频繁且数据量大的特点，压缩感知(CS)技术可用于图像压缩以提升传输效率、降低带宽需求并节省存储空间。CS 能实现对图像的非均匀采样、压缩和加密同步进行。自 Donoho 提出压缩感知理论[22]以来，众多基于 CS 的图像加密方案被提出。Lu 等人[23]提出基于 CS 和双随机相位编码技术的加密方案。Huang 等人[24]利用混沌系统对压缩图像进行置乱以增强 CS 算法安全性。这些方案虽然效果良好，但仍存在混沌性能不强、密钥空间较小、加密图像扩散性不足等问题。

针对上述问题，本文提出了一种复杂、安全的图像加密方案。通过结合混沌系统、压缩感知(CS)、二维离散余弦变换(DCT)与 DNA 编码扩散机制对图像加密。首先对原始图像进行 DCT 变换，实现稀疏表示；随后利用 Logistic 混沌序列构造测量矩阵，对稀疏系数进行压缩感知测量，并通过 Zigzag 索引置乱，破坏像素间的相关性。并在此基础上，引入四维超混沌系统生成的密钥流，与测量结果进行像素级异或操作，实现第一阶段加密。进一步地，采用 Logistic 映射与四维超混沌系统共同驱动 DNA 编码、DNA 运算与扩散机制，实现对加密图像的二次加密，从而获得最终密文图像。

本文的创新之处在于将混沌系统、压缩感知与 DNA 编码扩散机制进行多层次融合，构建了一种压缩与加密同步完成的图像加密方案。算法首先结合二维 DCT 变换实现图像稀疏表示，并利用 Logistic 混沌序列构造测量矩阵，从而增强压缩感知测量过程的随机性与安全性；随后完成 Zigzag 索引置乱并引入四维超混沌系统生成的密钥流，对测量结果进行像素级异或扩散，提高对密钥的敏感性。在此基础上，进一步利用 Logistic 映射与四维超混沌系统联合控制 DNA 编码规则、DNA 运算方式及块间扩散过程，实现二次加密，使密文同时具备良好的混淆性与扩散性。该方法在降低数据维度和传输开销的同时，有效扩大了密钥空间，具有良好的加密效果。

2. 基本理论

2.1. 四维超混沌系统

通过对经典的 Lorenz 混沌系统进行改进，构建四维超混沌系统[25]，其数学模型如式(1)所示：

$$\begin{cases} \dot{x} = -ax + by \\ \dot{y} = cx - dy - xz + mw \\ \dot{z} = -ez + xy \\ \dot{w} = -xz + mw \end{cases} \tag{1}$$

其中，a、b、c、d、e 和 m 为系统参数。当它们分别设置为 12、16、12、2、3 和 1，且初始值为$(1,-1,1,-2)$时，该系统对应的李雅普诺夫指数分别为：LE1 = 1.1227，LE2 = 0.1291，LE3 = 0.0530，LE4 = −2.4424，其存在三个正的李雅普诺夫指数，则系统处于超混沌状态。

2.2. 一维 Logistic 混沌映射

本文利用经典非线性离散动力系统——一维 Logistic 混沌映射。在压缩感知加密阶段，Logistic 混沌序列用于构造测量矩阵，对稀疏化后的图像数据进行线性测量，实现压缩与初步加密；在扩散与二次加密阶段，Logistic 映射产生的混沌序列，用于生成随机矩阵并参与像素级异或运算与 DNA 编码过程，从而增强密文对明文变化的敏感性。由于 Logistic 映射对初始条件和系统参数具有高度敏感性，其引入有效扩大了密钥空间，提高了算法的安全性和抗统计分析能力。其数学模型定义如式(2)所示：

$$x_{n+1} = \mu x_n \left(1 - x_n\right) \tag{2}$$

式中，n 表示迭代次数，x 是系统变量；μ 为控制参数；$x \in [0,1]$，$\mu \in [0,4]$。其中，当 $\mu \in (3.5699,4]$ 时，

系统处于混沌状态。

2.3. 压缩感知

压缩感知(Compressed Sensing, CS)技术突破了传统奈奎斯特采样定理的速率限制，实现了在远低于该速率下对信号的有效采样。其理论基础是信号的稀疏性，即信号在某些变换域(如离散余弦变换、离散傅里叶变换或离散小波变换)中可以被少量非零系数表征。基于这一特性，CS 技术不仅能同步完成信号的采样与压缩，若选用适当的测量矩阵，该过程还可兼具加密效果，为信号的安全高效处理提供了集成解决方案。

假设长度为 N 的一维实离散信号 $X \in \mathbb{R}^N$，可以采用 $N \times N$ 维正交基矩阵，$\varphi = [\varphi_1, \varphi_2, \cdots, \varphi_N]$ 的线性组合表示为：

$$x \in \sum_{i=1}^{n} \alpha_i \varphi_i = \varphi\alpha \tag{3}$$

其中，φ_i 为 φ 的列向量，α_i 为加权系数，能够对信号 x 进行压缩感知的前提条件是 x 具有稀疏性。如果 α 中有 K 个($K \ll N$)非零值，则 x 是 K 稀疏信号。用测量矩阵 Φ 对信号 x 进行投影 $y = \Phi x = \Phi\varphi\alpha$，该过程为降维过程，理论上最优的求解方法是解 l_0 范数最小化问题：

$$\min_{\alpha} \|\alpha\|_{l_0} \quad \text{s.t.} \quad y = \Phi\varphi\alpha \tag{4}$$

