基于超混沌系统和压缩感知的图像加密算法

许缓缓[1] 李富余[2]
XU Huanhuan LI Fuyu

摘 要 随着图像数据量的激增，人们对其产生了存储和安全传输的需求。混沌系统因其不可预测的特性及对初始条件的高度敏感性，已成为图像加密领域的关键技术。但提升解密图像质量和提高图像安全性仍是当前亟需解决的问题。因此，文章提出了一种基于超混沌系统和压缩感知的图像加密算法，采用先加密后压缩的模式。首先，对二维灰度图像进行行列置乱，交换整行整列元素的位置；然后，进行扩散处理，在不改变像素位置的前提下，将任意明文像素的信息尽可能分散隐藏到多个加密图像像素中；最后，对得到的加密图像进行采样得到压缩图像。此外，混沌系统的参数均采用 SHA-512 安全哈希算法生成，增强加密效果。实验结果与性能分析证实了该图像加密方案的可行性和可靠性，在压缩性能、抗统计攻击能力和抗差分攻击性方面展现出显著优势。

关键词 混沌系统；压缩感知；图像加密；安全性分析

doi：10.3969/j.issn.1672-9528.2026.03.035

0 引言

随着信息技术的持续发展，自媒体终端和智能设备已得到广泛应用。这些设备让人们能够轻松获取图片或视频，并通过微信、抖音等应用程序进行网络分享。虽然这种传播方式为人们提供了表达喜怒哀乐、分享信息的渠道，但也伴随着隐私泄露、图片篡改等风险与挑战，甚至可能成为不法分子的可乘之机[1-2]，特别是涉密的影像资料，一旦泄露，可能引发难以估量的后果。因此，图像安全防护已成为当前重点研究领域[3]。

图像加密是图像安全领域的关键技术。目前该领域主要分为三大类：混沌理论[4-5]、神经网络[6]和密码编码[7-8]。其中，混沌系统因其不可预测的特性及对初始条件的高度敏感性，已成为研究热点。典型的混沌图像加密算法包含置换与扩散两个阶段，通常需要经过多轮迭代处理。在每轮迭代中，数据首先通过密钥控制的置换操作进行排列，随后执行扩散操作——这种设计能确保每个输入位的变化都能影响尽可能多的扩散像素值，将排列后的数据扩散到更广的区域，从而弥补现有方案在加密容量、重建质量及安全性方面的不足。为此，文献 [4] 利用改进的约瑟夫算法进行置乱，利用三维混沌系统映射生成初始值，再通过扩散处理图像，以增加安全性。文献 [5] 提出了一种基于块压缩感知和新型整数混沌系统的图像加密方案，在压缩时减少了嵌入式设备的工作量。但现有方案存在一个短板——缺乏有效手段降低图像数据量，导致存储和传输负担加重。在实际应用中，设备资源有限往往使得传统信号采集与保护策略难以满足需求。因此，基于压缩感知的图像加密方案成为信息安全领域的关键技术之一。

1. 安顺职业技术学院信息工程系 贵州安顺 561000
2. 花旗金融信息服务（中国）有限公司 上海 201203

1 算法基础

1.1 混沌系统

在图像加密领域，超混沌洛伦兹系统是一种被广泛应用的混沌系统，它通过引入高维非线性动力学实现了更强的混沌行为。该系统在经典洛伦兹系统基础上引入了第四维变量，其数学模型可描述为：

$$\begin{cases} \dot{x} = a(y - x) + w \\ \dot{y} = cx - y - xz \\ \dot{z} = xy - bz \\ \dot{w} = -yz + rw \end{cases} \tag{1}$$

当参数设置为 a= 10、b = 83、c = 28 且 $r\in$ [−1.52, −0.06] 时，该系统呈现超混沌行为。该系统的动力学特性取决于 r 的取值：当 r = −1 时，式（1）至少产生两个正的李雅普诺夫指数。此类动力学行为通常通过相位图和李雅普诺夫指数谱进行分析。李雅普诺夫指数定量表征混沌特征——正值表示混沌动力学，负值则表示稳定状态。

