资源受限环境下面向多用户分级安全的图像加密算法

朱礼亚[1,2]，牟欣语[1]，普京[1]，闫茂德[1,2]，蒋东华[3]

（1. 长安大学电子与控制工程学院，710064，西安；
2. 长安大学西安市智能高速公路信息融合与控制重点实验室，710064，西安；
3. 中山大学计算机科学与工程学院，510006，广州）

摘要：为有效解决资源受限环境下不同权限等级用户的差异化隐私保护问题，提出了一种结合图像频率分类和分块压缩感知的图像加密算法。首先，将明文图像分块后进行离散余弦变换（DCT），利用 Zigzag 扫描将各图像块的 DCT 系数矩阵转换为包含不同频率分量的向量，完成频率分类；其次，提出了考虑图像特征的自适应阈值稀疏化方法，针对不同频率进行阈值稀疏化处理；再次，设计并利用改进的二维混沌系统构造测量矩阵，对各频率分量分别进行压缩测量，将测量结果重组后经过二次加密生成密文图像；最后，不同权限等级的用户利用对应的密钥获得差异化的解密图像，从而实现基于权限等级的图像信息分级保护。研究结果表明：该算法可为高、中、低 3 个权限等级用户提供具有显著差异的解密图像。在保证安全性的同时，压缩性能提升约 7～12 dB，时间开销减少了 38%以上，处理效率显著提高。所提算法适用于资源受限环境下的图像快速处理，能够有效实现面向多用户的图像安全分级保护。

关键词：图像加密；二维混沌系统；分级保护；压缩感知；自适应阈值稀疏化

中图分类号：TP391 **文献标志码**：A

DOI：10.7652/xjtuxb202604020 **文章编号**：0253-987X(2026)04-0239-11

An Image Encryption Algorithm for Multi-User Hierarchical Security in Resource-Constrained Environments

ZHU Liya[1,2], MU Xinyu[1], PU Jing[1], YAN Maode[1,2], JIANG Donghua[3]

(1. School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China;
2. Xi'an Key Laboratory of Smart Expressway Information Fusion and Control, Chang'an University, Xi'an, 710064, China;
3. School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China)

Abstract: To effectively address the issue of differentiated privacy protection for users with different authorization levels in resource-constrained environments, an image encryption algorithm integrating image frequency classification and block compressed sensing is proposed. First, the plaintext image is divided into blocks, and each block is transformed via the discrete cosine transform (DCT). Using Zigzag scanning, the DCT coefficient matrix of each image block is converted into a vector containing different frequency components, thereby completing frequency classification. Second, an adaptive threshold sparsification method that accounts for image characteristics is proposed to

收稿日期：2025-08-03。 作者简介：朱礼亚(1980—)，男，高级工程师，硕士生导师。 基金项目：国家自然科学基金资助项目(62372062)；长安大学中央高校基本科研业务费专项资金资助项目(300102325501)。
网络出版时间：2025-10-15 网络出版地址：https://link.cnki.net/urlid/61.1069.T.20251014.1849.004

perform sparsification on different frequency components according to varying thresholds. Third, an improved two-dimensional chaotic system is designed and used to construct a measurement matrix. Each frequency component is then measured separately via compressed sensing, after which the measurement results are reorganized and subjected to secondary encryption to generate the cipher image. Finally, users with different permission levels obtain differentiated decrypted images using corresponding keys, thereby achieving hierarchical protection of image information based on access rights. Experimental results show that the proposed algorithm can provide decrypted images with clearly distinguishable quality for users at high, medium, and low permission levels. While ensuring security, the compression performance is improved by approximately 7—12 dB, the time cost is reduced by more than 38%, and processing efficiency is significantly enhanced. The proposed algorithm is suitable for fast image processing in resource-constrained environments and can effectively achieve hierarchical image security protection for multiple users.

Keywords: image encryption; two-dimensional chaotic map; hierarchical protection; compressive sensing; adaptive-thresholding sparsification

随着通信系统和云存储技术的迅速发展，图像传输与存储中的安全问题日益凸显。包含隐私信息的图像一旦被非法访问，可能导致信息泄露、数据篡改等风险，严重威胁个人隐私、企业利益甚至国家安全。因此，图像隐私保护具有重要的研究意义。

为应对这一挑战，研究者提出了多种隐私保护方法，包括信息隐藏[1]、数字水印[2]和图像加密[3]等。其中，基于混沌理论的加密方法因其初值敏感性和伪随机性而受到广泛研究。文献[4]利用Henon映射生成伪随机序列提升安全性；文献[5]对一维记忆混沌进行改进，以进一步提高混沌映射的不可预测性。近年来，研究者们将压缩感知技术与混沌系统相结合，实现图像的同步加密和压缩[6]。已有的研究主要围绕算法的安全性、压缩性能和效率展开。例如，引入哈希函数[7]和计数器机制[8]，增强抵御已知明文和选择明文攻击的能力；对明文图像稀疏系数进行置乱和阈值化处理，改善压缩性能[9]；采用分块压缩感知(BCS)框架，提高算法的执行效率等[3]。

对解密方而言，上述方法均呈现出全有或全无的输出结果，难以满足分布式、多用户场景下的差异化访问需求。现有的图像分级加密算法主要分为两类。一类是针对图像感兴趣区域(ROI)的局部差异化分级方法，即通过对图像中不同区域实施差异化处理，使得高权限用户可访问包含隐私信息的敏感区域，而低权限用户仅能获取非敏感区域图像。文献[10]提出了1种面向社交媒体的人脸隐私分级保护框架，使不同权限用户可访问对应等级的人脸特征信息；文献[11]则对交通图像中的各区域进行重要性划分，实现了基于区域级别的访问控制。

另一类是面向整幅图像的渐进式分级保护方法，即通过逐步提升图像重建质量满足不同权限用户的差异化访问需求。文献[12]利用秘密图像共享技术，将影子图像分发给不同用户，用户获得的影子图像数越多，恢复的图像质量越高。文献[13]引入并行压缩感知(PCS)，将压缩图像分为多个子块后分发，通过多用户聚合完成图像的渐进式重建。

由以上分析可知：第一类方法是以区域化访问控制为特征的分级隐私保护；第二类方法则利用秘密载体的数量差异实现渐进式重建。考虑到许多应用场景的资源受限，在确保多用户分级访问控制的前提下，如何平衡安全性、压缩性能和运行效率，是图像分级安全加密算法需要重点研究的问题。