N 较大时该优化问题成为 NP-hard 问题，为解决这个难点，可通过解 l_1 范数问题近似替代原问题的求解：

$$\hat{\alpha} = \arg\min \|\alpha'\|_1 \quad \text{s.t.} \quad y = \Phi\varphi\alpha' \tag{5}$$

本文使用 logistic 混沌系统生成 CS 的随机测量矩阵。

2.4. DNA 序列编码

在生物学中，DNA 是由四种脱氧核苷酸组成的长链分子，四种脱氧核苷酸分别为腺嘌呤(A)、胞嘧啶(C)、鸟嘌呤(G)和胸腺嘧啶(T)。根据 DNA 碱基互补配对规律，A 与 T 互补配对，G 与 C 互补配对。由于二进制系统中的“0”和“1”具有互补关系，因此可以将 DNA 碱基对与二进制编码相对应。表 1 为 DNA 碱基之间互补规则的 8 种编码方式。

Table 1. Eight coding methods of DNA
表 1. DNA 的 8 种编码方式

		1	2	3	4	5	6	7	8
DNA 编解码方式	A	00	00	01	01	10	10	11	11
	G	01	10	00	11	00	11	01	10
	T	11	11	10	10	01	01	00	00
	C	10	01	11	00	11	00	10	01

3. 图像加密方案

本节将介绍一种基于一维 Logistic 混沌系统、四维超混沌系统、CS、二维 DCT 以及动态 DNA 编码的新型图像加密方案。该加密方案分为 2 个阶段：加密阶段和解密阶段。

3.1. 加密阶段

本文提出一种结合压缩感知与动态 DNA 编码的彩色图像加密方案，采用两级加密结构：第一级为基于压缩感知的混沌加密，第二级为基于动态 DNA 编码的超混沌加密。整个加密流程实现了压缩、置乱、扩散的有机结合。首先，通过混沌系统生成测量矩阵，对 DCT 稀疏化后的图像进行压缩感知采样，实现初步加密与数据压缩；随后利用 Zigzag 置乱和异或操作增强安全性。其次，引入 DNA 编码技术，以超混沌序列动态控制编码、运算与解码规则，在分块层面实现二次扩散加密。该方案通过双重加密机制，在保证压缩效率的同时显著提升了系统安全性。

基于压缩感知的混沌图像加密的具体步骤如下：

步骤 1 给定一张 $M*N*3$ 的彩色图像 I，其对应矩阵的大小的长度为 M 和宽度为 N，将彩色图像 I 转换为灰度图像，三个通道的图像分别记为 I1、I2 和 I3。由于三个通道加密方案一致，因此，在这里我们对其中一个通道进行详细说明。

步骤 2 测量矩阵可以分为 2 类，即确定性测量矩阵和随机性测量矩阵，本文使用一维 logistic 映射的混沌序列来生成确定性测量矩阵。首先设定压缩比 f，并根据式(6)计算测量值维度 M'。随后，利用 Logistic 混沌映射生成测量矩阵：用 $key_1\left(x_0,\mu\right)$ 迭代 logistic 映射生成得到混沌序列，得到的混沌序列中有 $M'N$ 个元素 $L=\left\{l_1,l_2,\cdots,l_{m'n}\right\}$，并将其转换成 $M'\times N$ 矩阵，即为压缩测量矩阵 Phi。

$$M'=round\left(f*N\right) \tag{6}$$

$$Phi=\begin{bmatrix} l_1 & l_{M'+1} & \cdots & l_{M'(N-1)} \\ l_2 & l_{M'+2} & \cdots & l_{M'(N-1)+1} \\ \vdots & \vdots & & \vdots \\ l_{M'} & l_{2M'} & \cdots & l_{MN} \end{bmatrix}$$

步骤 3 利用二维离散余弦变换(DCT)基矩阵 D 对图像进行稀疏变换，通过式(7)得到稀疏系数矩阵 P_s。

$$P_s=D'\times P \tag{7}$$

步骤 4 利用测量矩阵 Phi，对矩阵 P_s 进行测量，得到测量后的矩阵 Y，如式(8)所示：

$$Y=Phi\times P_s \tag{8}$$

步骤 5 通过采用广义 Zigzag 扫描(对角交替遍历)对稀疏后的图像进行置乱操作，得到混淆后的图像矩阵 Q。

步骤 6 通过函数式(9)对矩阵 Q 中的每一个元素值进行非线性变换得到矩阵 Q'。随后，通过式(10)取整量化，得到新的矩阵 H。

$$y=\frac{a_1}{1+\mathrm{e}^{-a_2\cdot(x-a_3)}} \tag{9}$$

$$H=round\left(Q'\right) \tag{10}$$

其中 a_1,a_2,a_3 为固定秘钥参数，x 是矩阵 Q 中的每个元素值。

步骤 7 利用四维超混沌系统生成四个混沌序列 x_1、y_1、z_1、u_1，对其中的第一个混沌序列 x_1 进行非线性变换得到序列 s_1，并截取 s_1 的前 $M'\times N$ 个元素，构成秘钥流 s_1'，并对其取模运算，如式(11)和式(12)：

$$s_1=\mathrm{mod}\left(floor\left(\left(x_1+100\right)\times10^{10}\right),10\times\max\left(M,N\right)\right)+1 \tag{11}$$

$$s_1'=\mathrm{mod}\left(s_1,256\right) \tag{12}$$

步骤 8 利用混沌密钥流 s_1' 对矩阵 H 进行扩散操作，得到矩阵 A。

基于动态 DNA 编码的混沌图像加密的具体步骤如下：

步骤 1 取原始灰度图像 A，其尺寸为 $M'\times N$。设定分块大小 $t=1$，即进行像素级处理。对图像进行补零操作，确保其行数和列数均为 t 的整数倍，使得图像可以被完整且均匀地分割。补零后的图像尺寸仍记为 $M'\times N$，总像素数记为 $SUM=M'\times N$，记为矩阵 A'。

