无干涉编码孔径相关全息的多图像双重混沌压缩加密方法*

李佳[1)] 于雪莲[1)†] 章跃辉[1)] 牛佳[2)4)] 贺磊[5)] 孙彦乾[3)4)] 李秀芳[3)4)]

1) (哈尔滨理工大学测控技术与通信工程学院, 黑龙江省量子调控重点实验室, 哈尔滨 150080)

2) (西安交通大学物理学院, 陕西省量子信息与光电量子器件重点实验室, 西安 710049)

3) (北京交通大学, 发光与光学信息教育部重点实验室, 北京 100044)

4) (大恒新纪元科技股份有限公司北京光电技术研究所, 北京 100085)

5) (哈尔滨新光光电科技股份有限公司, 哈尔滨 150078)

(2025 年 11 月 10 日收到; 2025 年 12 月 22 日收到修改稿)

随着图像数据量的激增及信息安全需求的提升, 传统单图像加密方法在多图像并行传输中面临安全性与效率瓶颈. 本文提出一种基于无干涉编码孔径相关全息的多图像混沌压缩双重加密方法, 构建了一个物理与数字协同的双重加密体系. 首先利用无干涉编码孔径相关全息成像构建前端物理加密层, 通过记录图像的点扩散全息图实现初步加密, 具备良好的抗物理攻击能力. 随后在数字加密层中采用分块离散余弦变换对全息图进行能量压缩与稀疏化, 并结合混沌系统生成的密钥序列与压缩感知理论实现次级加密, 从而同时提高安全强度与压缩效率. 仿真与实验结果证实了其在密钥空间规模、密钥敏感性、抗统计分析能力和鲁棒性方面的有效性, 同时在多图像压缩效率方面可平均降低约 30% 的数据量, 体现出明显的性能优势, 适用于监控、医学成像等场景中的图像数据安全传输与存储.

关键词: 多图像加密, 无干涉编码孔径相关全息, 压缩感知, 混沌系统

DOI: 10.7498/aps.75.20251533 **CSTR:** 32037.14.aps.75.20251533

1 引 言

随着互联网与物联网的迅猛发展以及高分辨率图像采集设备的普及, 图像数据呈现爆炸式增长, 给数据传输与存储带来巨大压力, 也引发了严重的安全问题. 在医疗、军事、远程通信等敏感领域, 图像数据的保密性和完整性尤为关键[1–3]. 然而, 传统的图像加密算法多针对单幅图像, 难以满足多图像并行传输的实际需求. 因此, 近年来多图像加密技术逐渐成为研究热点, 以应对大容量图像的安全传输挑战[4–6]. 光学成像加密技术因其天然的并行计算能力而备受关注[7–11]. 虽然传统光学加密方法如双随机相位加密等具成熟的结构, 但通常依赖于相干光和复杂的干涉过程, 系统对准要求高且容易受攻击[12]. 相比之下, 无干涉编码孔径相关全息 (interferenceless coded aperture correlation holography, I-COACH) 提供了一种新思路. 该方法采用非相干照明且无需波前分束, 能够以更简洁的系统结构获取物体的三维信息, 适用于光学加密领域[13–17]. 基于此原理, Yu 等[18] 于 2022 年首次提出了一种基于无透镜 I-COACH 的光学图像加

* 黑龙江省自然科学基金 (批准号: PL2024F020)、黑龙江省博士后出站科研启动金和教育部产学合作协同育人项目 (批准号: 231104090250214) 资助的课题.

† 通信作者. E-mail: yuxuelian@hrbust.edu.cn

密系统, 实现了对单幅图像的有效编码和加密. Zhang 等[19] 于 2024 年提出了一种基于三光束配置的非相干频率选择复用全息加密方案, 并证明该方法可以扩展到更多图像的并行加密. 总体而言, 非相干光学加密技术凭借其无干涉特性和随机掩模的可编程性, 在抗攻击性、系统稳定性方面展现出显著优势, 已成为光学加密领域的重要工具.

在数字域图像加密方面, 混沌映射因其对初始条件的高度敏感性与动力学复杂性而被广泛应用. 研究者提出了多种改进型混沌系统, 如高维超混沌、分数阶混沌和变参数系统, 以扩展密钥空间、提高加密强度[20–22]. 此外, 为了减小密文数据量并提高传输效率, 压缩感知技术逐渐被引入图像加密中[23–30]. 综述性研究指出, 多图像加密技术的发展主要围绕混沌系统、多维变换域及压缩感知等策略展开[31–36].2022 年, Wei 等[37] 提出了一种基于二维压缩感知和光学加密的多图像压缩-加密算法, 同时引入分数阶混沌系统以增强加密复杂性. 2024 年, Hu 等[32] 基于块级压缩感知和非线性二叉树扩散设计了多图像加密算法, 显著提高了加密容量和重建质量.Hosny 等[38] 提出的多图像加密方案, 利用多层二维混沌映射对图像通道进行置乱和扩散, 有效提升了密钥空间和抗攻击能力. 此外, 混沌系统与分层加密的结合进一步拓展了多图像加密的应用场景. 例如, Zhang 等[39] 提出一种面向医学图像的分层加密方案, 通过混沌密钥分级实现差异化解密, 并结合行-列混淆与闭环双向扩散机制, 在保证安全性的同时有效提升了多图像批处理的加解密效率.2025 年, Xue 等[40] 提出了一种基于双随机相位编码与压缩感知的多图像加密方案, 该方案通过复合采样与混沌映射实现批量认证, 并利用双重嵌入方法完成视觉安全传输, 从而提升了认证效率与系统鲁棒性. 这些研究表明, 压缩感知能够显著降低待传输的密文规模, 而混沌映射则显著增强了系统的抗攻击能力. 混沌系统与压缩感知的融合在提高图像加密安全性的同时, 也有效减小了数据量, 满足了海量图像传输场景的需求.

基于无干涉编码孔径相关全息, 本文提出了一种结合光学加密与数字加密的多图像双重混沌压缩加密方法. 该方法首先利用 I-COACH 系统作为前端物理加密层, 充分发挥其对密钥点源全息图的敏感性和物理实现的独特性. 随后, 对全息图数据进行分块离散余弦变换 (discrete cosine transform, DCT), 以实现能量压缩和稀疏化. 接着, 采用混沌系统生成的序列对 DCT 系数进行置乱或扰动, 从而增强加密的随机性和密钥敏感性. 最后, 通过压缩感知理论对扰动后的稀疏系数进行测量和压缩, 进一步降低数据冗余, 并提升安全性. 每个环节均引入密钥参数, 构成一个庞大的密钥空间和多重安全壁垒. 通过仿真实验, 对所提方法的加密效果、密钥空间、密钥敏感性、抗统计攻击能力以及抗噪声和遮挡攻击的鲁棒性进行分析和验证. 结果表明, 该方法能够有效加密多幅图像, 不仅确保了较高的安全性, 同时也具备良好的鲁棒性和压缩性能, 对多图像的安全传输与存储具有重要的应用价值.

2 方法原理

2.1 I-COACH 光学成像原理

I-COACH 是一种基于空间非相干照明的无干涉全息技术. 其核心思想是通过记录两幅强度图像: 一幅是点扩散全息图 (point spread hologram, PSH), 另一幅是物体全息图. 然后, 通过反卷积运算对这两幅图像进行处理, 以重建物体信息.

图 1 为本文提出的基于 I-COACH 的双重混沌压缩加密方法原理图. 在图 1(a) 所示的光学加密流程图中, 光学系统采用非相干 LED 光源, 其发出的光束经透镜 L_1 准直后照射物平面, 随后通过透镜 L_2 进行二次准直. 光束经偏振片 P 后入射至空间光调制器 (spatial light modulator, SLM) 所在平面, P 的偏振方向与 SLM 的调制偏振方向严格匹配.SLM 上加载有预先设计的编码相位掩膜 (coded phase mask, CPM), 对入射光场进行相位调制, 最终在图像传感器平面形成全息图. 物平面到 SLM 所在平面的距离记为 z_{s}, SLM 到图像传感器所在平面的距离记为 z_{h}.