1.2 压缩感知

压缩感知理论证明，稀疏信号可以通过亚奈奎斯特采样率下获取的测量值精确重构。在编码阶段，对于 K 稀疏信号 $\boldsymbol{x}\in\mathbf{R}^{N\times1}$，可以通过测量矩阵 $\boldsymbol{\Phi}\in\mathbf{R}^{M\times N}$（其中 $M\times N$）获得 M

维测量值。压缩感知中的采样过程用数学模型描述为：

$$\boldsymbol{y}=\boldsymbol{\Phi x}=\boldsymbol{\Phi\Psi}s=\boldsymbol{\Theta}s \tag{2}$$

式中：$\boldsymbol{y}\in\mathbf{R}^{N\times1}$ 表示测量值；$\boldsymbol{\Psi}\in\mathbf{R}^{N\times M}$ 表示正交变换基；$\boldsymbol{\Theta}=\boldsymbol{\Phi\Psi}$ 表示传感矩阵。压缩感知中的恢复过程涉及在获取测量值 $\boldsymbol{y}$ 后，于解码端重建原始信号 $\boldsymbol{x}$。通过求解优化问题获得稀疏解 s 来实现，用公式表示为：

$$\begin{aligned}&\min\|s\|_1\\&\text{s.t.}\quad \boldsymbol{y}=\boldsymbol{\Phi\Psi}s\end{aligned} \tag{3}$$

式中：$\|\cdot\|_1$ 表示 L_1 范数。

研究表明，非凸的 L_0 范数可以通过 L_1 范数进行近似。

2 基于混沌系统和压缩感知的图像加密算法

本节详细阐述了所提出的加密方案的算法工作流程。通过利用超混沌 Lorenz 系统在图像加密中的固有特性，该方法通过扩展密钥空间和提升计算复杂度来增强安全性。整个框架包含 3 个核心阶段：密钥生成、加密处理和解密处理，如图 1 所示。

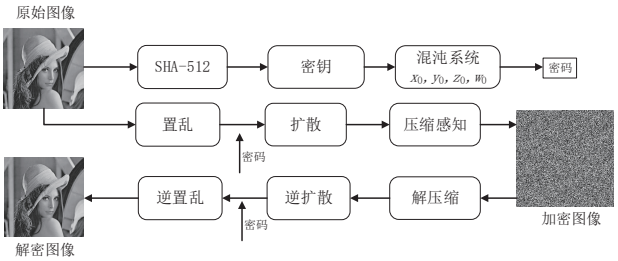


图 1 提出的图像加密方法的整体框架图

2.1 混沌序列生成

使用超混沌系统生成随机序列时，初始值由 SHA-512 哈希函数生成，如式（1）所示。在提出的方案中，超混沌系统的离散化形式可表示为：

$$\begin{cases}x_{n+1}=x_n+\dfrac{\sum_{i=1}^{4}K_{ix}}{6}\\[2ex]y_{n+1}=y_n+\dfrac{\sum_{i=1}^{4}K_{iy}}{6}\\[2ex]z_{n+1}=z_n+\dfrac{\sum_{i=1}^{4}K_{iz}}{6}\\[2ex]w_{n+1}=w_n+\dfrac{\sum_{i=1}^{4}K_{iw}}{6}\end{cases} \tag{4}$$