步骤 2 使用一维 Logistic 混沌映射生成伪随机序列，迭代产生长度为 $SUM+1000$ 的序列 p，去除前 1000 个瞬态点，获得动力学特性更稳定的序列。将序列 p 进行变换并对其进行量化，重塑为一个 $M'\times N$ 的随机矩阵 R，此矩阵将在后续 DNA 运算中使用。该过程可用式(13)~式(14)表示：

$$p'=\mathrm{mod}\left(ceil\left(p*10^3\right),256\right) \tag{13}$$

$$R=reshape\left(p',M',N\right) \tag{14}$$

步骤 3 根据四个给定的初值，使用龙格–库塔法(ODE45)求解超混沌系统，生成足够长度的四维轨迹。舍弃前 1501 个点，以确保系统进入充分混沌状态。最后，得到四个混沌序列，分别记为混沌序列 X，Y，Z，U。该过程可用式(15)表示：

$$\begin{cases} X_0=floor\left(x_0\times10^4\right)/10^4 \\ Y_0=floor\left(y_0\times10^4\right)/10^4 \\ Z_0=floor\left(z_0\times10^4\right)/10^4 \\ U_0=floor\left(u_0\times10^4\right)/10^4 \end{cases} \tag{15}$$

步骤 4 根据式(16)对序列 X，Y，Z，U 进行量化和模运算，将其转换为控制 DNA 操作的密钥流 X'，Y'，Z'，U'。其中 X' 用于控制图像矩阵 A' 的 DNA 编码规则，Y' 用于控制随机矩阵 R 的 DNA 编码规则，Z' 用于控制 DNA 的运算规则，U' 用于控制 DNA 的解码规则。

$$\begin{cases} X'=\mathrm{mod}\left(floor\left(X\times10^4\right),8\right)+1 \\ Y'=\mathrm{mod}\left(floor\left(Y\times10^4\right),8\right)+1 \\ Z'=\mathrm{mod}\left(floor\left(Z\times10^4\right),8\right)+1 \\ U'=\mathrm{mod}\left(floor\left(U\times10^4\right),8\right)+1 \end{cases} \tag{16}$$

步骤 5 从补零后的图像 A' 和随机矩阵 R 中分别提取第 i 个 $t\times t$ 大小的块。将图像块 $A'(i)$ 的每个像素值(8 位)拆分为 4 个 2 位组，分别代表一个碱基(A, C, G, T)，根据密钥流 $X'(i)$ 指定的 8 种映射规则之一，将 2 位二进制数映射为对应的碱基字符，生成 DNA 编码矩阵 W1；同样地，对随机矩阵块 $R(i)$根据密钥流 $Y'(i)$ 指定的规则进行 DNA 编码生成 DNA 编码矩阵 W2。根据密钥流 $Z'(i)$ 指定的规则(加法、减法或异或)，对 W1 和 W2 两个 DNA 矩阵进行逐字符的运算，得到结果矩阵 W3。

步骤 6 对每个图像块都进行步骤 5 的加密操作。并将当前结果矩阵与前一个结果矩阵再次根据 $Z'(i)$ 进行指定的 DNA 运算，实现 DNA 域内的链式扩散。

步骤 7 将扩散后的 DNA 矩阵根据密钥流 $U'(i)$ 指定的 8 种规则之一，将碱基字符反向解码为 2 位二进制数，再组合成 8 位的像素值，得到解密后的图像块。将解密后的块合并成矩阵 S。

步骤 8 由于其是彩色图像，因此需对三个通道，均实行上述加密操作，最终，合并三个通道得到加密图像。

3.2. 解密阶段

解密方案包括 DNA 域内行列逆扩散、像素域内逆扩散、逆 Zigzag 置乱以及图像重构过程。首先，对密文图像执行基于动态 DNA 编码的逆运算：利用 Logistic 映射与四维超混沌系统生成与加密方案中一致的混沌序列，动态确定 DNA 解码规则与运算方式，在分块层面依次完成 DNA 解码和逆扩散操作，从而消除第二级超混沌 DNA 加密所引入的扩散效应，恢复一级压缩感知加密后的数据。随后，进入基于压缩感知的逆重构阶段，依次进行反异或、反非线性映射以及逆 zigzag 置乱操作，以抵消混沌置乱与扩散的影响；在此基础上，利用与加密阶段一致的测量矩阵和 DCT 稀疏基，通过 SL_0 稀疏重构算法对压缩感知采样数据进行重建和反变换恢复出原始彩色图像。