在图 1(a) 所示 I-COACH 光学系统中, 针孔平面上任意坐标点 $(\bar{r}_{\mathrm{s}}, z_{\mathrm{s}}) = (x_{\mathrm{s}}, y_{\mathrm{s}}, z_{\mathrm{s}})$ 处的点源场分布的振幅为 $\sqrt{I_{\mathrm{s}}}$, 透镜焦距为 f_0. 为了简化分析, 透镜 L_2 至 SLM 的波前传播距离近似为 0. 此时, SLM 平面处的复振幅分布可表述为 $\sqrt{I_{\mathrm{s}}}G_1L(\bar{\boldsymbol{r}}_{\mathrm{s}}/z_{\mathrm{s}})\times Q\left(z_{\mathrm{s}}^{-1}\right)$, 其中 G_1 为复常数, Q 和 L 为二次相位函数, 分别由 $Q(a)=\exp\left[\dfrac{\mathrm{i}\pi a}{\lambda}(x^2+y^2)\right]$ 和 $L\left(\dfrac{\bar{r}_{\mathrm{s}}}{z_{\mathrm{s}}}\right)=\exp\left[\dfrac{\mathrm{i}2\pi a}{\lambda z_{\mathrm{s}}}(s_x x+s_y y)\right]$ 给出, λ 表示中心波长, x 和 y 表示空间坐标分量, s_x 和 s_y 分别表示 $\bar{r}_{\mathrm{s}}$ 沿 x 轴

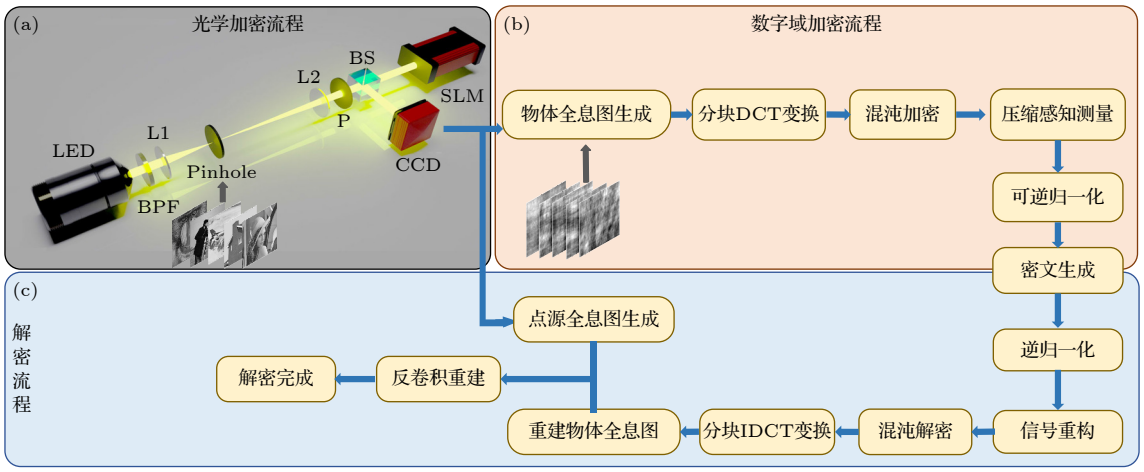


图 1 基于 I-COACH 的双重混沌压缩加密方法原理图

Fig. 1. Schematic of the dual chaotic compression encryption method based on I-COACH.

和 y 轴的分量. 经过 SLM 调制后的光场的复振幅记为 $\sqrt{I_{\mathrm{s}}}G_1L\left(\overline{r}_{\mathrm{s}}/z_{\mathrm{s}}\right)Q\left(z_{\mathrm{s}}^{-1}\right)Q\left(f_0^{-1}\right)\exp\left[\mathrm{i}\phi_m(\overline{r})\right]$, 其中 ϕ_m 表示为第 m 个 CPM 的相位. 该光波经过距离 z_{h} 的传播后到达图像传感器平面, 并被记录下来. 图像传感器记录的强度分布可表示为

$$P_m = \left|\sqrt{I_{\mathrm{s}}}G_1Q\left(\frac{1}{z_{\mathrm{s}}}\right)L\left(\frac{\overline{r}_{\mathrm{s}}}{z_{\mathrm{s}}}\right)Q\left(-\frac{1}{f_0}\right) \times \exp\left[\mathrm{i}\phi_m\left(\overline{r}\right)\right] * Q\left(\frac{1}{z_{\mathrm{h}}}\right)\right|^2, \tag{1}$$

其中, *为卷积运算.

在具体实验中, 为减小图像背景噪声, SLM 上通常加载总数量为 t 个不同的 CPM 合成 PSH, 其表达式为

$$H_{\mathrm{PSH}} = \sum_{m=1}^{t} P_m \exp\left(\mathrm{i}m2\pi/t\right), \tag{2}$$

其中, H_{PSH} 表示最终记录的 PSH, P_m 表示使用第 m 个 CPM 生成的 PSH.

相应地, 二维物体 O 经过 SLM 上 t 个不同的 CPM 调制后记录的物体全息图强度可以表示为

$$\begin{cases} I_{\mathrm{OH},m} = O * P_m, \\ I_{\mathrm{OH}} = \displaystyle\sum_{m=1}^{t} I_{\mathrm{OH},m}\exp\left(\mathrm{i}m2\pi/t\right), \end{cases} \tag{3}$$

其中, $I_{\mathrm{OH},m}$ 表示经过第 m 个 CPM 调制后生成的物体全息图强度分布, I_{OH} 表示最终合成的物体全息图强度分布.

2.2 加密过程

如图 1 所示, 本文提出了一种物理光学加密与数字域加密的协同架构, 加密算法的输入为 n 幅明文灰度图像 $\{O_1, O_2, \cdots, O_n\}$, 输出为一幅密文图像 Y. 所使用的密钥分为光学密钥和数字密钥. 光学加密的主要密钥包括 PSH, 中心波长 λ, 衍射距离 z_{s} 和 z_{h}. 数字域加密的主要密钥包括 Logistic 映射与 Henon 映射的初始值和参数, 以及构建测量矩阵所需的随机种子等. 加密步骤如下.

步骤 1 物理光学层编码

使用 Gerchberg-Saxton 算法生成两幅不同的 CPM, 根据 (2) 式来合成最终的 PSH.其表达式为

$$H_{\mathrm{PSH}} = P_2 - P_1, \tag{4}$$

其中, P_1 和 P_2 分别表示使用两个不同的 CPM 生成的两个 PSH.

接着分别用 n 幅明文图像替换图 1(a) 的针孔, 并且每张灰度图像经过 I-COACH 系统调制时, 分别采用构造 PSH 时使用的两个不同 CPM 进行加密, 从而生成两个不同的物体全息图. 根据 (3) 式可知对这两个全息图进行相减, 得到所需的最终物体全息图, 记为 I_n. 其表达式为

$$\begin{cases} I_{n,m} = O_n * P_m, \\ I_n = I_{n,2} - I_{n,1}, \end{cases} \tag{5}$$

其中, O_n 为第 n 幅明文灰度图像的复振幅, $I_{n,m}$ 表示第 n 幅明文灰度图像经过第 m 个 CPM 调制后生成的物体全息图强度分布, 且 $m = 1, 2$.

步骤 2 分块离散余弦变换

物体全息图 I_n 的分辨率记为 $a \times b$ 像素. 将每幅全息图图像 I_n 分割为 $B \times B$ 的不重叠图像块, 共有 $(a/B) \times (b/B)$ 个块. 对于位于位置 (i, j) 的图

像块, 可以表示为 $B_n(i,j)$, 其中 $i \in \{1, B+1, \cdots, a-B+1\}$, $j \in \{1, B+1, \cdots, b-B+1\}$.

$$\begin{cases} D_n(i,j) = \mathrm{DCT2}[B_n(i,j)], \\ \mathrm{DCT2}(X)_{u,v} = \alpha_u \alpha_v \displaystyle\sum_{x=0}^{B-1}\sum_{y=0}^{B-1} X_{x,y} \cos\left[\frac{\pi(2x+1)u}{2B}\right] \\ \qquad \times \cos\left[\frac{\pi(2y+1)v}{2B}\right], \\ v(i,j) = \left[D_1(i,j)(:); D_2(i,j)(:); \cdots; D_n(i,j)(:)\right], \end{cases} \tag{6}$$

其中, $\mathrm{DCT2}(X)_{u,v}$ 表示块 X 在频域坐标 (u,v) 处的二维 DCT 系数, u和v 为频域索引, α_u和α_v 表示归一化系数, $v(i,j)$ 表示位置 (i,j) 处对应的合并 DCT 系数向量.