系统变量的初始值为：$x_0=K(1)$，$y_0=K(2)$，$z_0=K(3)$，$w_0=K(4)$。

2.2 加密阶段

超混沌 Lorenz 系统包含多重混杂与扩散机制。在二维图像的行列混杂处理中，需要对整行或整列元素进行位置交换。具体流程分为三个步骤：

首先将二维图像展开为一维向量，接着采用随机混杂算法实现元素位置互换，最后将经过混杂处理的一维向量重新组合成二维图像矩阵。对二维图像进行行或列混淆需要 $M+N$ 个随机数，而展开成一维向量后再进行混淆则需 $M\times N$ 个随机数。具体实现细节为将二维图像矩阵 $\boldsymbol{P}$ 按行或列展开为一维向量 $\boldsymbol{A}$ 后，使用超混沌算法生成长度为 MN 的伪随机序列 X_i。在 Lorenz 系统中，当 $i=1, 2, \cdots, M\times N$ 时，系统仅保留 X 中首次出现的重复伪随机序列，并将集合 $1, 2, \cdots, M\times N$ 中未出现在 X 中的数值按升序添加到 X 的末尾。最后，交换 $\boldsymbol{A}(X_i)$ 和 $\boldsymbol{A}(X_{M\times N-i}+1)$ 的位置。

在图像加密系统中，扩散处理是一项关键技术。它能在不改变像素位置的前提下，将明文像素的信息尽可能多地隐藏到密文像素中。扩散过程包含正向扩散和逆向扩散两个阶段。具体来说，明文图像被扩展为一维向量 $\boldsymbol{P}$，对应的密文也是一维向量 $\boldsymbol{C}$；其中 $\boldsymbol{S}$ 表示加密向量，i 的取值范围为 $1\sim M\times N$。初始值 $\boldsymbol{C}_0$ 由密钥生成：

$$\begin{cases}\boldsymbol{C}_1=\boldsymbol{C}_0\oplus\boldsymbol{S}_1\\\boldsymbol{C}_2=\boldsymbol{C}_0\oplus\boldsymbol{S}_1\oplus\boldsymbol{S}_2\oplus\boldsymbol{P}_1\\\boldsymbol{C}_3=\boldsymbol{C}_0\oplus\boldsymbol{S}_1\oplus\boldsymbol{S}_2\oplus\boldsymbol{S}_3\oplus\boldsymbol{P}_1\oplus\boldsymbol{P}_2\oplus\boldsymbol{P}_3\\\boldsymbol{C}_4=\boldsymbol{C}_0\oplus\boldsymbol{S}_1\oplus\boldsymbol{S}_2\oplus\boldsymbol{S}_3\oplus\boldsymbol{S}_4\oplus\boldsymbol{P}_1\oplus\boldsymbol{P}_2\oplus\cdots\oplus\boldsymbol{P}_4\end{cases} \tag{5}$$

可以看出，明文图像中像素 $\boldsymbol{P}_1$ 的信息通过异常操作扩散到密文的所有像素中。$\boldsymbol{P}_2$ 的信息通过异常操作扩散到密文的 $\boldsymbol{C}_2\sim\boldsymbol{C}_{M\times N}$ 中，$\boldsymbol{P}_{M\times N}$ 的信息将隐藏在 $\boldsymbol{C}_{M\times N}$ 中。

将扩散后的图像进行采样。初始一个 $\boldsymbol{F}\in\mathbf{R}^{M\times N}$ 模板矩阵，$\boldsymbol{p}^t\in$ 为 $\boldsymbol{P}$ 的映射版本。应用压缩感知对图像 $\boldsymbol{P}$ 的映射版本进行采样：

$$\boldsymbol{Y}^t=\text{Phi1}\,\boldsymbol{p}^t\,\text{Phi2}^T=\boldsymbol{Y}-\boldsymbol{Y}_F \tag{6}$$

式中：$\boldsymbol{Y}\in\mathbf{R}^{M\times N}$，$\boldsymbol{Y}^t\in\mathbf{R}^{M\times N}$ 和 $\boldsymbol{Y}_F\in\mathbf{R}^{M\times N}$ 分别表示 $\boldsymbol{P}$、$\boldsymbol{P}_t$ 和 $\boldsymbol{F}$ 的二维测量值。将二维测量值量化到区间 [0, 255]，得到压缩图像。

2.3 解密阶段

解密算法是加密算法的逆过程，这里将替换和扩散结合起来，即同时改变像素的位置和灰度值，使任意像素的灰度信息尽可能多地隐藏在其他像素中，然后进行压缩感知，提高图像的安全性的同时减轻传输负担。