4. 实验仿真与测试

4.1. 实验结果

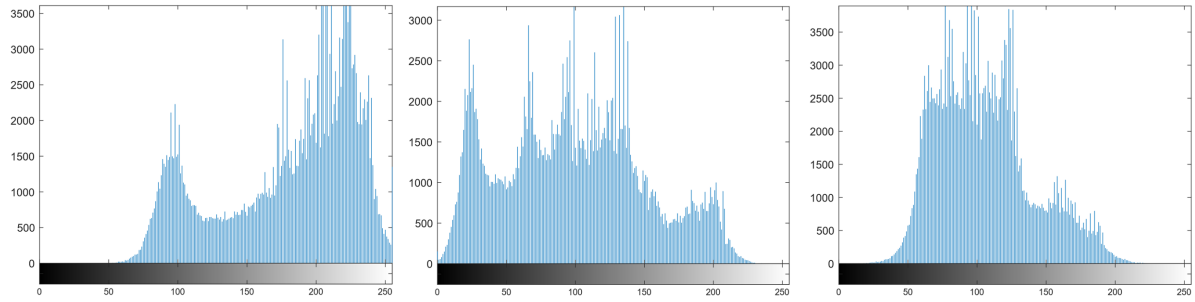
本节概述了在配备 2.40 GHz CPU 和 16 GB RAM 的 Windows 11 操作系统平台上，基于软件 MatlabR2023b 仿真环境对提出的加密算法进行了性能评估。设置四维超混沌系统参数分别为 $a=12$、$b=16$、$c=12$、$d=2$、$e=3$、$m=1$ 且初始值为 0.1，0.1，0.1，0.1，Logistic 混沌系统参数为 $\mu=4$，$\mu=3.99$，初始值分别为 0.6 和 0.1，压缩率为 0.85。实验随机采用大小为 $256\times256\times3$ 的 Girl、Fruit 和 $512\times512\times3$ 的 Lena 作为测试图像，仿真结果如图 1 所示，其中图 2(a)，图 2(d)和图 2(g)为原始图像，图 2(b)，图 2(e)和图 2(h)为加密图像，图 2(c)，图 2(f)和图 2(i)为解密图像。从图 1 可以看出，压缩加密图像的大小不等于原始图像的大小，且解密图像与原始图像在视觉上并没有明显区别，表明该压缩加密算法效果良好。

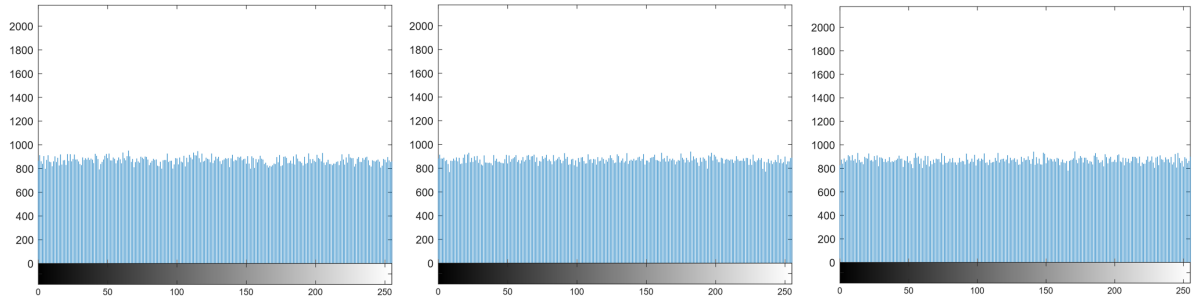
(a) Couple 原图　(b) Couple 加密图　(c) Couple 解密图

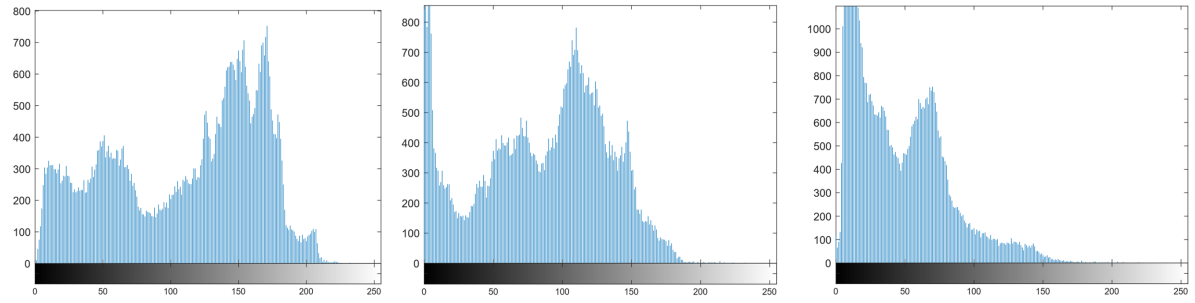
(d) Fruit 原图　(e) Fruit 加密图　(f) Fruit 解密图

(g) Lena 原图　(h) Lena 加密图　(i) Lena 解密图

Figure 1. Experimental diagram of digital image encryption and decryption
图 1. 数字图像加解密实验图