因此，本文将图像频率分类与分块压缩感知相结合，提出了一种面向资源受限环境的图像分级安全加密算法，其创新点包括：①在BCS框架下，对图像的离散余弦变换(DCT)系数分类后分别压缩，利用低频与高频分量的差异，结合分级密钥分发体系，确保不同权限用户获取差异化的解密图像；②改进Henon混沌映射以提升混沌特性，并用于构造受控测量矩阵，有效实现算法安全性与计算效率的平衡；③优化了与图像特征相适应的阈值稀疏化方法，进一步提升了算法的压缩性能。研究结果表明：本文所提算法能够在实现多用户分级访问控制的同时，有效平衡算法的安全性、压缩性能和运行效率，为资源受限场景下的图像分级隐私保护提供有效的解决方案。

1　混沌理论

1.1　Henon 混沌映射

作为一种典型的二维离散混沌映射，Henon 映射的系统方程为

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

式中：x_n、y_n 分别为状态变量；n 为迭代次数；a 和 b 为控制参数，当 $a = 1.4$、$b = 0.3$ 时，系统进入混沌状态。

由 Henon 映射的分岔图、吸引子轨迹和李雅普诺夫指数图分析可得，其动力学特性存在以下几点局限性：①混沌行为仅出现在有限的参数范围内；②混沌轨迹结构单一；③最大李雅普诺夫指数趋近于 0，系统的混沌复杂度有限。

1.2　改进型二维混沌映射

针对 Henon 混沌映射的局限性，本文对其进行改进，即在式(1)中引入二次非线性项以增强复杂性，并结合三角函数实现有界的周期调制。此外，还通过模运算以保证状态变量的有界性。本文提出的改进型 Henon 映射(2D-IHCM)的系统方程为

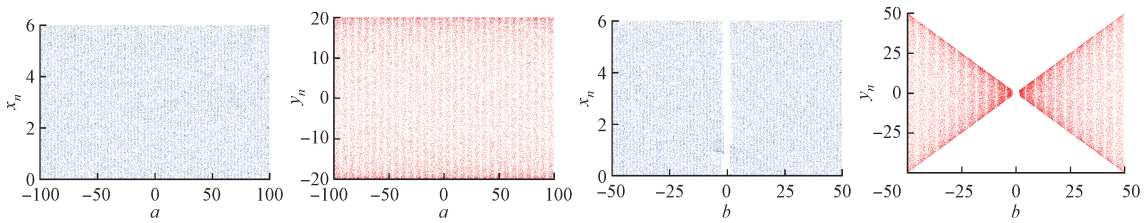
$$\begin{cases} x_{n+1} = (1 + ay_n - by_n^2) \bmod 2\pi \\ y_{n+1} = b\cos(x_n) \end{cases} \tag{2}$$

式中：$x_n, x_{n+1} \in (0, 6\pi)$，$y_n, y_{n+1} \in (-20, 20)$；mod 为取模运算。本文算法中，2D-IHCM 用于构建测量矩阵。

1.3　改进混沌映射的性能分析

1.3.1　分岔图

图 1 为 2D-IHCM 的分岔图。当参数满足 $(x_0, y_0) = (0.1, 0.2)$ 且 $b = 20$ 时，2D-IHCM 在 $a \in [-100, 100]$ 内呈现出典型的满映射特征，验证了其稳定的混沌特性。当 $a = 10$ 且 $b \in [-50, 50]$ 时，系统仅在有限范围内表现出周期性行为。



(a)$b=20$，x 分岔图　(b)$b=20$，y 分岔图　(c)$a=10$，x 分岔图　(d)$a=10$，y 分岔图

图 1　改进型 Henon 混沌映射的分岔图

Fig. 1　Bifurcation diagram of the improved Henon chaotic map

1.3.2　香农熵

香农熵量化了序列的随机性和信息含量[8]。混沌系统生成的混沌序列越无序，相应的香农熵越高；反之香农熵越低。图 2 对比了文献[14-16]中所提二维混沌系统和本文所提 2D-IHCM 系统的香农熵。

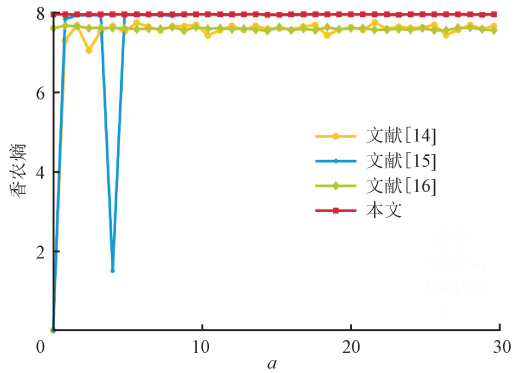


图 2　本文和文献香农熵的对比

Fig. 2　Comparison between this paper and the literatures on Shannon entropy

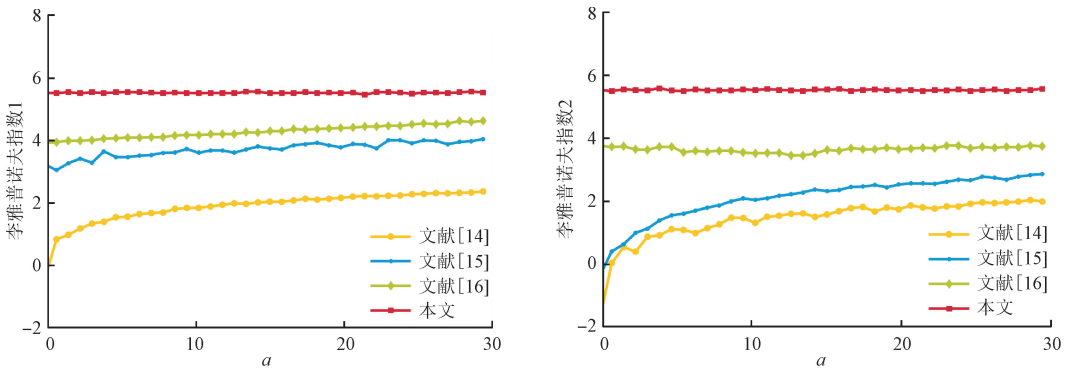
由图 2 可知，2D-IHCM 的香农熵始终大于 0，并且更高，这表明其生成序列具有更强的随机性。同时，在整个参数区间内，该映射的熵值始终维持在稳定的波动范围内，体现出更可靠的混沌稳定性。

1.3.3　李雅普诺夫指数

李雅普诺夫指数是表征混沌系统动力学特性的重要方法。对于一个 N 维混沌系统，存在 N 个对应的李雅普诺夫指数。将本文 2D-IHCM 与文献[14-16]中所提二维混沌映射的李雅普诺夫指数进行比较，结果如图 3 所示。由图可知，2D-IHCM 的李雅普诺夫指数始终为正且更大，表明其具有更复杂的混沌特性。

1.3.4　NIST SP800-22 测试

本小节采用 NIST SP800-22 标准统计测试套件，对 2D-IHCM 映射生成的二进制序列进行评估[14]，各子项的测试结果如表 1 所示。其中，P 为判断被测序列是否具有随机性的指标。