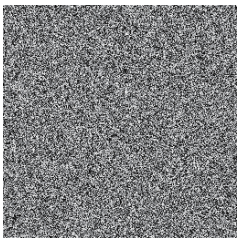
3 实验结果与分析

为验证本文算法的有效性，所有实验是在 2.5 GHz CPU、16 GB 内存、Windows 10 操作系统和 MATLAB R2018b 配置下完成。本文使用“Lena”，256 px×256 px 经典测试图像。同时，实验对密钥空间分析、信息熵、相关系数、直方图分析等性能指标进行综合评估。

3.1 加密和解密效果评估

仿真结果如图 2 所示，加密后的图像没有任何视觉信息，解密图像和原始图像在视觉上没有区别，说明所提加密算法具有较好的安全性，不会影响图像的后续使用。


（a）Lena 原始图像


（b）Lena 加密图像

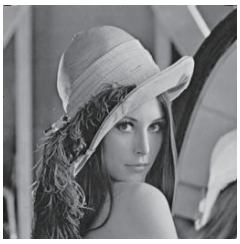

（c）Lena 解密图像

图 2 所提加密算法的仿真结果

3.2 密钥空间分析

密钥空间指所有有效加密密钥的集合。为确保所提出的加密方案具备强大的安全性，能有效抵御暴力攻击，使其在当前计算能力下难以实施。这需要足够大的密钥空间来抵御穷举搜索攻击。本算法中的密钥由超混沌系统的初始值构成，即 $K=\{x_0, y_0, z_0, w_0\}$，其中 x_0、y_0 和 z_0 的步长设为 10^{-13}，w_0 的步长设为 10^{-12}。因此密钥空间规模约为 $2.56\times10^{59}\approx2^{197}$，相当于 197 比特的密钥长度，足以抵御穷举攻击，增大暴力破解难度。

3.3 信息熵

信息熵表示加密图像 I_i 的随机性和不可预测性，反映密文图像的信息不确定性。对于 256 灰度级图像，理想熵值为 8 比特 / 像素，表明所有灰度值出现概率均等，密文信息完全随机，其表达式为：

$$H(I)=-\sum_{i=0}^{n}P(I_i)\log_2 P(I_i) \tag{7}$$

式中：$P(I)$ 表示符号 I 的出现概率，由此计算出 Lena 原始图像的信息熵值为 6.870 1，通过加密算法加密后。加密图像的信息熵值为 7.999 6，该值非常接近理想值 8，说明加密过程中的信息泄露最小，因此该方案能有效抵抗基于信息熵的攻击。