步骤 3 双重混沌扰动

为了增强加密的安全性, 本文引入两种混沌映射对向量 $v(i,j)$ 进行扰动.

第 1 阶段采用 Logistic 映射生成一个长度为 M 的伪随机序列 $L = \{l_1, l_2, \cdots, l_M\}$, 该序列的初始状态 x_0 和参数 μ 作为第一级密钥, 对每个高维向量 $v(i,j)$ 进行元素乘积扰动, 具体公式如下:

$$\begin{cases} x_{k+1} = \mu x_k (1 - x_k), \\ v_L(i,j) = v(i,j) \odot L, \end{cases} \tag{7}$$

其中, $x_k \in [0,1]$ 是第 k 次迭代的值, μ 是控制参数, 当 $3.5699 < \mu \leqslant 4$ 时, 系统处于混沌状态 [41]. 本文使用 $\mu = 3.99$ 作为控制参数, 初始值 $x_0 = 0.1$, $\odot$ 表示哈达玛积, 即元素对应相乘.

第 2 阶段利用 Henon 映射生成一个伪随机序列 $H = \{h_1, h_2, \cdots, h_{N_{\mathrm{block}}}\}$, 其初始状态 (y_0, z_0) 和参数 (α, β) 构成第 2 级密钥. N_{block} 为 Henon 映射的长度. 本文对第 p 个块 (对应位置 (i,j) 的向量 $v_L(i,j)$) 应用一个基于 h_p 的缩放因子进行扰动, 其中 $p \in \{1, 2, \cdots, N_{\mathrm{block}}\}$, 具体公式表示为

$$\begin{cases} y_{q+1} = 1 - \alpha y_q^2 + z_q, \\ z_{q+1} = \beta y_q, \\ v_H(i,j) = v_L(i,j) \times (1 + \delta \cdot h_p), \end{cases} \tag{8}$$

其中, y_q 和 z_q 是系统状态变量. 当 $\alpha = 1.4$, $\beta = 0.3$ 时, Henon 映射表现出混沌行为, 其轨迹对初始条件极为敏感, 产生的序列呈现伪随机性且具有不可预测性 [42]. 序列初始值选取 $y_0 = 0.1$ 和 $z_0 = 0.1$, 根据初始状态 (y_0, z_0) 通过迭代运算得到 h_p 序列中的每一个元素.

步骤 4 压缩感知测量

经过混沌扰动的 DCT 系数仍然保持稀疏特性, 本文利用压缩感知 (compressed sensing, CS) 构建一个满足约束等距特性的测量矩阵 $\boldsymbol{\Phi}$, 大小为 $K \times M$, 并且 $K < M$, 以实现数据压缩. $\boldsymbol{\Phi}$ 是一个独立同分布的高斯随机矩阵, 并按行进行 ℓ_2 范数归一化. 将扰动后的高维向量 $v_{\mathrm{H}}(i,j)$ 通过测量矩阵 $\boldsymbol{\Phi}$ 进行线性测量, 得到长度为 K 的测量向量 $Y(i,j)$. 最后, 将该测量向量重塑为二维图像, 以获得密文 Y, 其公式表示为

$$Y(i,j) = \Phi v_{\mathrm{H}}(i,j). \tag{9}$$

2.3 解密过程

解密过程作为加密的逆变换, 其核心在于通过稀疏重构、混沌解扰以及反卷积校正的级联处理实现信息的精确恢复, 显著提升了系统对测量噪声与密钥误差的鲁棒性. 解密步骤如下.

步骤 1 压缩感知重构. 令加密端第 (i,j) 块的测量向量 $Y(i,j)$, 满足 (9) 式测量模型. 当 $K = M$ 时, 此时 CS 测量矩阵 $\boldsymbol{\Phi}$ 是正交矩阵, 无需 CS 重构算法即可通过 $\boldsymbol{\Phi}^{\mathrm{T}}$ 进行逆变换来精确恢复, 当 $K < M$ 时, 需要 CS 重构算法进行恢复. 快速迭代收缩阈值算法 (fast iterative shrinkage-thresholding algorithm, FISTA) 是一种求解上述 ℓ_1 范数正则化最小二乘问题的快速迭代算法. 解密端先利用满足约束等距特性的高斯随机测量矩阵 $\boldsymbol{\Phi}$ 和 CS 重构算法 FISTA, 重构出扰动后的稀疏系数向量的估计值 $\hat{v}_{\mathrm{H}}(i,j)$. 解得每块稀疏向量后, 按加密时的块排列恢复扰动后的 DCT 系数矩阵.FISTA 重构算法的步长参数 $\eta = 1/L$, 其中 $L = \left|\left|\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{\Phi}\right|\right|_F$ 为矩阵 $\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{\Phi}$ 的 Frobenius 范数, 满足 $\eta \leqslant 1/L_{\max}$, $L_{\max}$ 为 $\boldsymbol{\Phi}^{\mathrm{T}}\boldsymbol{\Phi}$ 的最大特征值, 确保了梯度下降的稳定性. 这个过程利用了原始信号在 DCT 域的稀疏性, 其公式表示为

$$\hat{v}_H(i,j) = \arg\min_{z \in \mathbb{R}^M} ||z||_1 \ \text{s.t.}\ Y(i,j) = \boldsymbol{\Phi} z, \tag{10}$$

其中, z 表示待求解的稀疏系数向量.

步骤 2 混沌解扰. 根据加密时使用的混沌映射与初始密钥 (Logistic 初始值与参数、Henon 的初始值与参数及缩放因子等) 在解密端精确再生相同的伪随机序列 H 和 L. 依次进行 Henon 解扰和

Logistic 解扰恢复原始联合 DCT 系数向量. 这一步骤确保了解密过程的准确性和安全性.

步骤 3 系数分离与逆 DCT.将解扰后的向量分割成 n 个长度为 B^2 的子向量, 将每个子向量重新转化为 $B\times B$ 的矩阵, 再对每个块应用二维逆 DCT 变换, 直到最后所有块都被处理, 将所有解密的图像块根据其在原图像中的位置 (i,j) 进行重组, 从而得到 n 张解密后的物体全息图.

步骤 4 将步骤 3 获得的 n 张物体全息图分别和 2.2 节加密过程记录的 I-COACH 系统光学密钥 H_{PSH} 进行反卷积运算得到最终解密的 n 张灰度图像.

3 仿真分析与评价

为了验证所提方案的有效性, 本文使用 MATLAB 平台进行数值模拟仿真实验. 仿真中使用图像数量 $n=5$ 幅灰度图像进行 2.2 节的加密处理, 每张图像分辨率为 $a\times b=256\times 256$, LED 光源中心波长为 $\lambda_{\mathrm{LED}}=532$ nm, 5 幅灰度图像与 SLM 之间的距离 z_{s} 为 300 mm, SLM 到图像传感器的距离 $z_{\mathrm{h}}=300$ mm, 块大小设置为 $B=16\times 16$ 像素. 在解密端, 执行 2.3 节逆过程完成图像恢复, 并评价图像解密质量, 本文采用结构相似度 (structural similarity index, SSIM) 作为评价图像加密方法的指标, 对该方案的性能与安全性进行了定量分析, 其数值越接近 1, 表明解密图像的失真越少, 两幅图像的相似性越高.

3.1 加密效果与统计安全性分析

图 2(a) 展示了 5 张原始灰度图像, 分别是“狒狒”、“摄影师”、“飞机”、“房子”以及“Lena”. 图 2(b) 所示为通过本方案光学加密后生成的物体全息图, 图 3(a) 为 I-COACH 系统记录的点源全息图密钥, 图 3(c) 为在 $K=M$ 的情况下生成的最终密文图像, 从密文图像可以看出, 原始图像的内容和结构信息已被完全隐藏, 密文呈现出伪随机噪声的视觉特性.