Lena 明文 R 通道直方图　Lena 明文 G 通道直方图　Lena 明文 B 通道直方图


Lena 密文 R 通道直方图　Lena 密文 G 通道直方图　Lena 密文 B 通道直方图


Fruit 明文 R 通道直方图　Fruit 明文 G 通道直方图　Fruit 明文 B 通道直方图

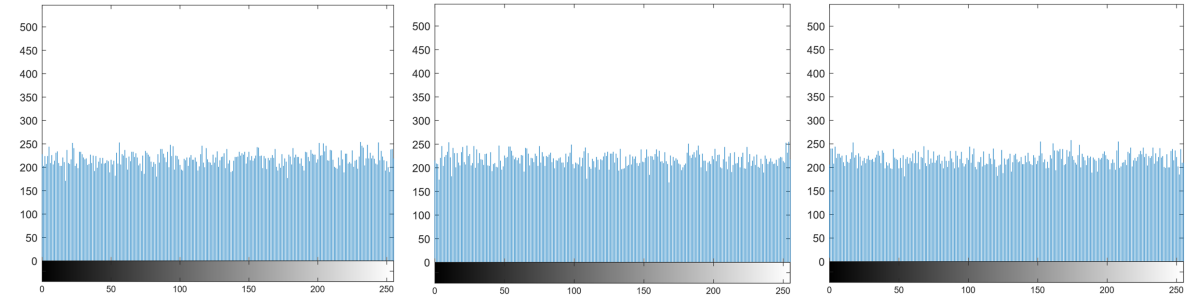

Fruit 密文 R 通道直方图　Fruit 密文 G 通道直方图　Fruit 密文 B 通道直方图

Figure 2. The histogram comparison of each channel before and after image encryption
图 2. 图像加密前后在各个通道上的直方图对比

4.2. 密钥空间分析

密钥空间是指密码系统中所有可能且彼此不同的有效密钥所构成的集合，密钥空间的大小直接影响系统的整体安全强度。通常而言，密钥空间越大，系统抵抗暴力破解的能力越强，因为攻击者必须穷举所有潜在密钥组合才能成功恢复明文。在本文提出的图像加密方案中，系统密钥由六个初始条件和十一

个控制参数共同构成，形成了较为庞大的密钥空间。这种设计使得攻击者在现实可行的时间范围内难以完成穷举搜索，从而有效提升了加密系统的安全性。由于计算机准确度为 10^{-15}，始密钥空间如式(17)所示。

$$\text{秘钥空间} = \prod_{t=1}^{17} 10_t^{15} \tag{17}$$

式(17)的结果为 10^{255}，远大于 2^{100}。对于安全的彩色图像加密算法，其密钥空间充足。因此，该系统的密钥空间足以挫败穷举攻击。

4.3. 直方图分析

密文图像的直方图用于描述像素取值的分布情况，是衡量加密算法抗统计分析能力的重要依据。所谓统计分析攻击，是指攻击者通过研究加密图像的统计规律，试图推断出密钥或原始图像信息，从而实施针对性的攻击。由图可见，加密后图像在 R、G、B 三个通道上的直方图均接近均匀分布，说明像素值分布趋于随机，原有的统计特征已被有效削弱和掩盖。因而，密文图像与明文图像在统计结构上存在明显差异，表明该算法具备较强的抗统计攻击能力。

本文选取了“Lena”和“Fruit”两幅不同图像进行加密实验，实验结果如图 2 所示。从结果可以看出，加密前的明文图像直方图呈现明显的不均匀分布，而加密后的图像直方图则趋于平坦，显示出较好的均匀性。

4.4. 信息熵分析

信息熵用于度量信息的不确定程度，是评价图像加密性能的重要指标之一。对于 8 位灰度图像而言，其理论最大信息熵为 8。当信息熵值越接近该上限时，说明图像像素分布越均匀、随机性越强，表明加密结果越接近理想的随机状态，从而具有更优的安全性。本文选取 Lena、Fruit 和 Couple 彩色图像作为测试样本，将所提出方法加密后的信息熵与文献[26] [27]中算法的结果进行对比分析，结果如表 2 所示。信息熵的计算公式如式(18)所示：

Table 2. Comparison of information entropy in color images
表 2. 彩色图像信息熵对比

测试图像	R 通道	G 通道	B 通道
Couple 图像	7.9966	7.9970	7.9968
Fruit 图像	7.9965	7.9966	7.9970
Lena 图像	7.9991	7.9993	7.9992
文献[26] (Lena)	7.9912	7.9917	7.9912
文献[27] (Lena)	7.9912	7.9913	7.9914