3.4 相关系数分析

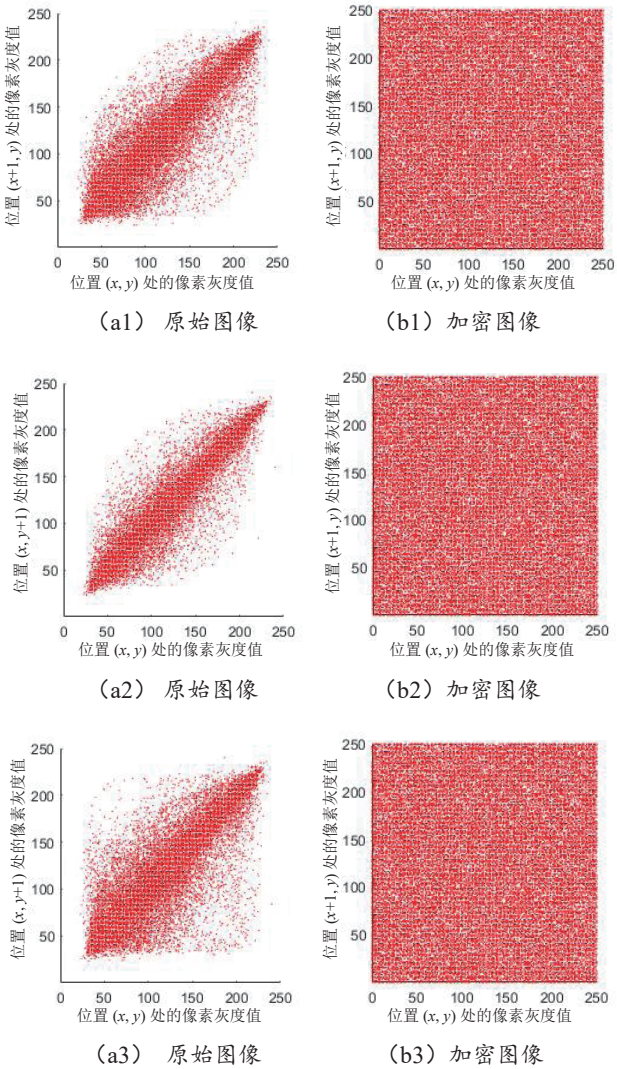
为防止窃听者进行统计分析，加密图像中相邻像素间的相关性应保持较低。在评估像素相关性时，采用相关系数对原始图像和加密图像中的水平、垂直及对角线相邻像素对进行分析。其计算公式可表示为：

$$\mathrm{CC}_{xy}=\frac{E\left(\left(x-E(x)\right)\left(y-E(y)\right)\right)}{\sqrt{D(x)D(y)}} \tag{8}$$

式中：$E(x)$ 和 $D(x)$ 分别表示灰度值 x 的期望值（均值）和方差。本算法从每幅图像中选取 5 000 对相邻像素，计算其水平、垂直、对角方向的相关系数。如表 1 和图 3 所示，可以看到：明文图像中的相邻像素表现出强相关性，而密文图像中的相邻像素则呈现近乎零的相关性。理论上两个独立随机序列之间的相关系数应为 0。而通过本方案加密后，密文图像在所有方向上都显示出极其微弱的相关性，在表 1 的数据中也得到印证。因此，能够证明所提出的方法具备抵御统计攻击的安全性。

表 1 原始图像和加密图像的相邻像素的相关系数

图像	水平方向	垂直方向	对角方向
原始图像	0.943 3	0.918 7	0.882 3
加密图像	0.002 4	0.003 2	−0.009 1



（a1） 原始图像　（b1）加密图像

（a2） 原始图像　（b2）加密图像

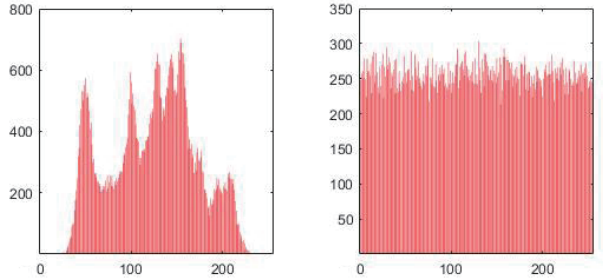
（a3） 原始图像　（b3）加密图像

图 3 图像在水平、垂直和对角方向上相邻像素的分布图

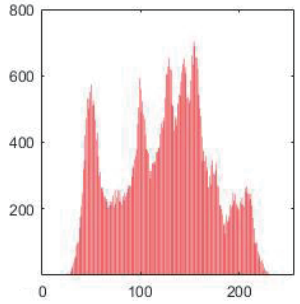
3.5 直方图分析

图像直方图直观呈现像素分布特征。对于加密图像而言，加密算法应能生成均匀分布或相近的直方图形态，这种特性

可有效阻止攻击者通过统计分析破解原始图像。图 4 展示了 256 px×256 px 量级的原始图像及其对应加密图像的直方图对比。实验结果表明：明文图像的直方图具有特定分布特征，而密文图像的直方图则呈现均匀分布状态，充分说明攻击者难以从密文图像中获取有效统计信息。