(a)李雅普诺夫指数谱 1 (b)李雅普诺夫指数谱 2

图 3 本文与文献李雅普诺夫指数的对比

Fig. 3 Comparison between this paper and the literatures on Lyapunov exponent spectra

表 1 NIST 随机性测试实验数据

Table 1 Experimental data of NIST randomness test

测试项目	P	结果
近似熵检验	0.986 04	通过
分块频数检验	0.951 87	通过
前向累积和测试	0.922 43	通过
后向累积和测试	0.890 51	通过
离散傅里叶变换测试	0.600 92	通过
频数检验	0.811 88	通过
线性复杂性检验	0.751 83	通过
最长游程检验	0.998 84	通过
非重叠模板检验	0.812 82	通过
重叠模板检验	0.866 71	通过
随机游动检验	0.959 00	通过
随机游动状态频数检验	0.871 10	通过
二元矩阵秩检验	0.645 41	通过
游程检验	0.687 77	通过
序列检验	0.967 52	通过
线性复杂性检验	0.939 29	通过
通用统计检验	0.800 31	通过

由表中可知，本文所提的 2D-IHCM，其生成序列的所有测试项的 P 均显著高于预设的显著性水平($\alpha=0.01$)。因此，2D-IHCM 生成的序列通过全部 NIST 随机性检验，验证了其良好的伪随机特性。

2 图像分级加密算法

本文结合图像频率分类和分块压缩感知，融合 2D-IHCM 和自适应阈值稀疏化，提出了一种高效的图像分级加密算法，加密过程如图 4 所示，其中，k 为控制参数。首先，对明文图像分块，对各图像块的 DCT 系数进行分类与置乱；其次，对图像块的各频率分量分别进行压缩，并结合自适应阈值稀疏化提升压缩性能；最后，组合压缩块并进行二次加密，生成类噪声密文。此外，加密过程引入基于计数器的参数扰动机制动态更新密钥，以增强安全性。

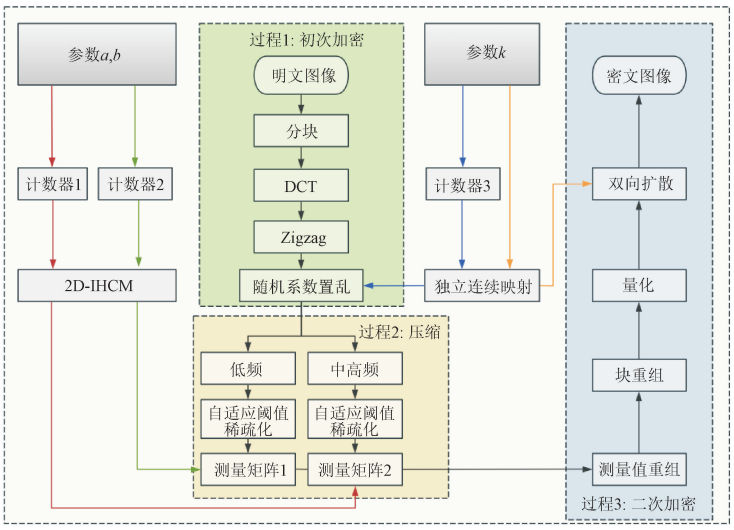


图 4 图像分级加密算法流程图

Fig. 4 Flowchart of image grading encryption algorithm

2.1　算法设计思路

2.1.1　基于频率分类的分级压缩

分块压缩感知是将原始图像分为若干不重叠的图像块后分别进行测量。测量矩阵 $\boldsymbol{\Phi}$ 的表达式为

$$\boldsymbol{\Phi}=\begin{bmatrix}\boldsymbol{\Phi}_1 & 0 & \cdots & 0\\ 0 & \boldsymbol{\Phi}_2 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & \boldsymbol{\Phi}_i\end{bmatrix} \tag{3}$$

式中：i 表示第 i 个图像块。该方法可对各图像块进行并行处理，但未能充分考虑自然图像不同区域的特征差异和非均匀稀疏特性，导致重建性能受限。

因此，本文提出一种基于图像频率分类的分级压缩方法。根据各频段的不同特性实施差异化采样，其思路为，承载图像基本结构信息的低频分量，采用较高压缩率采样，而反映图像细节的高频分量则采用较低压缩率采样。该方法能够在保留 BCS 较高效率的同时，有效实现基于身份的访问控制。

压缩过程首先是对图像块进行 DCT 变换，并通过 Zigzag 扫描对 DCT 系数进行从低频到高频的排序，随后采用随机系数置乱(CRP)方法[17]对其进行置乱，以消除空间相关性并优化稀疏分布。

置乱过程中的随机序列由 ICM 映射[18]生成，其系统方程为

$$x_{n+1}=\cos(((4+k)\pi-k\sin(\pi x_n))\arccos(x_n)) \tag{4}$$

当控制参数 $k\in[0,4]$时，系统为混沌状态。

置乱完成后，将重排序的系数分为低频(LF)和中高频(MHF)两个部分。再利用不同的压缩率分别进行压缩，从而实现针对用户权限等级的差异化访问。其中，低权限用户仅能获取 MHF 分量，重建结果仅保留基本轮廓；中等权限用户可获得 LF 分量访问权，重建图像具有较完整结构但细节模糊；高权限用户则可获取全部频率分量信息，实现对图像的完整重建。

2.1.2　基于自适应阈值的稀疏化方法

在压缩感知过程中，通常采用固定阈值对信号进行稀疏化处理。然而，该方法未能充分考虑图像不同区域的特征差异性，同时也可能导致冗余信息的过保留或关键细节的丢失。

因此，文献[9]提出一种基于列的自适应阈值(CBAT)稀疏化方法，即为每个图像列设定独立的目标稀疏度，自适应稀疏度方程为

$$Q=\mathrm{floor}(\theta\omega C_{\mathrm{R}}^{\omega}\mathrm{e}^{-\theta C_{\mathrm{R}}^{\omega}}N) \tag{5}$$

式中：Q 为所得的稀疏度；C_{R} 为压缩率；N 为列长；θ 和 ω 为控制参数，由重建算法决定；floor(•) 为向下取整运算。

上式能够提供一个较为合理的目标稀疏度，但针对不同图像或参数设置的适应性仍有待进一步提升。考虑到矩阵的数值特性可以通过其 Lp 范数来反映。因此，利用稀疏系数矩阵的 L_1 和 L_2 范数共同决定稀疏度 J_{p}。对于压缩率为 C_{R}、列长为 N 的图像块，本文所提的自适应阈值稀疏化(ATS)表达式为

$$\begin{cases}S_{\mathrm{p}}=\dfrac{\sqrt{c}-(\sum|\boldsymbol{h}_o|)/\sqrt{\sum\boldsymbol{h}_o^2}}{\sqrt{c}-1}\\ J_{\mathrm{p}}=\mathrm{floor}(S_{\mathrm{p}}C_{\mathrm{R}}^{\tau}\mathrm{e}^{-S_{\mathrm{p}}C_{\mathrm{R}}^{2\tau}}rN)\end{cases} \tag{6}$$