在统计特性分析中, 图 4(a) 呈现了 5 幅原始灰度图像的直方图分布特征, 而图 4(b) 则是密文图像的统计直方图. 结果显示, 密文图像的像素值分布更为均匀, 表明加密方案有效破坏了原始图像的像素统计特性, 增强了抵抗统计分析攻击的能力. 同时, 密文的信息熵达到 7.9996 bit, 接近理想随机分布的熵值, 进一步印证了其随机性. 在此基础上, 通过相邻像素相关性分析验证方案对纯密文攻击的抵御能力.图 4(c)—(e) 的密文图像水平、垂直及对角方向相关性点图显示, 加密后像素间的相关性显著降低. 为进一步量化验证, 本文将上述 3 个方向的相关性指标与其他多图像加密方案进行对比, 从表 1 对比结果可见, 本方法在破坏图像像素相关性方面表现出与已有多图像加密方案相当甚至更优的性能, 进一步体现了所提算法在安全性方面的有效性与竞争力.

在差分攻击的常用手段分析中, 本文通过归一化像素对比率 (normalized pixel contrast ratio, NPCR) 和统一平均变化强度 (unified average changing intensity, UACI) 来衡量. 仿真中, 改变原始各个灰度图像中 (50, 60) 处的像素值后, 计算出的 NPCR 和 UACI 的结果中平均 NPCR 为 99.44%, 平均 UACI 为 33.04%. 表明密文对原始图像的微小变化具有高度敏感性, 可有效抵御差分攻击.

3.2 抗噪声与抗剪裁性分析

为评估加密系统的鲁棒性, 本文对密文进行了抗噪声和抗剪裁性能分析. 图 2(c), (d) 分别给出对密文添加强度为 0.5 的椒盐噪声和强度为 0.5 的高斯白噪声后, 对 5 张灰度图像解密的结果, 可以看出解密后图像依然能够区分原始图像的轮廓. 图 2(e) 分析了对密文裁切 1/6 后, 对 5 张灰度图像解密的结果, 可以看出解密后图像依然能够清晰恢复原始图像的主要特征. 为进一步量化分析, 表 2 列出了解密图像与原始图像的 SSIM 指标. 综合主观视觉评估与客观指标分析, 该加密系统表现出良好的抗噪声干扰能力和抗局部剪裁鲁棒性.

3.3 密钥敏感性分析

密钥是图像加密系统的核心要素. 本文数字域加密的密钥包括 Logistic 映射的初始值 x_0 和参数 μ, Henon 映射的初始值 (y_0,z_0)、参数 (α,β) 和缩放因子 δ, 以及构建测量矩阵 $\boldsymbol{\Phi}$ 所需的随机种子等. 光学加密的主要密钥包括 PSH, 中心波长 λ, 衍射距离 z_{s} 和 z_{h}. 混沌系统的混沌特性保证了对初始条件的极端敏感性. 即使密钥中任何一个参数发生微小改变, 产生的混沌序列或测量矩阵也会

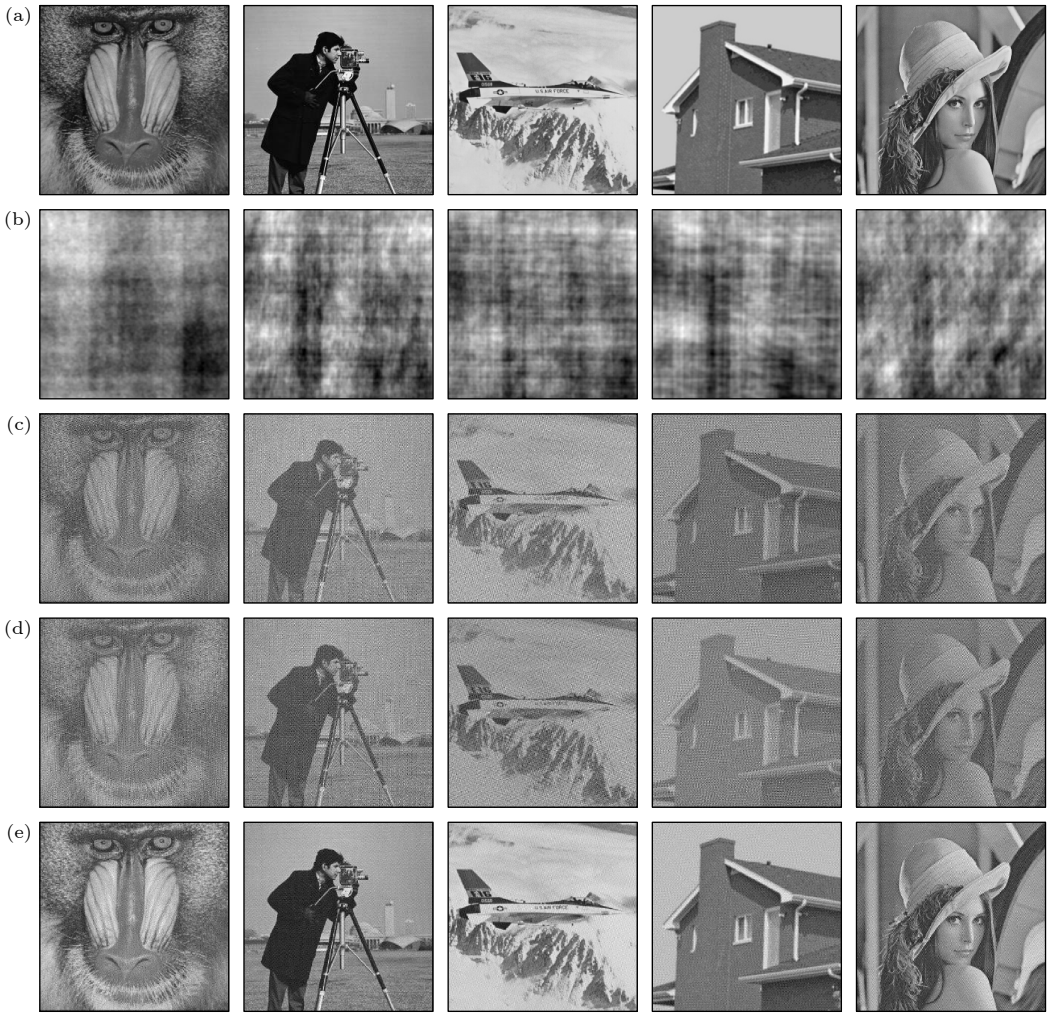


图 2 原始图像经 I-COACH 系统处理及其在不同干扰条件下解密图 (a) 原图; (b) 经过 I-COACH 系统后的物体全息图; (c) 对密文添加强度为 0.5 的椒盐噪声后的解密图; (d) 对密文添加强度为 0.5 的高斯白噪声后的解密图; (e) 对密文裁切 1/6 后的解密图

Fig. 2. Original image processed by the I-COACH system and decrypted images under different interference conditions: (a) Original image; (b) object hologram obtained after processing by the I-COACH system; (c) decrypted image after adding salt-and-pepper noise with an intensity of 0.5 to the ciphertext; (d) decrypted image after adding Gaussian white noise with an intensity of 0.5 to the ciphertext; (e) decrypted image after cropping 1/6 of the ciphertext.

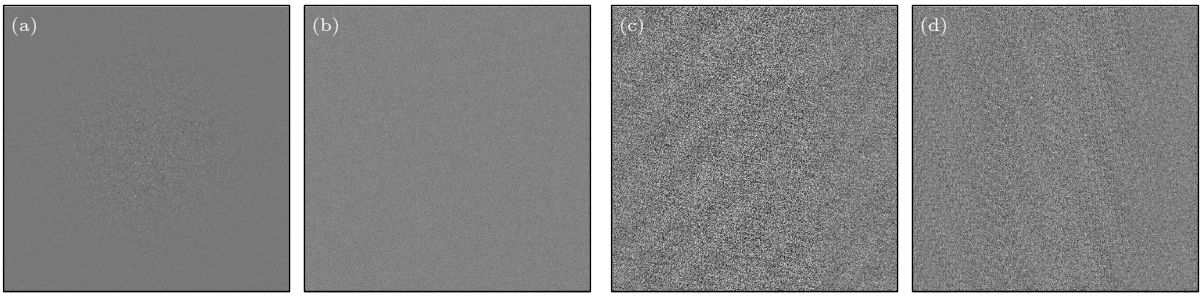


图 3 加密过程密钥图像以及不同采样率下的密文图像 (a) I-COACH 系统记录的点源全息图; (b) 在 $K = M$ 的情况下的密钥正交矩阵图像; (c) 在 $K = M$ 的情况下生成的最终密文图像; (d) 在 $K < M$, 取采样率为 0.7 的情况下生成的最终密文图像

Fig. 3. Key images in the encryption process and ciphertext images under different sampling rates: (a) Point-source hologram recorded by the I-COACH system; (b) orthogonal key matrix image under the condition of $K = M$; (c) final ciphertext image generated under the condition of $K = M$; (d) final ciphertext image generated with a sampling rate of 0.7 under the condition of $K < M$.