（a）原始图像　　（b）加密图像



（c）解密图像

图 4 图像加密和解密图像的直方图

3.6 密钥敏感性分析

安全图像加密算法必须对密钥保持高度敏感性。本章以灰度图像 Lena 为测试对象，采用像素改变率（NPCR）和统一平均变化强度（UACI）两项指标，系统评估密钥微小改动对加密图像的影响。该指标可通过公式推导得出：

$$\begin{cases} \mathrm{NPCR} = \frac{1}{M\times N}\sum_{i,j} D(i,j) \times 100\% \\ D(i,j) = \begin{cases} 1, C_1(i,j) = C_2(i,j) \\ 0, C_1(i,j) \neq C_2(i,j) \end{cases} \end{cases}$$

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%\right] \quad (9)$$

式中：C_1 和 C_2 表示两个加密图像；M 和 N 表示加密图像的高度和宽度。值得一提的是，NPCR 和 UACI 的理想值分别为 99.61% 和 33.46%。实验结果表明，本文提出的多图像加密方法具有显著的明文敏感性和出色的抗差分攻击能力。

表 2 加密图像的 NPCR 和 UACI

图像	NPCR	UACI
加密图像	0.996 2	0.334 5

这里，对像素值进行稍微修改以评估密钥敏感性的 NPCR 和 UACI，结果如表 2 所示。从结果可以看出，NPCR 和 UACI 接近理想值 99.61% 和 33.46%，这表明所提出的方法是密钥敏感的。

4 结语

本文提出了一种基于超混沌系统和压缩感知的加密方案。该方案创新性地将随机置乱与扩散方法相结合，能快速降低相邻像素间的相关性，并通过压缩感知进行采样、加密、压缩，在增强安全性的同时满足减轻传输压力的要求。实验结果表明，该方案具有优异的安全性能，可有效抵御暴力攻击、差分攻击和统计攻击，为医学影像隐私数据提供可靠保护。未来研究值得探索将 DNA 与量子计算技术融入混沌系统，并关注多模态数据加密，从而构建更完善且易于落地的加密生态系统。

参考文献：

[1] 王斌 . 混合云环境下重要数据多层加密研究 [J]. 信息技术与信息化 ,2025(7):113-116.

[2] 赵治斌 , 冯黎 . 并行属性基加密技术下物联网隐私数据安全共享算法 [J]. 信息技术与信息化 ,2025(4):158-161.

[3] 王星垚 , 丁海洋 . 基于分组密码的加密域图像可逆信息隐藏算法研究与实现 [J]. 信息技术与信息化 ,2024(9):190-196.

[4] 丁元明 , 朱安迪 , 冯建新 . 基于约瑟夫置乱和三维混沌的图像加密算法 [J]. 计算机仿真 ,2025,42(3):226-230.

[5] 范海菊 , 岳爽 , 窦育强 , 等 . 基于新型混沌系统和二进制块压缩感知的图像加密算法 [J/OL]. 计算机科学 ,1-16[2025-07-31].https://link.cnki.net/urlid/50.1075.TP.20250307.1118.004.

[6] 秦学姣 , 章庆勇 , 黄炜 , 等 . 惯性神经网络的固定 / 指定时间同步及在医学图像加密中的应用 [J]. 现代信息科技 , 2025, 9(6):89-92.

[7] 唐亦昕 , 张英男 . 基于 SM2 和 DNA 的图像加密算法 [J]. 陕西科技大学学报 ,2025,43(1):203-210.

[8] 邓文博 , 刘帅 , 刘福才 , 等 . 基于压缩感知和 DNA 编码的图像加密算法 [J]. 计算机工程与科学 ,2022,44(9):1574-1582.

【作者简介】

许缓缓（1987—），女，河南永城人，硕士研究生，讲师，研究方向：图像加密、计算机视觉。

李富余（1989—），女，河南夏邑人，硕士研究生，高级软件工程师，研究方向：大数据开发。

（收稿日期：2025-08-27　修回日期：2026-03-09）