式中：$\boldsymbol{h}_o$ 表示向量 $\boldsymbol{h}$(低频分量或中高频分量)的第 o 个分量；c 为 $\boldsymbol{h}$ 包含的元素的个数；S_{p} 是对向量 $\boldsymbol{h}$ 稀疏程度的度量；τ 为控制参数，本文经大量实验统计，设置为经验值 2.085；r 为不同频率分量的比例。

对于任意一列，将 J_{p} 作为索引取对应的数值设为自适应阈值 T_{S}，将小于 T_{S} 绝对值的像素值置 0，从而消除噪声和不必要的细节。这种自适应机制能够根据图像局部统计特性自动调整阈值，避免固定阈值带来的过度平滑的问题，有效提升图像的重建质量，同时计算复杂度较低。

2.2　密钥更新

本文利用密钥更新机制为每个加密块生成独立且唯一的密钥序列，以有效抵御选择明文攻击。利用基于计数器的参数扰动机制，对混沌系统参数进行动态更新，具体步骤如下。

步骤 1　对计数器的值 c 进行定义，表达式为

$$c_{s+1}=(c_s+1)\bmod 10^{\lambda},\ s=1,2\cdots,N_{\mathrm{c}} \tag{7}$$

式中：N_{c} 和 s 分别表示计数器数量和计数次数；λ 为安全参数，且 $sN_{\mathrm{c}}<10^{\lambda}$。

步骤 2　归一化扰动项，其表达式为

$$\delta_s=\sin\left(\frac{c_s}{10^{\lambda}}\pi\right) \tag{8}$$

式中：δ_s 为扰动参数，用以实现双向调节平衡，且 $\delta_s\in[-1,1]$。

步骤 3　对混沌系统的参数进行扰动，以 ICM 映射中的控制参数 k 为例，定义其表达式为

$$k_s=k+\varepsilon\delta_s \tag{9}$$

式中：$\varepsilon=0.01$，为扰动强度因子，用于控制扰动幅值。

本文算法中，密钥 $K_1=(x_0,y_0)$，$K_2=(x_1,y_1)$ 用于迭代 2D-IHCM 生成测量矩阵；密钥 $K_3=(K_1,K_2)$ 是 K_1 和 K_2 的组合，确保与 K_1、K_2 的同步更新。密钥 v_0 用于迭代 ICM 生成密码流执行置乱与扩散操作；为使局部的密文图像变化能扩散到整幅图像，将 v_0 与其他密钥相关联，设为 $v_0=(x_0+x_1$

$+y_0+y_1)\bmod 1$。

2.3 加密流程

2.3.1 初次加密

步骤 1 将大小为 $N\times N$ 的明文图像 $\boldsymbol{X}$ 均匀分成大小为 $n_b\times n_b$ 个不重叠图像块，图像块的数量为 B。

步骤 2 对各图像块进行 DCT 变换，得到对应的 DCT 系数矩阵，然后利用 Zigzag 扫描将其分别转换成对应的向量 $\boldsymbol{\alpha}_i$，$i=1,2,\cdots,B$。

步骤 3 根据密钥 v_0 迭代 ICM 映射，利用密钥更新机制，获得混沌序列 $\boldsymbol{Z}$，并对其量化取模后转为整型数值序列 $\boldsymbol{Z}'$，作为置乱操作索引。$\boldsymbol{Z}'$ 的表达式为

$$\boldsymbol{Z}'=\mathrm{mod}(\mathrm{floor}(\boldsymbol{Z}+100)\times 10^{10},L)+1 \tag{10}$$

式中：L 为迭代次数。

步骤 4 利用 CRP 方法将 $\boldsymbol{\alpha}_i$ 进行置乱得到向量 $\boldsymbol{\beta}_i$，其表达式为

$$\boldsymbol{\beta}_i^j=f_{\mathrm{CRP}}(\boldsymbol{\alpha}_i^j,\boldsymbol{Z}'_j),\ j=1,2\cdots,n_b^2 \tag{11}$$

式中：$\boldsymbol{\beta}_i^j$ 和 $\boldsymbol{\alpha}_i^j$ 分别表示 $\boldsymbol{\beta}_i$ 和 $\boldsymbol{\alpha}_i$ 的第 j 个频率分量。$f_{\mathrm{CRP}}(\cdot)$ 表示利用 CRP 方法进行置乱。

2.3.2 压缩

遍历所有的图像块，并分别进行以下步骤。

步骤 1 对于第 i 个图像块的 $\boldsymbol{\beta}$，根据设定的低频分量比例 r_L（低频分量长度占总体向量的长度），将向量 $\boldsymbol{\beta}$ 分为低频分量 $\boldsymbol{\beta}_L$ 和中高频分量 $\boldsymbol{\beta}_{\mathrm{MH}}$。

步骤 2 设定整体压缩率为 C_{RZ}，$\boldsymbol{\beta}_L$ 的压缩率为 C_{RL}，则 β_{MH} 的压缩率 C_{RMH} 表达式为

$$C_{\mathrm{RMH}}=(C_{\mathrm{RZ}}-C_{\mathrm{RL}}r_L)/(1-r_L) \tag{12}$$

步骤 3 将 K_1、K_2 作为初始值，利用密钥更新机制对 2D-IHCM 进行迭代。构建 $(r_Ln_b^2C_{\mathrm{RL}})\times(r_Ln_b^2)$ 大小的测量矩阵 $\boldsymbol{\Phi}_1$ 和 $((1-r_L)n_b^2C_{\mathrm{RMH}})\times((1-r_L)n_b^2)$ 大小的测量矩阵 $\boldsymbol{\Phi}_2$，其表达式为

$$\boldsymbol{\Phi}_l=\sqrt{\frac{N}{M}}\boldsymbol{DFR},\ l=1,2 \tag{13}$$

式中：$\boldsymbol{R}$ 为随机置换矩阵；$\boldsymbol{F}$ 为标准正交矩阵；M 为测量值；$\boldsymbol{D}$ 为下采样矩阵，用于随机选择 $\boldsymbol{FR}$ 的 M 行子集；系数 $\sqrt{N/M}$ 使得测量向量的能量与原始信号的能量一致。