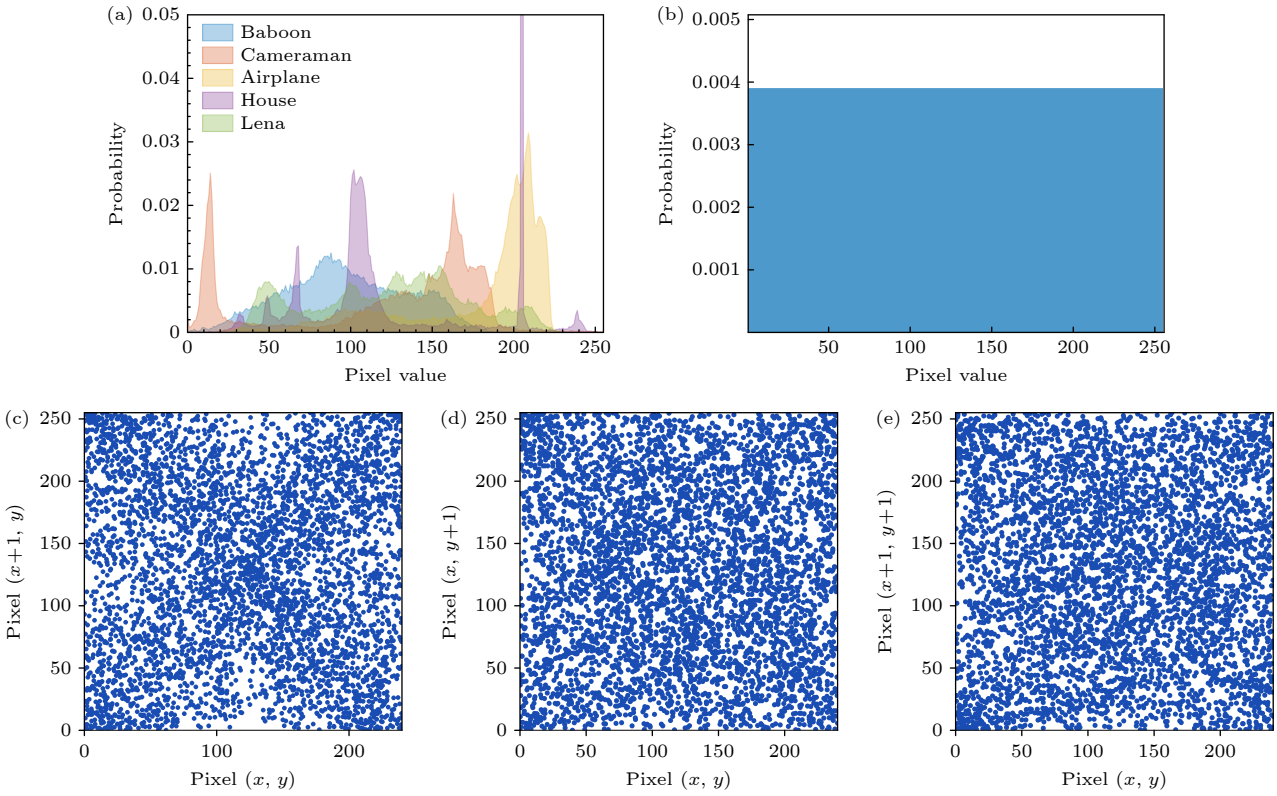


图 4 灰度图像及其加密图像的统计特性与相邻像素相关性分析 (a) 原始 5 张灰度图像的直方图; (b) 密文图像的直方图; (c) 水平方向相邻像素相关性点图; (d) 垂直方向相邻像素相关性点图; (e) 对角线方向相邻像素相关性点图

Fig. 4. Statistical characteristics and adjacent-pixel correlation analysis of grayscale images and their encrypted counterparts: (a) Histograms of the five original grayscale images; (b) histogram of the ciphertext image; (c) scatter plot of horizontal adjacent-pixel correlations; (d) scatter plot of vertical adjacent-pixel correlations; (e) scatter plot of diagonal adjacent-pixel correlations.

表 1 不同加密方案的相关系数比较

Table 1. Comparisons for the correlation coefficients of different encryption scheme.

方向	明文图像					密文(本文)	密文[10]	密文[7]
	狒狒	摄影师	飞机	房子	Lena			
水平	0.8248	0.9595	0.9279	0.9839	0.9543	–0.0047	0.0013	–0.0013
垂直	0.8686	0.9335	0.9358	0.9866	0.9158	–0.0305	0.0020	0.0283
对角线	0.7880	0.9056	0.8860	0.9722	0.8931	0.0078	0.0032	0.0465

截然不同, 导致解密失败, 重构出完全不同的图像. 这满足了加密算法的扩散特性. 此外, 结合 CS 的测量过程和混沌系统的双重扰动, 增强了抵抗已知明文/选择明文攻击的能力. 图 5(a) 所示为当采用错误的光学加密密钥 CPM 生成错误的 PSH, 而其他参数都正确时, 经过解密过程得到的对应 5 张灰度图像解密结果, 图 5(b) 所示为采用错误的测量矩阵密钥得到的对应解密结果. 如表 2 所示, 在上述两种密钥错误情形下, 解密图像与原始图像的 SSIM 均低于 0.2, 从图中无法识别出任何原始图像的有效信息. 显然所提加密算法对安全密钥的敏感度满足加密安全要求.

表 2 解密图像与原始图像的结构相似度

Table 2. The structural similarity of the decrypted image and the original image.

图像	子图像对应的SSIM				
	狒狒	摄影师	飞机	房子	Lena
图2(c)	0.5842	0.7766	0.6689	0.6863	0.6223
图2(d)	0.5988	0.7805	0.7078	0.6804	0.6214
图2(e)	0.8149	0.9094	0.8432	0.9440	0.8765
图5(a)	0.0145	0.1345	0.0756	0.1119	0.0281
图5(b)	0.0031	0.1249	0.1321	0.0373	0.0598
图5(c)	1.0000	1.0000	1.0000	1.0000	1.0000
图5(d)	0.6011	0.6064	0.6284	0.6011	0.6202