$$M(x) = -\sum_{k=0}^{2^N-1} p(x_k)\log_2 p(x_k) \tag{18}$$

表 2 可以看出，本文获得的值更接近理论值 8。

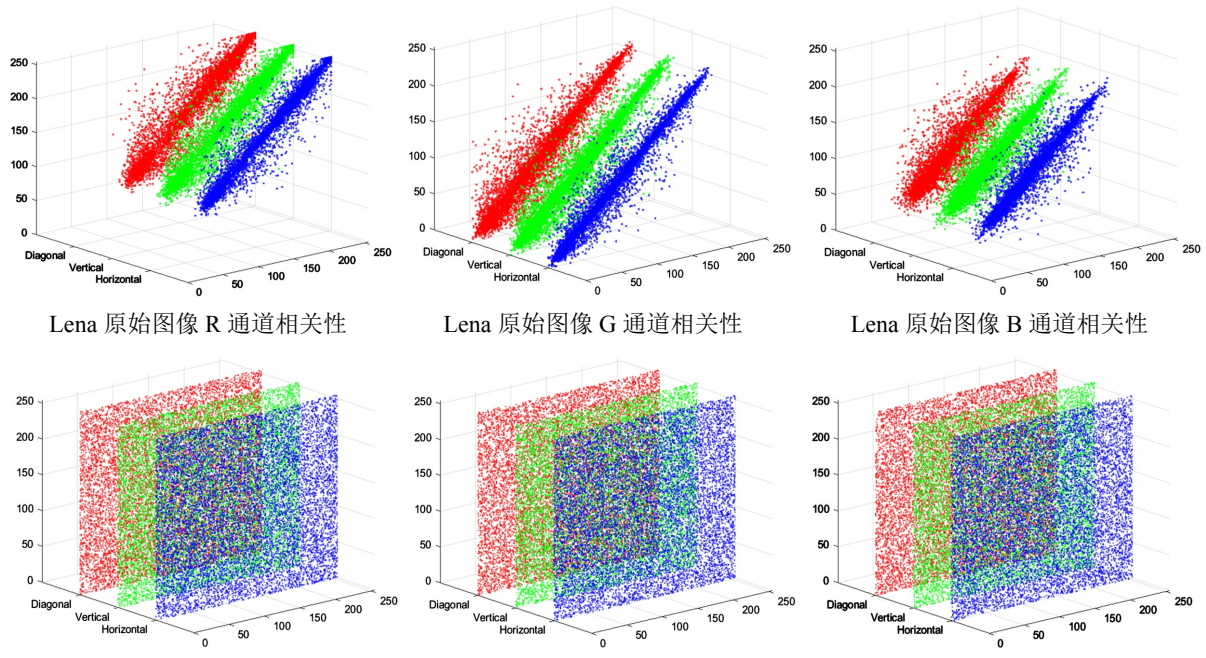
4.5. 相关性分析

在图像中，像素之间普遍存在较高的相关性，尤其是相邻像素在水平方向、垂直方向及对角方向上

的关联程度较强，这种特性在一定程度上增加了图像被分析和破解的风险。通常情况下，原始图像在这三个方向上的相关系数都接近 1，表明像素值变化具有明显的连续性。对于加密图像而言，削弱甚至消除相邻像素间的相关性是评价算法有效性的重要标准。理想状态下，密文图像的像素相关系数应接近 0，以体现高度随机性，尽管在实际应用中完全达到零相关往往难以实现。相关系数可以通过以下式(19)定量计算：

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \\ \operatorname{cov}(x,y) = \dfrac{1}{n}\sum_{k=1}^{n} E\left(x_k - E(x)\right)\left(y_k - E(y)\right) \\ E(x) = \dfrac{1}{n}\sum_{k=1}^{n} x_k \\ D(x) = \dfrac{1}{n}\sum_{k=1}^{n}\left(x_k - E(x)\right)^2 \end{cases} \tag{19}$$

其中 x_k 和 y_k 表示两个相邻像素。n 是像素数。$E(x)$ 和 $D(x)$ 分别表示图像的期望值和方差。在本文中，从明文图像和密文图像中随机选择了 10,000 对相邻像素进行测试，得到了三个通道不同方向上的相关性。明文图像和加密图像的相关性分布如图 3 所示。很明显，明文图像表现出很强的相关性，而密文图像破坏了这些相关性。本文以 Couple、Fruit 和 Lena 彩色图像作为实验对象，将图像加密后的相邻像素点相关性(取绝对值)与与原图的相邻像素点相关性(取绝对值)分别从水平、垂直、对角线三个方向进行对比，结果如表 3 所示。表 3 说明该加密算法将图像相邻像素点的高相关性(接近 1)成功破坏至接近 0 的水平，显著增强了安全性。



Lena 原始图像 R 通道相关性　Lena 原始图像 G 通道相关性　Lena 原始图像 B 通道相关性

Lena 密文图像 R 通道相关性　Lena 密文图像 G 通道相关性　Lena 密文图像 G 通道相关性

Figure 3. Correlation comparison of Lena image R, G, and B channels before and after encryption in different directions
图 3. Lena 图像 R、G、B 三个通道加密前后不同方向上相关性对比

Table 3. Correlation of adjacent pixels (absolute values)
表 3. 相邻像素点相关性(取绝对值)

测试图像	明文			密文		
	水平	垂直	对角线	水平	垂直	对角线
Couple	0.9321	0.9642	0.9057	0.0049	0.0114	0.0001
Fruit	0.9347	0.9648	0.9075	0.0099	0.0164	0.0049
Lena	0.9344	0.9645	0.9073	0.0066	0.0019	0.0080

4.6. 压缩性能分析

峰值信噪比(PSNR)是常用的解密图像质量评价指标，用于对通过正确密钥解密重构图像的质量进行评价。峰值信噪比的计算公式如式(20)所示：

$$\mathrm{PSNR}=10\log_{10}\frac{255\times 255}{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(P_1(i,j)-P(i,j)\right)^2} \tag{20}$$