步骤 4 根据自适应阈值稀疏化方法，为每个 $\boldsymbol{\beta}_L$ 和 $\boldsymbol{\beta}_{\mathrm{MH}}$ 设置不同的阈值，将低于阈值绝对值的像素值置 0，并利用 $\boldsymbol{\Phi}_1$ 和 $\boldsymbol{\Phi}_2$ 分别得到测量值 $\boldsymbol{\beta}'_L$ 和 $\boldsymbol{\beta}'_{\mathrm{MH}}$，其表达式为

$$\begin{cases}\boldsymbol{\beta}'_L=\boldsymbol{\Phi}_1\boldsymbol{\beta}_L\\ \boldsymbol{\beta}'_{\mathrm{MH}}=\boldsymbol{\Phi}_2\boldsymbol{\beta}_{\mathrm{MH}}\end{cases} \tag{14}$$

步骤 5 将测量值拼接成新的向量，并将其转换为 $m\times n_b$ 大小的矩阵，其中 $m=C_{\mathrm{RZ}}n_b$。

步骤 6 组合各测量块，得到 $M\times N$ 大小的矩阵 $\boldsymbol{X}_1$。

2.3.3 二次加密

步骤 1 量化 $\boldsymbol{X}_1$ 中的元素 X_1，输出由元素 X_2 组成的矩阵 $\boldsymbol{X}_2$，其表达式为

$$X_2=\mathrm{round}\left(255\frac{X_1-X_{1\min}}{X_{1\max}-X_{1\min}}\right) \tag{15}$$

式中：$X_{1\max}$ 和 $X_{1\min}$ 分别表示 $\boldsymbol{X}_1$ 矩阵元素中的最大值和最小值；round(·)表示取最接近的整数值。

步骤 2 利用密钥 v_0 迭代 ICM 映射，生成长度为 $2\times M\times N$ 的整数密码流 $\boldsymbol{S}$，将其分成 2 个长度均为 $M\times N$ 的序列 $\boldsymbol{S}_1$ 和 $\boldsymbol{S}_2$。

步骤 3 对 $\boldsymbol{X}_2$ 执行双向扩散操作生成密文图像矩阵 $\boldsymbol{E}$，其第 $i(i=1,2,\cdots,MN)$ 个元素 E_i 的计算公式为

$$\begin{cases}X_{3,i}=(X_{3,i-1}+S_{1,i}+X_{2,i})\bmod 256\\ E_i=(E_{i-1}+S_{2,i}+X_{3,i})\bmod 256\end{cases} \tag{16}$$

式中：$X_{3,i}$、$X_{3,i-1}$ 分别为过渡矩阵 X_3 第 i、$i-1$ 个元素；$S_{1,i}$、$S_{2,i}$、$X_{2,i}$、E_i 分别为矩阵 $\boldsymbol{S}_1$、$\boldsymbol{S}_2$、$\boldsymbol{X}_2$、$\boldsymbol{E}$ 中第 i 个元素；$X_{3,i}$、$X_{3,i-1}$ 分别为过渡矩阵 $\boldsymbol{X}_3$ 第 i、$i-1$ 个元素。

3 解密算法

解密方根据密钥生成的测量矩阵和密码流进行解密。首先，对密文图像执行逆扩散、逆量化和分块重组操作。然后，不同权限的用户根据对应密钥从密文图像中提取信息并进行重建。最后，用户对重建图像执行解密操作，得到对应权限等级的解密图像。

3.1 解密

步骤 1 对密文图像矩阵 $\boldsymbol{E}$ 进行解扩散操作得到矩阵 $\boldsymbol{Y}_1$，其表达式为

$$\begin{cases}Y_i=(2\times 256+E_i-E_{i+1}-S_{2,i})\bmod 256\\ Y_{1,i}=(2\times 256+Y_i-Y_{i-1}-S_{1,i})\bmod 256\end{cases} \tag{17}$$

式中：Y_i 为过渡矩阵 $\boldsymbol{Y}$ 的第 i 个元素 。

步骤 2 对矩阵 $\boldsymbol{Y}_1$ 中的元素 Y_1 进行逆量化操作得到由元素 Y_2 组成的矩阵 $\boldsymbol{Y}_2$，将 $\boldsymbol{Y}_2$ 均匀分成大小为 $m\times n$ 的不重叠图像。其表达式为

$$Y_2=\frac{Y_1(X_{1\max}-X_{1\min})}{255}+X_{1\min} \tag{18}$$

3.2 基于身份的分级解密

遍历所有的图像块，针对不同身份权限分别进行以下操作。

(1)对于低权限等级用户，分配密钥 K_2 以匹配其权限等级，解密的具体步骤如下。

步骤 1　用户从压缩数据中提取中高频信息，并利用重建算法 SL_0 完成重建，得到中高频分量 $\boldsymbol{R}_{MH}$。

步骤 2　将全 0 向量 $\boldsymbol{\delta}_1$ 与 $\boldsymbol{R}_{MH}$ 拼接，形成组合向量。

步骤 3　对组合向量进行 CRP 逆变换和 Zigzag 逆扫描，然后通过 DCT 逆变换得到对应系数图像块 $\boldsymbol{W}_{MH}$。

步骤 4　组合所有系数图像块，得到大小为 $N \times N$ 的解密图像 $\boldsymbol{Y}_3$。

步骤 5　利用线性对比度拉伸和伽马矫正对 $\boldsymbol{Y}_3$ 进行处理，得到低权限等级对应的解密图像 $\boldsymbol{Y}_4$。

(2)对于中权限等级用户，分配密钥 K_1 以匹配其权限等级，解密的具体步骤如下。

步骤 1　提取低频信息后通过 SL_0 重建算法对其进行重建，得到低频分量 $\boldsymbol{R}_L$。

步骤 2　将 $\boldsymbol{R}_L$ 与全零向量 $\boldsymbol{\delta}_2$ 拼接为组合向量 $\boldsymbol{R}'_L$。

步骤 3　与低权限等级用户步骤 3 相同。

步骤 4　将步骤 3 中所得的图像块均匀划分为 4 个尺寸均为 $n_b/2 \times n_b/2$ 的正方形子块。

步骤 5　分别计算每个子块的像素均值，生成均值向量 $\boldsymbol{A} = [A_1, A_2, A_3, A_4]$。

步骤 6　对各子块的均值进行相似性判定：若均值间的差异在阈值范围内，则取各均值的算术平均，将其作为全局均值填充至所有子块；反之，则保留各子块的原始均值。其表达式为

$$A_{max} - A_{min} < \chi \frac{\sum A_i}{4} \tag{19}$$

式中：A_{min} 和 A_{max} 分别表示向量 $\boldsymbol{A}$ 中的最小值和最大值，χ 为判断参数，本文中设为 0.2。

步骤 7　将处理后的子图像块按原始位置重组后，组合所有的图像块，得到大小为 $N \times N$ 的解密图像 $\boldsymbol{Y}_5$。

(3)对于高权限等级用户，密钥为 $K_3 = (K_1, K_2)$，解密的具体步骤如下。

步骤 1　提取出低频信息和中高频信息。

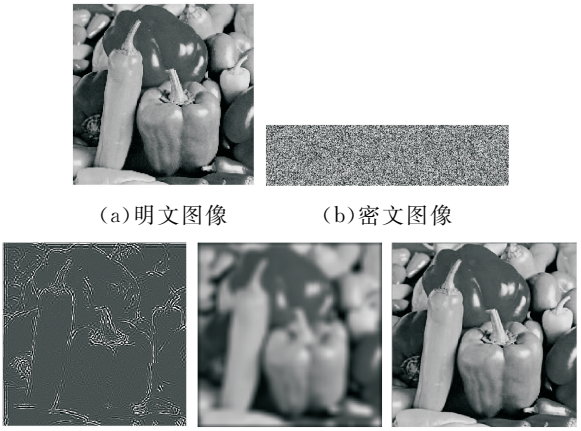
步骤 2　利用 SL_0 算法分别对低频信息和中高频信息进行重建，组合后得到重建向量。