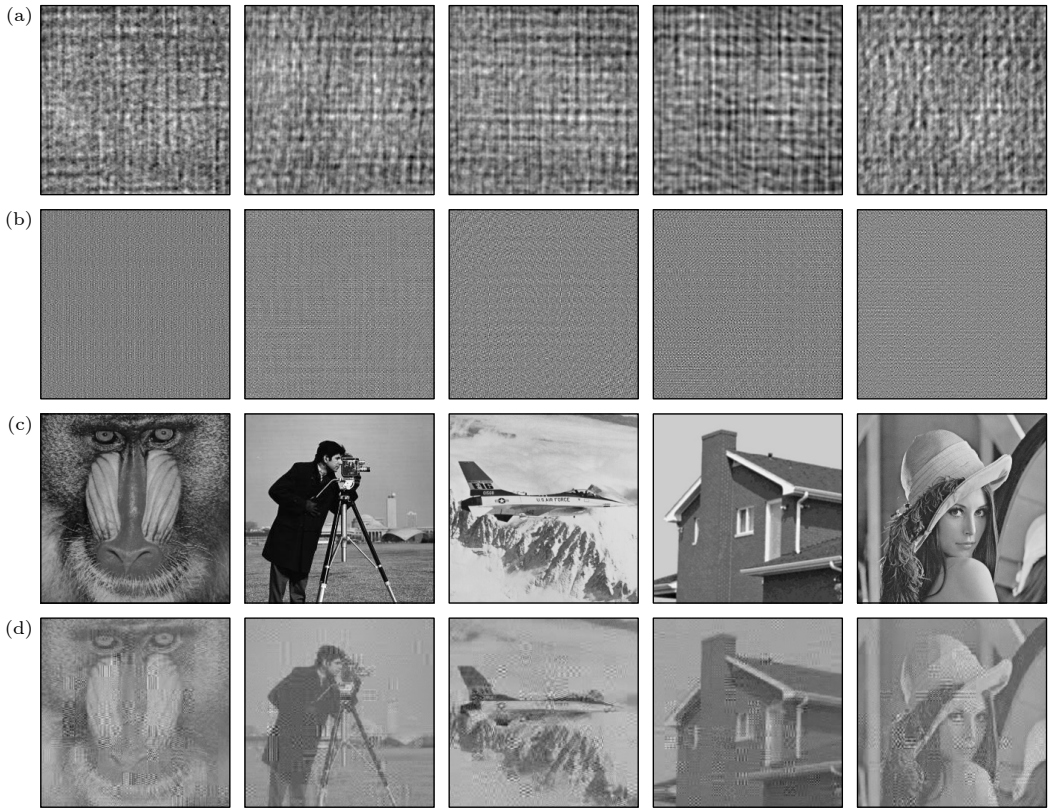


图 5 解密图像在不同条件下的视觉表现 (a) 采用错误 CPM 生成错误的 PSH 后得到的解密图像; (b) 采用错误的测量矩阵密钥后得到的解密图像; (c) 在 $K = M$ 的情况下解密后的图像; (d) $K < M$, 取采样率为 0.7 的情况下解密后的图像

Fig. 5. Visual performance of decrypted images under different conditions: (a) Decrypted image obtained using an incorrectly generated PSH with erroneous CPM; (b) decrypted image obtained using an incorrect measurement matrix key; (c) decrypted image under the condition of $K = M$; (d) decrypted image with a sampling rate of 0.7 under the condition of $K < M$.

密钥敏感度直接决定了系统的安全强度. 一般而言, 密钥敏感度越高, 系统的抗攻击能力越强. 为验证光学加密过程的密钥敏感性, 图 6 分析了中心波长 λ, 衍射距离 z_{s} 和 z_{h} 对解密效果的影响. 在图 6(b) 中, 显示了当中心波长 λ 有偏差时, 对 5 张不同灰度图像解密得到的 SSIM 变化曲线. 从曲线图中可以看出, 加密方法对中心波长 λ 的变化极为敏感, 当波长变化在 1 nm 的情况下, SSIM 值就大幅下降至 0.4 以内. 图 6(c), (d) 显示了当物距和像距分别有偏差时, 对 5 张不同灰度图像解密得到的 SSIM 变化曲线. 从曲线图中可以看出, 加密方法对衍射距离的变化极为敏感, 当衍射距离变化在 2 mm 的情况下, SSIM 值就大幅下降至 0.4 以内. 可见加密方法对中心波长以及衍射距离有着极高的敏感性. 为验证数字加密过程的密钥敏感性, 本文对混沌系统 Logistic 映射参数、Henon 映射参数及其初始值分别施加微小扰动, 在保持其余参数不变的情况下进行解密. 仿真结果如表 3 所示, 当密钥任一参数发生微小扰动时, 5 张解密图像均严重失真, 平均均方误差由零急剧上升至 10^4 量级, 平均峰值信噪比由无穷大降至 8 dB 以下, 平均 SSIM 接近 0, 说明解密图像与原图几乎无相关性. 这充分证明了所提算法对密钥的高度敏感性和安全性.

3.4 效率与压缩性能评价

在 $K = M$ 的情况下, 密钥正交矩阵图像如图 3(b) 所示, 解密后的图像如图 5(c) 所示, 与原始图像相比最小均方误差为 0, SSIM 均为 1, 可实现无损重建. 在 $K < M$, 取采样率为 0.7 的情况下, 最终加密后的图像如图 3(d) 所示, 原始输入图像的数据大小为 5 张 256×256 的 8 位灰度图像, 而获得的密文分辨率大小为 479×479 像素, 由此可见, 密文数据量相较于明文总数据量减少了约 30%. 如图 5(d) 与表 2 所示, 解密图像与原始每张图像相比, SSIM 均可达到 0.6 以上, 且不同图像的峰值信噪比均超过 25 dB, 表明在允许的误差范围下能够较好地对图像进行重构. 此外, 整个解密和

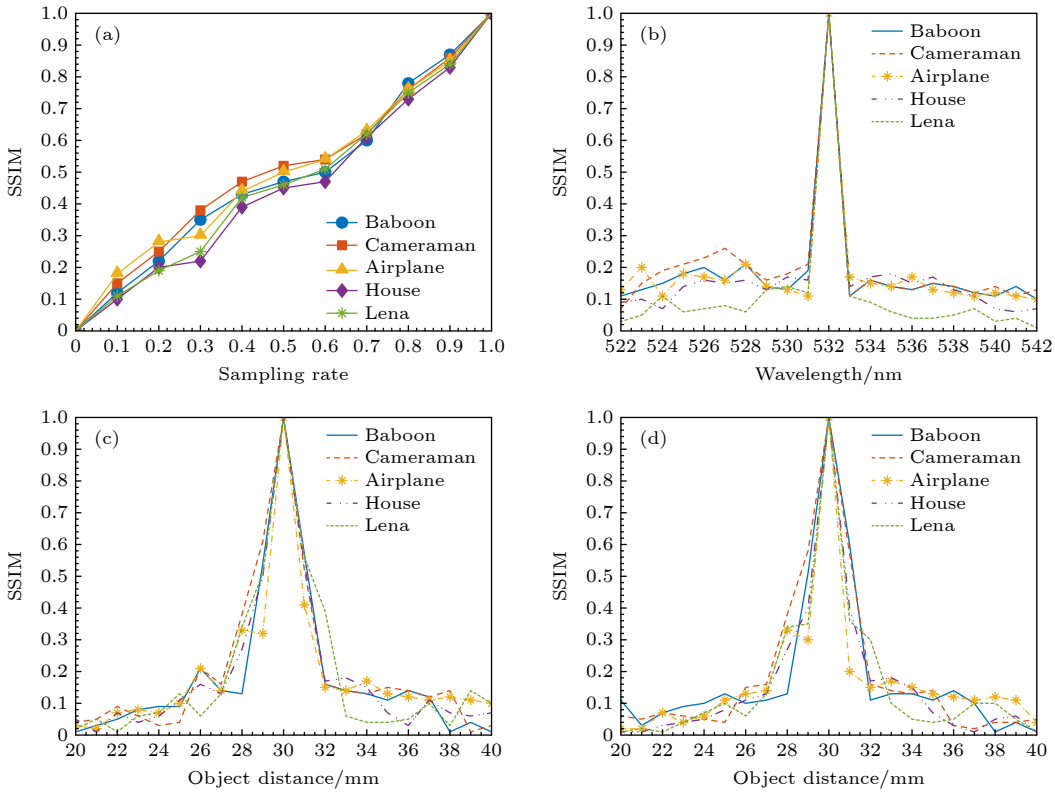


图 6 不同条件对解密图像 SSIM 的影响 (a) 不同采样率下解密后图像的 SSIM 变化曲线; (b) 中心波长 λ 偏差解密后得到的 SSIM 变化曲线; (c) 衍射距离 z_{s} 偏差解密后得到的 SSIM 变化曲线; (d) 衍射距离 z_{h} 偏差解密后得到的 SSIM 变化曲线

Fig. 6. Influence of different conditions on the SSIM of decrypted images: (a) Variation curve of SSIM for decrypted images under different sampling rates; (b) SSIM variation curve for decrypted images with central wavelength deviation; (c) SSIM variation curve for decrypted images with diffraction distance deviation; (d) SSIM variation curve for decrypted images with diffraction distance deviation.

表 3 混沌系统密钥参数敏感性分析

Table 3. Sensitivity analysis of key parameters in chaotic systems.