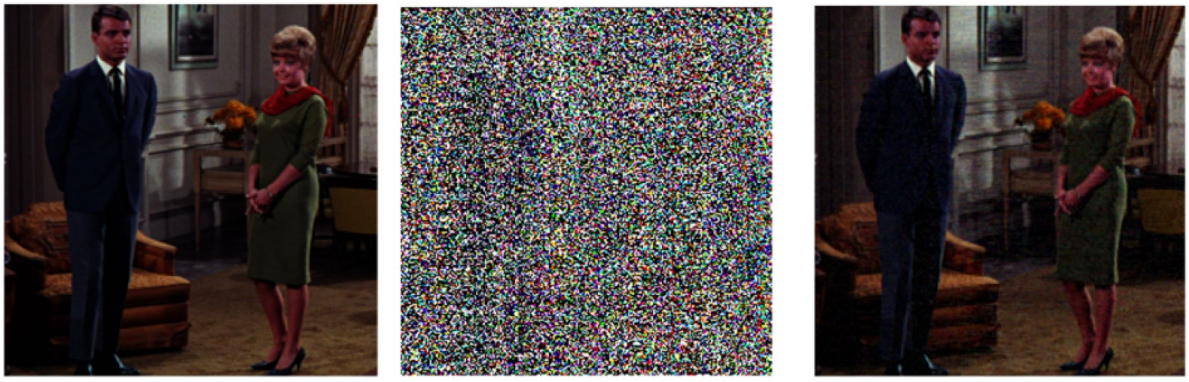
其中，P 和 P_1 是原始图像和重构图像的像素值。峰值信噪比通常以分贝(dB)为单位，通过计算 PSNR 值，可以量化地评估恢复图像的还原质量。PSNR 的计量单位为 dB，其数值越高，意味着经过加密后图像失真度越低，代表恢复图像和明文图像越相似。图为不同压缩率下的 PSNR 值。从表 4 中可以看出，PSNR 值越小，图像失真越大。当压缩比为 85%或 75%时，恢复图像与原始图像基本相同。当压缩比为 50%时，PSNR 值较小，重构后的图像质量在一定程度上可以接受。因此，本文算法具有良好的压缩性能，可以减少在网络中传输的图像负载。

Table 4. PSNR values at different compression ratios
表 4. 不同压缩率下的 PSNR 的值

图像	压缩率	加密图像	解密图像	PSNR
	0.85			33.33
	0.75			32.00
	0.5			27.84

4.7. 密钥敏感性分析

图 4 是将加密“Couple”图片时的密钥之一的由加密时采用的 0.1 在解密时改为 0.1000000000000001，得到的错误密钥下的解密图像。从结果可以看出，密钥仅仅改动了 10^{-16}，但解密后的图像无法复原，展现此算法的极强密钥敏感性。



原图　　错误密钥下的解密图像　　正确密钥下的解密图像

Figure 4. Key sensitivity analysis
图 4. 密钥敏感性分析

5. 结束语

本文提出了一种融合混沌系统、压缩感知与动态 DNA 编码的图像压缩加密方案。该方案首先利用二维离散余弦变换实现图像稀疏表示，并结合由 Logistic 混沌映射生成的测量矩阵完成二维压缩感知测量，在实现数据压缩的同时引入初步加密机制；随后通过 Zigzag 全局索引置乱破坏像素间相关性，并经非线性映射量化后，结合高维混沌系统生成的混沌序列完成扩散操作。进一步地，基于 Logistic 混沌映射与四维超混沌系统构建动态 DNA 编码机制，使 DNA 编码规则和运算方式随混沌序列动态变化，并在 DNA 域与块级之间实现级联扩散，从而显著提升密钥空间规模与扩散强度。最后，通过逆加密过程及重构算法实现图像的有效恢复。实验结果表明，该方法在保持较高压缩效率和良好解密质量的同时，具有较大的密钥空间、较低的像素相关性、均匀的直方图分布以及良好的抗统计攻击和抗暴力破解能力。与传统低维混沌加密方法相比，本文方案结构更加复杂、安全性更高，可为安全高效的图像传输提供一种可行的技术路径。

参考文献

[1] Zhu, L., Jiang, D., Ni, J., Wang, X., Rong, X. and Ahmad, M. (2022) A Visually Secure Image Encryption Scheme Using Adaptive-Thresholding Sparsification Compression Sensing Model and Newly-Designed Memristive Chaotic Map. *Information Sciences*, **607**, 1001-1022. https://doi.org/10.1016/j.ins.2022.06.011

[2] Wang, X., Teng, L., Jiang, D., Leng, Z. and Wang, X. (2023) Triple-Image Visually Secure Encryption Scheme Based on Newly Designed Chaotic Map and Parallel Compressive Sensing. *The European Physical Journal Plus*, **138**, Article No. 156. https://doi.org/10.1140/epjp/s13360-023-03755-2

[3] Alexan, W., Shabasy, N.H.E., Ehab, N. and Maher, E.A. (2025) A Secure and Efficient Image Encryption Scheme Based on Chaotic Systems and Nonlinear Transformations. *Scientific Reports*, **15**, Article No. 31246. https://doi.org/10.1038/s41598-025-15794-z

[4] Wang, S., Sun, B., Wang, Y. and Du, B. (2023) Image Encryption Algorithm Using Multi-Base Diffusion and a New Four-Dimensional Chaotic System. *Multimedia Tools and Applications*, **83**, 10039-10060. https://doi.org/10.1007/s11042-023-16025-1

[5] Hu, L., Chen, M., Wang, M. and Zhou, N. (2024) A Multi-Image Encryption Scheme Based on Block Compressive Sensing and Nonlinear Bifurcation Diffusion. *Chaos, Solitons & Fractals*, **188**, Article ID: 115521. https://doi.org/10.1016/j.chaos.2024.115521

[6] Rohit, Tripathi, S.K., Gupta, B. and Lamba, S.S. (2026) A Companion Matrix and 2D Compressive Sensing Based Efficient Image Encryption Method. *Signal Processing*, **239**, Article ID: 110304. https://doi.org/10.1016/j.sigpro.2025.110304

[7] Yan, X., Wang, X. and Xian, Y. (2021) Chaotic Image Encryption Algorithm Based on Arithmetic Sequence Scrambling