步骤 3、4　与低权限等级用户解密过程的步骤 3、4 一致。最终得到高权限等级用户对应的解密图像 $\boldsymbol{Y}_6$。

4　仿真实验与结果分析

4.1　仿真实验结果

本文的测试平台为 Matlab2021b。选择 Peppers 作为明文图像。初始值和参数设置如下：$(x_0, y_0) = (0.31, 0.13)$，$(x_1, y_1) = (0.84, 0.36)$，$n = 16$，$C_R = 0.25$，$C_{RL} = 12/16$，$r_L = 2/16$。仿真实验结果如图 5 所示。



(a)明文图像　(b)密文图像　(c)解密图像-低　(d)解密图像-中　(e)解密图像-高

图 5　Peppers 仿真结果

Fig. 5　Simulation results of Peppers

由图可知，加密处理后的图像呈现类噪声特征，完全隐藏了原始视觉信息，且大小压缩为明文图像的 1/4。解密图像质量与用户权限严格对应：低权限用户仅能获取基本轮廓信息；中等权限用户可获得降质模糊的图像；高权限用户则可完整恢复原始图像数据。

为定量评估解密图像质量，采用峰值信噪比(PSNR)和平均结构相似度(MSSIM)两项指标[18]，其结果如表 2 所示。由表可知，最高权限用户解密图像的 PSNR 值超过 30 dB，MSSIM 值接近理想值 1。同时，低、中、高权限结果形成明显梯度差异，即 PSNR 差值约为 8～14 dB。该结果表明，该算法在实现分级差异化的同时，仍赋予高权限等级用户优异的压缩性能。

表 2　仿真结果的定量评估

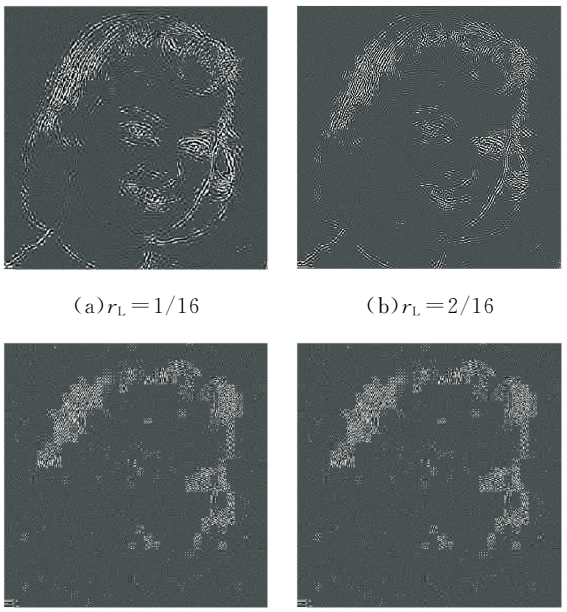
Table 2　Quantitative evaluation of simulation results

明文图像	峰值信噪比/dB			高权限平均结构相似度
	低权限	中权限	高权限	
Parrots	9.036	22.275	37.457	0.963
Woman	10.153	24.561	39.541	0.967
Peppers	10.976	22.134	33.569	0.952

4.2　低频分量比例设置分析

为了在重建图像的视觉效果和压缩性能之间取得平衡，本文算法中的低频、中高频分量占比必须设置合理。由图 6 和表 3 可知，当低频分量比例 $r_L = 1/16$ 时，低权限用户解密图像的视觉效果最佳，

MSSIM 最大；随着 r_L 的增加，低权限等级用户解密图像的可辨识度和 MSSIM 均下降。与此同时，高权限用户解密图像的 MSSIM 逐渐提升。



(a)$r_L=1/16$ (b)$r_L=2/16$

(c)$r_L=3/16$ (d)$r_L=4/16$

图 6 低权限用户解密图像

Fig. 6 Decrypted images for low privilege users

在本文的分级加密框架下，低权限用户解密图像质量依赖于图像的中高频信息。r_L 较小时，低权限用户图像的辨识度较好，但高权限用户因低频信息不足导致解密图像质量欠佳。随着 r_L 的增加，低权限用户解密图像的视觉辨识度下降，同时，更多的低频信息有助于提升高权限用户的解密图像质量。

综合分级保护效果与图像整体重建质量，当 r_L 为 2/16 时，保留的低频分量既能让高权限用户获得较完整的图像结构信息，又能在实现较高 PSNR 和 MSSIM 的同时，使低权限用户的解密图像保持较强的辨识度，从而达到二者的平衡。

表 3 不同低频分量比例下的图像质量评估

Table 3 Image quality assessment under different low frequency ratios

r_L	峰值信噪比/dB				高权限平均结构相似度
	低权限	中权限	高权限	低权限	
1/16	10.388	22.264	31.702	0.271	0.914
2/16	11.706	24.164	35.818	0.240	0.964
3/16	11.774	24.164	36.341	0.234	0.975
4/16	11.728	24.165	36.446	0.186	0.981

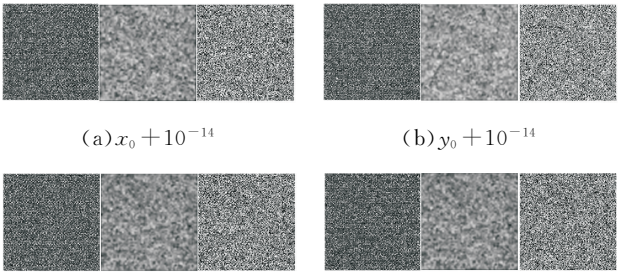
4.3 安全性分析

4.3.1 密钥空间

本文所提算法的密钥包括 x_0、y_0、x_1 和 y_1。根据 IEEE 754 浮点数精度标准，密钥空间大小为 $(6\pi\times10^{14})^2(40\times10^{14})^2=5.76\pi^2\times10^{60}\approx2^{205}$，远大于所建议的密钥空间值 2^{100}。这表明本文所提算法具有足够大的密钥空间，可有效抵抗暴力攻击。