评价指标	扰动参数(微小扰动值 $\Delta = 0.0001$)					
	$\alpha+\Delta$	$\beta+\Delta$	$\mu+\Delta$	$x_0+\Delta$	$y_0+\Delta$	$z_0+\Delta$
平均均方误差/10^4	1.0781	1.0983	1.2914	1.2738	1.0612	1.0820
平均SSIM	0.1985	0.1921	0.1868	0.2022	0.2050	0.1947
平均峰值信噪比/dB	7.8042	7.7237	7.0202	7.0797	7.8728	7.7885

重构过程的总耗时为 10.01 s, 表明了算法具有较高的运行效率. 图 6(a) 分析了在不同采样率下各解密结果与原始明文之间的 SSIM, 进一步验证了该方法的稳健性和适用性.

4 实验结果与分析

为验证基于 I-COACH 的多图像双重混沌压缩加密方法在实际光学环境中的可行性, 本研究搭建了对应的光学验证平台. 该加密系统的实验光路配置如图 1(a) 所示. 本文采用单色 LED(大恒光学 GCI-060403, 最大功率 3 W, 中心波长 $\lambda_{\mathrm{LED}}=528.2$ nm, 光谱带宽 $\Delta\lambda_{\mathrm{LED}}=25$ nm) 作为非相干光源. 透镜 L_1 与 L_2 之间的距离约为 180 mm, 其焦距分别为 30 mm 和 150 mm. 明文图像是 USAF-1951 光学分辨率测试板的一部分, 本文选用数字“2”, “3”和“4”三幅中心明文图像, 它们与 SLM(大恒光学 GCI-770402, 反射式 SLM, 1280×720 像素, 像素间距 6.3 μm) 之间的距离 z_{s} 约为 300 mm. SLM 和图像传感器 (大恒图像水星系列 MER-130-30 UM, 1280×1024 像素, 像素间距 5.2 μm) 之间的距离 z_{h} 约为 150 mm. 透镜成像中得到的明文信息如图 7(a) 所示. 相应的 PSH 和 3 幅物体全息图均由 CCD 记录, 分别如图 7(b), (d)—(f) 所示. 经过双重混沌压缩加密方法后的最终密文如

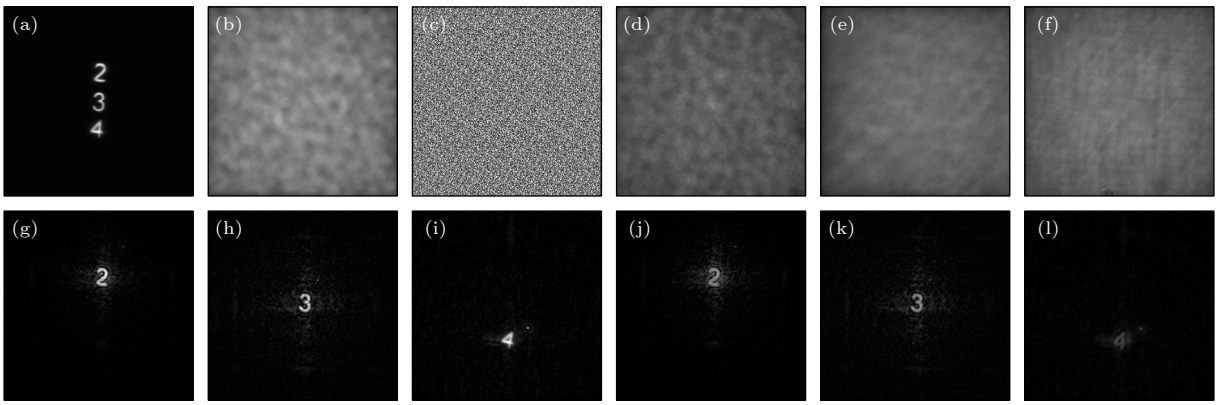


图 7 基于 I-COACH 的多图像双重混沌压缩加密实验结果 (a) 透镜成像的明文信息; (b) 记录的 PSH 图像; (c) 密文; (d)—(f) 数字“2”, “3”和“4”的物体全息图; (g)—(i) 解密重建图像; (j)—(l) 压缩采样率为 0.7 时的解密图像

Fig. 7. Experimental results of I-COACH-based multi-image dual-chaotic compression encryption: (a) Plaintext obtained by lens imaging; (b) recorded PSH image; (c) ciphertext; (d)–(f) holograms of numbers “2”, “3”, and “4”; (g)–(i) decrypted reconstruction images; (j)–(l) decrypted images at 0.7 compression sampling ratio.

图 7(c) 所示, 用肉眼无法从图中识别出任何明文的相关信息. 之后对加密图进行解密, 得到解密图像如图 7(g)—(i) 所示. 由以上实验数据可知, 提出的物理-数字协同加密方法可以精确地恢复各个明文图像. 进一步, 本文对密文图像进行了采样率为 0.7 的压缩处理, 得到的解密结果如图 7(j)—(l) 所示, 可以看出系统在数据压缩条件下仍能保持原始明文的基本轮廓特征, 验证了所提方法的鲁棒性.

5 结 论

本文提出的方法结合了 I-COACH 的光学特性、DCT 的能量压缩能力、混沌系统的非线性动力学特性以及 CS 的数据缩减与加密功能, 构建了一个物理-数字协同的多图像加密架构, 从而在安全性与压缩效率方面实现同步提升. 具体而言, 该方法首先利用 I-COACH 系统在物理层面将多幅明文图像编码为物体全息图, 实现初步光学加密; 随后, 在数字域中对记录的全息图进行分块离散余弦变换以获取稀疏系数, 并依次采用 Logistic 与 Henon 混沌映射对系数进行双重扰动, 增强密钥敏感性与随机性; 最后, 通过 CS 对扰动后的数据进行测量与压缩, 在提升安全性的同时有效减少了约 30% 的数据量. 这种多阶段、多技术协同的设计策略有效克服了单一加密技术的局限性, 最终构建了一个具有更高安全性、更大密钥空间且兼具数据压缩能力的图像加密系统.

参考文献

[1] Wang Y, Wong K W, Liao X F, Chen G R 2011 *Appl. Soft Comput.* **11** 514
[2] Kaur M, Kumar V 2020 *Arch. Comput. Method. E.* **27** 15
[3] SaberiKamarposhti M, Ghorbani A, Yadollahi M 2024 *Chaos Soliton. Fract.* **178** 114361
[4] Patro K A K, Acharya B 2021 *Nonlinear Dynam.* **104** 2759
[5] Zhou N R, Tong L J, Zou W P 2023 *Signal Process.* **211** 109107
[6] Zhou N R, Hu L L, Huang Z W, Wang M M 2024 *Expert Syst. Appl.* **238** 122052
[7] Sui L S, Zhou B, Ning X J, Tian A L 2016 *Opt. Express* **24** 499
[8] Wang X G, Li M, Yu N N, Xi S X, Wang X L, Lang L Y 2019 *Acta Phys. Sin.* **68** 240503 (in Chinese) [王雪光, 李明, 于娜娜, 席思星, 王晓雷, 郎利影 2019 物理学报 **68** 240503]
[9] Hazer A, Yıldırım R 2021 *J. Opt.* **23** 113501
[10] Wang Y H, Wu Y X, Fang H, Zhang X, Su Y G 2024 *J. Opt.* **53** 4997
[11] Fang G Q, Lin H, Wang S Y, Peng P, Fang Z Y 2025 *Acta Phys. Sin.* **74** 064205 (in Chinese) [方国全, 林瀚, 王思越, 彭璞, 方哲宇 2025 物理学报 **74** 064205]
[12] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[13] Vijayakumar A, Rosen J 2017 *Opt. Express* **25** 13883
[14] Rosen J, Anand V 2024 *Photonics.* **11** 115
[15] Zhang M H, Wan Y H, Man T L, Zhang W X, Zhou H Q 2024 *Opt. Laser. Eng.* **173** 107929
[16] Yu X L, Wang K W, Xiao J J, Li X F, Sun Y Q, Chen H 2022 *Opt. Lett.* **47** 409
[17] Yang L, Yang J P, Huang T, Li J S, Zhang Q N, Di J L, Zhong L Y 2024 *Opt. Laser Technol.* **169** 110096
[18] Yu X L, Chen H, Xiao J J, Sun Y Q, Li X F, Wang K W 2022 *Opt. Commun.* **510** 127889
[19] Zhang W B, Zou Z H, Ren Y C, Sun X D, Yu Y X, Tsai C W, Zhang Z J 2024 *Opt. Express* **32** 27444
[20] Liu H J, Wang X Y 2011 *Opt. Commun.* **284** 3895
[21] Li Y P, Wang C H, Chen H 2017 *Opt. Laser. Eng.* **90** 238
[22] Wei D Y, Jiang M J, Deng Y 2023 *Expert Syst. Appl.* **213** 119074
[23] Chai X L, Gan Z H, Chen Y R, Zhang Y S 2017 *Signal Process.* **134** 35
[24] Chai X L, Zheng X Y, Gan Z H, Han D J, Chen Y R 2018 *Signal Process.* **148** 124
[25] Shi H, Wang L D 2019 *Acta Phys. Sin.* **68** 200501 (in