Model and DNA Encoding Operation. *Multimedia Tools and Applications*, **80**, 10949-10983. https://doi.org/10.1007/s11042-020-10218-8

[8] Li, H., Zhang, L., Cao, H. and Wu, Y. (2023) Hash Based DNA Computing Algorithm for Image Encryption. *Applied Sciences*, **13**, Article 8509. https://doi.org/10.3390/app13148509

[9] Patidar, V. and Kaur, G. (2023) A Novel Conservative Chaos Driven Dynamic DNA Coding for Image Encryption. *Frontiers in Applied Mathematics and Statistics*, **8**, Article 1100839. https://doi.org/10.3389/fams.2022.1100839

[10] Zhang, J., Huang, Z., Li, X., Wu, M., Wang, X. and Dong, Y. (2021) Quantum Image Encryption Based on Quantum Image Decomposition. *International Journal of Theoretical Physics*, **60**, 2930-2942. https://doi.org/10.1007/s10773-021-04862-5

[11] Khorrampanah, M., Houshmand, M. and Lotfi Heravi, M.M. (2022) New Method to Encrypt RGB Images Using Quantum Computing. *Optical and Quantum Electronics*, **54**, Article No. 245. https://doi.org/10.1007/s11082-022-03581-3

[12] Mondal, B., Singh, S. and Kumar, P. (2019) A Secure Image Encryption Scheme Based on Cellular Automata and Chaotic Skew Tent Map. *Journal of Information Security and Applications*, **45**, 117-130. https://doi.org/10.1016/j.jisa.2019.01.010

[13] Ping, P., Zhang, X., Yang, X. and Hashems, Y.A.A. (2022) A Novel Medical Image Encryption Based on Cellular Automata with ROI Position Embedded. *Multimedia Tools and Applications*, **81**, 7323-7343. https://doi.org/10.1007/s11042-021-11799-8

[14] Fridrich, J. (1998) Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *International Journal of Bifurcation and Chaos*, **08**, 1259-1284. https://doi.org/10.1142/s021812749800098x

[15] Ahmad, M. and Alam, M.S. (2009) A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping. *International Journal on Computer Science and Engineering*, **2**, 46-50.

[16] 舒永录, 张玉书, 肖迪, 等. 基于置乱扩散同步实现的图像加密算法[J]. 兰州大学学报(自然科学版), 2012, 48(2): 113-116.

[17] Li, C., Xie, T., Liu, Q. and Cheng, G. (2014) Cryptanalyzing Image Encryption Using Chaotic Logistic Map. *Nonlinear Dynamics*, **78**, 1545-1551. https://doi.org/10.1007/s11071-014-1533-8

[18] Ahuja, B. and Doriya, R. (2023) A Secure Algorithm Using High-Dimensional Sine Map for Color Image Encryption. *International Journal of Information Technology*, **15**, 1535-1543. https://doi.org/10.1007/s41870-023-01190-1

[19] Li, Y., Deng, Y., Jiang, M. and Wei, D. (2024) Fast Encryption Algorithm Based on Chaotic System and Cyclic Shift in Integer Wavelet Domain. *Fractal and Fractional*, **8**, Article 75. https://doi.org/10.3390/fractalfract8020075

[20] Chen, J., Zhu, Z., Zhang, L., Zhang, Y. and Yang, B. (2018) Exploiting Self-Adaptive Permutation-Diffusion and DNA Random Encoding for Secure and Efficient Image Encryption. *Signal Processing*, **142**, 340-353. https://doi.org/10.1016/j.sigpro.2017.07.034

[21] Zhu, C., Gan, Z., Lu, Y. and Chai, X. (2019) An Image Encryption Algorithm Based on 3-D DNA Level Permutation and Substitution Scheme. *Multimedia Tools and Applications*, **79**, 7227-7258. https://doi.org/10.1007/s11042-019-08226-4

[22] Donoho, D.L. (2006) Compressed Sensing. *IEEE Transactions on Information Theory*, **52**, 1289-1306. https://doi.org/10.1109/tit.2006.871582

[23] Lu, P., Xu, Z., Lu, X. and Liu, X. (2013) Digital Image Information Encryption Based on Compressive Sensing and Double Random-Phase Encoding Technique. *Optik*, **124**, 2514-2518. https://doi.org/10.1016/j.ijleo.2012.08.017

[24] Huang, R. and Sakurai, K. (2011) A Robust and Compression-Combined Digital Image Encryption Method Based on Compressive Sensing. 2011 *Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Dalian, 14-16 October 2011, 105-108. https://doi.org/10.1109/iihmsp.2011.53

[25] Qiao, L., Mei, Q., Jia, X. and Ye, G. (2024) Image Encryption Scheme Based on Pseudo-DWT and Cubic S-Box. *Physica Scripta*, **99**, Article ID: 085259. https://doi.org/10.1088/1402-4896/ad635d

[26] 张赛男, 李千目. 一种基于 Logistic-Sine-Cosine 映射的彩色图像加密算法[J]. 计算机科学, 2022, 49(1): 353-358.

[27] Teng, L., Wang, X., Yang, F. and Xian, Y. (2021) Color Image Encryption Based on Cross 2D Hyperchaotic Map Using Combined Cycle Shift Scrambling and Selecting Diffusion. *Nonlinear Dynamics*, **105**, 1859-1876. https://doi.org/10.1007/s11071-021-06663-1