4.3.2 密钥敏感度

为测试本文算法的抗攻击能力，对明文图像 Parrots 加密后，对其中一个密钥进行极小的扰动，其余密钥不变，对应解密图像如图 7 所示。由图可知，利用错误密钥得到的解密图像无法提取出任何有视觉意义的图像信息，证明本文算法具有良好的密钥敏感度。



(a)x_0+10^{-14} (b)y_0+10^{-14}

(c)x_1+10^{-14} (d)y_1+10^{-14}

左图—低权限 中图—中权限 右图—高权限

图 7 错误密钥得到的解密图像

Fig. 7 Decrypted images obtained with the wrong keys

5 对比实验与性能分析

5.1 同类算法比较

为评估本文算法与同类分级安全加密算法的差异，从算法类型、消耗带宽、各等级用户的视觉效果等方面进行对比分析。

由表 4 的对比结果可知，本文与文献[11]具有相同的传输带宽；相比于文献[12]，本文算法的传输带宽降低至 1/16。在视觉分级效果上，本文算法呈现出更明显的分级差异。尽管文献[11]具有图像区域分级保护的特点，但其整体的压缩性能较低。

此外，对于同一测试图像，本文算法的高权限解密图像 PSNR 为 34.35 dB，较文献[13]的 27.92 dB 提升了 23.03%，较文献[11]的 30.10 dB 提升了 14.11%。综合比较，本文在多用户分布式场景下能够更有效的平衡压缩性能与安全性。

5.2 与其他压缩算法比较

本文以高权限等级用户解密图像为例，与其他压缩算法进行比较，包括基于 PCS 的算法[19-22]、BCS

算法[8，23-24]以及二维压缩感知算法[25]。

5.2.1　压缩性能

表 5 为本文与其他文献算法压缩性能的对比，其中，3D IWT 为三维整数小波变换，2DPG-ED 为二维投影梯度嵌入解密算法，HWT 为哈尔小波变换。由表 5 可知，与 PCS 和 BCS 框架相比，本文算法的 PSNR 有 7～12 dB 的性能增益。与文献[25]相比，本文算法的 PSNR 差距为 0.5～1.3 dB，考虑到稀疏基和重建算法的差异，损失在可接受范围之内。综合而言，本文算法在压缩性能方面具有较大优势。

表 4　本文算法与其他文献算法的对比

Table 4 Comparison of the proposed algorithm with existing algorithms

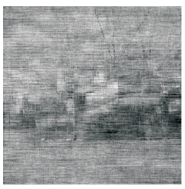
算法来源	类型	传输带宽	分级视觉效果		
			低权限	中权限	高权限
文献[11]	ROI 分级	$M\times N$			
文献[12]	图像整体渐进分级	$nN\times N$			
文献[13]	图像整体渐进分级	$M\times\lambda N$			
本文	图像整体渐进分级	$M\times N$			

表 5　本文算法与其他文献算法的压缩性能的对比

Table 5 Comparison of compression performance between the proposed algorithm and existing algorithms

明文图像	对比文献	稀疏基	重建算法	峰值信噪比/dB
Peppers	本文	DCT	SL_0	33.57
	文献[19]	DCT	SL_0	23.15
	文献[25]	3D IWT	2DPG-ED	34.78
Woman	本文	DCT	SL_0	39.54
	文献[19]	DCT	SL_0	28.97
	文献[25]	3D IWT	2DPG-ED	39.92
Barbara	本文	DCT	SL_0	34.35
	文献[21]	HWT	SL_0	26.47
	文献[23]	DCT	SL_0	26.04
Milkdrop	本文	DCT	SL_0	38.04
	文献[19]	DCT	SL_0	26.98
	文献[24]	DCT	SPL	30.56

5.2.2　阈值设定对压缩性能的影响

为验证本文所提自适应阈值稀疏化方法的有效性，对固定阈值方法(综合评估后 T_S 为 15)和文献[9]中的 CBAT 方法进行比较分析。

由表 6 可知，相较于固定阈值法，本文所提 ATS 方法的 PSNR 提升了 0～2 dB；与 CBAT 方法相比，PSNR 能提升 1～2 dB。该结果证明了所提方法的有效性与适应性。

表 6　不同阈值设定的对比结果

Table 6 Comparison results of different threshold settings

明文图像	峰值信噪比/dB		
	$T_S=15$	CBAT	ATS
Parrots	36.834	36.435	37.457
Woman	38.195	38.551	39.541
Peppers	33.141	32.545	33.569

5.2.3 运行效率

为验证算法的可行性，本小节对算法的运行效率进行对比。表 7 为本文算法与其他文献算法的计算复杂度对比。由表可知，频率分类与 BCS 的结合显著降低了基于 PCS 框架[20]和二维压缩感知框架[25]的计算开销。此外，相比于文献[23]中 8×8 分块大小的 BCS 框架，本文算法也具有更低的计算复杂度。

表 7 本文算法与其他文献算法计算复杂度的对比

Table 7 Computational complexity comparison between the proposed algorithm and existing algorithms

算法来源	加密复杂度	解密复杂度
文献[20]	$O(C_R N^2+N^2\mathrm{lb}N)$	$O(C_R N^2+N^2\mathrm{lb}N+N^3\mathrm{lb}N/C_R)$
文献[23]	$O(11N^2)$	$O(11N^2+N^2B\mathrm{lb}B/C_R)$
文献[25]	$O(N^2\mathrm{lb}N)$	$O(N^2\mathrm{lb}N+N^3\mathrm{lb}N/C_R)$
本文	$O(5N^2)$	$O(5N^2+N^2B\mathrm{lb}B/C_R)$

注：$O(\cdot)$用来描述算法的时间复杂度。

表 8 为基于 10 次测试的平均运行时间。尽管由于分级访问控制复杂度的增加，加密时间为其余算法的 2 倍，但 BCS 框架和二维混沌系统显著提升了解密效率。相较于文献[8]的 BCS 框架结合四维超混沌的系统，本文整体时间开销减少了 38%；较文献[22]的 PCS 框架相比，整体用时减少了 53%。因此，本文算法具有最低的计算复杂度和较高的运行效率。

表 8 本文算法与其他文献算法运行时间的对比

Table 8 Comparison results of running time between the proposed algorithm and existing algorithms

分辨率	过程	运行时间/s		
		本文	文献[8]	文献[22]
512×512	加密	0.141	0.064	0.076
	解密	0.566	1.067	1.417
	整体	0.707	1.131	1.493

6 结 论

针对资源受限环境下面向多用户的图像安全问题，本文提出一种融合频率分类压缩、二维混沌映射与自适应阈值稀疏化的图像分级加密算法。与现有的算法相比，在身份访问控制的灵活性、计算效率以及压缩性能等方面均有不同程度的提升，得到以下结论。