Chinese) [石航, 王丽丹 2019 物理学报 **68** 200501]
[26] Xu Q Y, Sun K H, He S B, Zhu C X 2020 *Opt. Laser. Eng.* **134** 106178
[27] Qin Y, Man T L, Wan Y H, Wang X 2023 *Laser Optoelectron. Prog.* **60** 0400001 (in Chinese) [秦怡, 满天龙, 万玉红, 王兴 2023 激光与光电子学进展 **60** 0400001]
[28] Wang C, Song L 2023 *Inf. Sci.* **642** 119166
[29] Wen H P, Yang L C, Bai C X, Lin Y T, Liu T Y, Chen L, He D J 2024 *Sci. Rep.* **14** 8805
[30] Jia J W, Zhang Z, Zhou H Y, Chen X B 2025 *Opt. Precis. Eng.* **33** 624 (in Chinese) [贾静雯, 张钊, 周红艳, 陈雪波 2025 光学精密工程 **33** 624]
[31] Eltoukhy M M, Alsubaei F S, Elnabawy Y M, Hosny K M 2025 *Alex. Eng. J.* **125** 367
[32] Hu L L, Chen M X, Wang M M, Zhou N R 2024 *Chaos Soliton. Fract.* **188** 115521
[33] Huang L L, Gao H 2024 *IEEE Trans. Circuits Syst. I-Regul. Pap.* **71** 3726
[34] Zhou L L, Chen P Y, Tan F 2025 *Phys. Scr.* **100** 025223
[35] Lan Y C, Wang C M 2025 *IEEE Access* **13** 43316
[36] Acharya B, Sravan J V, Potnuru D J R, Patro K A K 2025 *IEEE Access* **13** 62773
[37] Wei J J, Zhang M, Tong X J 2022 *Entropy* **24** 784
[38] Hosny K M, Elnabawy Y M, Salama R A, Elshewey A M 2024 *Sci. Rep.* **14** 30597
[39] Zhang Z Y, Mou J, Banerjee S, Cao Y H 2024 *Chin. Phys. B* **33** 020503
[40] Xue L L, Ai C H, Ge Z H 2025 *Phys. Scr.* **100** 035539
[41] Wang L Y, Cheng H 2019 *Entropy* **21** 960
[42] Hénon M 1976 *Commun. Math. Phys.* **50** 69

Multi-image dual-chaotic compression encryption method for interferenceless coded aperture correlation holography*

LI Jia [1)] YU Xuelian [1)†] ZHANG Yuehui [1)] NIU Jia [2)4)] HE Lei [5)]
SUN Yanqian [3)4)] LI Xiufang [3)4)]

1) (*Heilongjiang Provincial Key Laboratory of Quantum Control, School of Measurement and Communication Engineering, Harbin University of Science and Technology, Harbin* 150080, *China*)

2) (*Shanxi Key Laboratory of Quantum Information and Quantum Optoelectronic Devices, School of Physics, Xi'an Jiaotong University, Xi'an* 710049, *China*)

3) (*Key Laboratory of Luminescence and Optical Information of Ministry of Education, Beijing Jiaotong University, Beijing* 100044, *China*)

4) (*Daheng New Epoch Technology, Inc., Beijing* 100085, *China*)

5) (*Harbin Xinguang Optic-electronics Technology Co., Ltd., Harbin* 150078, *China*)

(Received 10 November 2025; revised manuscript received 22 December 2025)

Abstract

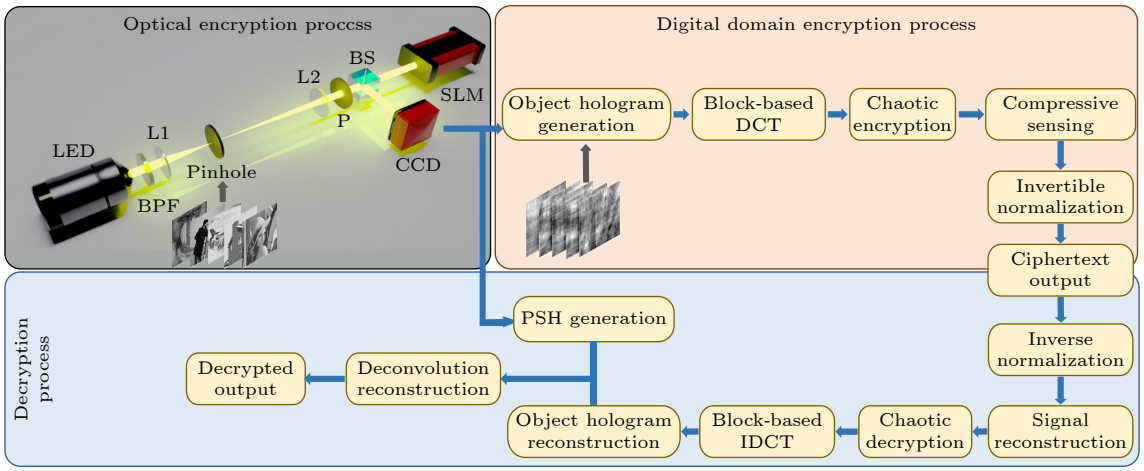
To improve the security and efficiency of multi-image encryption, this study proposes a hybrid encryption method that combines interferenceless coded aperture correlation holography (I-COACH) with chaotic modulation and compressed sensing techniques. This method constructs a dual-layer encryption framework that integrates optical and digital processing, thereby overcoming the limitations of single-domain schemes.

In the optical layer, I-COACH is used to encode multiple input images by recording their point spread holograms without interference, providing initial encryption and resistance to physical attacks. Then, resulting hologram is processed using block-wise discrete cosine transform (DCT) to achieve sparsity. Dual chaotic sequences perturb DCT coefficients to enhance key sensitivity and randomness. Finally, compressed sensing is used to achieve secondary encryption while reducing the data volume by 30%, enabling efficient and secure

* Project supported by the Natural Science Foundation of Heilongjiang Province, China (Grant No. PL2024F020), the Postdoctoral Research Startup Foundation of Heilongjiang Province, China, and the Industry-University Collaborative Education Program of the Ministry of Education, China (Grant No. 231104090250214).

† Corresponding author. E-mail: yuxuelian@hrbust.edu.cn

storage or transmission. The experimental results show that the proposed method against differential attacks achieves an average number of pixels change rate (NPCR) of 99.44% and a unified average changing intensity (UACI) of 33.04%, with a ciphertext entropy of 7.9996 bit. Moreover, it exhibits excellent encryption performance in terms of key sensitivity, robustness, and resistance to statistical analysis. This method provides a practical solution for secure image application scenarios such as medical imaging and surveillance.



Keywords: multi-image encryption, interferenceless coded aperture correlation holography, compressed sensing, chaotic systems

DOI: 10.7498/aps.75.20251533 **CSTR:** 32037.14.aps.75.20251533

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

无干涉编码孔径相关全息的多图像双重混沌压缩加密方法

李佳　于雪莲　章跃辉　牛佳　贺磊　孙彦乾　李秀芳

Multi-image dual-chaotic compression encryption method for interferenceless coded aperture correlation holography

LI Jia　YU Xuelian　ZHANG Yuehui　NIU Jia　HE Lei　SUN Yanqian　LI Xiufang

引用信息 Citation: Acta Physica Sinica, 75, 050404 (2026)　DOI: 10.7498/aps.75.20251533
CSTR: 32037.14.aps.75.20251533
在线阅读 View online: https://doi.org/10.7498/aps.75.20251533
当期内容 View table of contents: http://wulixb.iphy.ac.cn