(1)针对不同权限等级用户实现了分级访问控制，使得不同权限的用户获取差异化的解密图像，各权限对应解密图像的 PSNR 差值约为 8～14 dB。

(2)对经典二维 Henon 混沌进行改进，进一步提升了混沌特性。在保证算法安全性的同时，时间开销减少了 38%以上，运行效率显著提升。

(3)提出的自适应阈值稀疏化方法与频率分类压缩相结合，能够获得 7～12 dB 的压缩性能增益。

综上所述，本文所提算法具有差异化的分级安全隐私保护效果、良好的压缩性能和较低的计算复杂度，适用于资源受限环境下图像信息的分级保护。

参考文献：

[1] 张丽娜，辛鹏，侯明会，等. 扩展汉明码下二级 QR 码信息隐藏方案 [J]. 计算机工程与科学，2025，47(5)：832-842.
ZHANG Lina，XIN Peng，HOU Minghui，et al. An information hiding scheme of two-level QR code using extended Hamming code [J]. Computer Engineering & Science，2025，47(5)：832-842.

[2] 李谢华，娄芹，杨俊雪，等. 结合可逆神经网络和逆梯度注意力的抗屏摄攻击水印方法 [J]. 电子与信息学报，2024，46(7)：3046-3053.
LI Xiehua，LOU Qin，YANG Junxue，et al. Screen-shooting resilient watermarking scheme combining invertible neural network and inverse gradient attention [J]. Journal of Electronics & Information Technology，2024，46(7)：3046-3053.

[3] HU Longlong，CHEN Mingxuan，WANG Mengmeng，et al. A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion [J]. Chaos Solitons & Fractals，2024，188：115521.

[4] SU Wenyi，ZHOU Mingjie，BAO Jiaqing，et al. Image encryption design based on Henon mapping [C]// 2024 Asia-Pacific Conference on Image Processing，Electronics and Computers (IPEC). Piscataway，NJ，USA：IEEE，2024：280-285.

[5] ZHU Liya，JIANG Donghua，NI Jiangqun，et al. A visually secure image encryption scheme using adaptive-thresholding sparsification compression sensing model and newly-designed memristive chaotic map [J]. Information Sciences，2022，607：1001-1022.

[6] 任花，牛少彰，任如勇，等. 基于二维压缩感知的有意义图像加密算法研究 [J]. 通信学报，2022，43(5)：45-57.
REN Hua，NIU Shaozhang，REN Ruyong，et al. Research on meaningful image encryption algorithm based on 2-dimensional compressive sensing [J]. Journal on

Communications，2022，43(5)：45-57.

[7] LIU Wenhao，WANG Huihai，CHEN Yongjiu，et al. A new image encryption scheme based on block compressive sensing and chaotic laser system for IoT [J]. The European Physical Journal Plus，2024，139(6)：473.

[8] ZHU Liya，SONG Huansheng，ZHANG Xi，et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding [J]. Signal Processing，2020，175：107629.

[9] HUA Zhongyun，ZHANG Kuiyuan，LI Yuanman，et al. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing [J]. Signal Processing，2021，183：107998.

[10] HE Xiaofei，LI Lixiang，TONG Fenghua，et al. Multilevel privacy protection for social media based on 2-D compressive sensing [J]. IEEE Internet of Things Journal，2024，11(4)：6878-6892.

[11] HE Xiaofei，LI Lixiang，PENG Haipeng，et al. A multi-level privacy-preserving scheme for extracting traffic images [J]. Signal Processing，2024，220：109445.

[12] CHEN Hao，XIONG Lizhi，YANG C N. Progressive secret image sharing based on Boolean operations and polynomial interpolations [J]. Multimedia Systems，2024，30(4)：189.

[13] XIE Dong，LI Lixiang，PENG Haipeng，et al. A secure and efficient scalable secret image sharing scheme with flexible shadow sizes [J]. PLoS One，2017，12(1)：e0168674.

[14] TENG Lin，WANG Xingyuan，XIAN Yongjin. Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion [J]. Information Sciences，2022，605(C)：71-85.

[15] HUANG Xingfan，TANG Jianeng，ZHANG Zezong. Efficient and secure image encryption algorithm using 2D LIM map and Latin square matrix [J]. Nonlinear Dynamics，2024，112(24)：22463-22483.

[16] HUA Zhongyun，ZHU Zhihua，CHEN Yongyong，et al. Color image encryption using orthogonal Latin squares and a new 2D chaotic system [J]. Nonlinear Dynamics，2021，104(4)：4505-4522.

[17] GAO Zhirong，XIONG Chengyi，DING Lixin，et al. Image representation using block compressive sensing for compression applications [J]. Journal of Visual Communication and Image Representation，2013，24(7)：885-894.

[18] 蒋东华，朱礼亚，沈子懿，等. 结合二维压缩感知和混沌映射的双图像视觉安全加密算法 [J]. 西安交通大学学报，2022，56(2)：139-148.
JIANG Donghua，ZHU Liya，SHEN Ziyi，et al. A double image visual security encryption algorithm combining 2D compressive sensing and chaotic mapping [J]. Journal of Xi'an Jiaotong University，2022，56(2)：139-148.

[19] CHEN Kehan，ZHANG Haijun，YAN Fei. An adaptive image compression-encryption scheme using 2D logarithm-exponent-squared-sine coupling map [J]. Nonlinear Dynamics，2025，113(2)：1827-1856.

[20] GAO Yuhui，LIU Jingyi，ZHANG Bo，et al. Image encryption algorithm based on four-dimensional memristor hyperchaotic system and parallel compressive sensing [J]. Nonlinear Dynamics，2024，112(22)：20381-20400.

[21] LU Yang，GONG Mengxin，CAO Lvchen，et al. Exploiting 3D fractal cube and chaos for effective multi-image compression and encryption [J]. Journal of King Saud University-Computer and Information Sciences，2023，35(3)：37-58.

[22] CHAI Xiuli，WU Haiyang，GAN Zhihua，et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding [J]. Optics and Lasers in Engineering，2020，124：105837.

[23] LI Zhen，YANG Siqi，TAN Weijie，et al. A remote sensing image encryption and compression scheme using novel hyperchaotic system and plaintext related random S-box [J]. Nonlinear Dynamics，2025，113(3)：2769-2790.

[24] DOU Yuqiang，YUE Shuang，ZHANG Xinke，et al. A special image encryption strategy based on a novel digital chaotic system and binary block compressed sensing for fixed-point DSP [J]. Nonlinear Dynamics，2025，113(9)：10535-10558.

[25] HU Longlong，CHEN Mingxuan，WANG Mengmeng，et al. Visually meaningful triple images encryption algorithm based on 2D compressive sensing and multi-region embedding [J]. Knowledge-Based Systems，2025，324：113804.

（编辑　刘懿莹）