# 基于二维置换加密鬼成像研究*

赵一宁 陈琳珊 孔令鑫 王翀 任承 徐宝龙† 曹德忠‡

(烟台大学物理与电子信息学院, 烟台 264005)

(2025 年 5 月 3 日收到; 2025 年 5 月 30 日收到修改稿)

本文提出了一种基于鬼成像的二维图像置换加密方案, 以二维随机矩阵之 Kronecker 积作为测量矩阵, 结合置换矩阵, 形成灵活多变的加密方式. 加密方案以图像的二维分布为基准, 采用两个随机矩阵和两个置换矩阵, 对图像进行加密操作. 这些矩阵及其排序信息都是图像加密的有效手段. 只有当随机矩阵和置换矩阵的具体形式及其排序信息完全正确时, 才能够成功解密图像. 具体而言, 在鬼成像研究中, 首先利用矩阵相乘及其 Kronecker 积, 将随机矩阵和置换矩阵制备成实验所需的测量矩阵, 再将测量矩阵形成一系列待投影散斑图案. 实验上, 采用空间光调制器加载物体和随机散斑图案, 利用 CCD 作为桶探测器采集桶测量信号, 研究了 8 种排序的图像置换加密及相应解密方案. 方案所提出的二维置换鬼成像加密方法灵活多变, 也为图像水印与图像隐匿等图像处理技术提供了一种新思路.

**关键词:** 鬼成像, 置换加密, Kronecker 积

**PACS:** 42.15.Eq, 42.30.–d, 42.30.Va **DOI:** 10.7498/aps.74.20250592

**CSTR:** 32037.14.aps.74.20250592

## 1 引 言

计算鬼成像 (computational ghost imaging, CGI)[1] 技术得到了越来越广泛的关注. 在 CGI 中, 一系列的散斑图案照亮物体, 桶探测器收集物光并转换为一维桶测量信号. 物体图像不能从散斑图案或桶测量信号中直接获得, 而是联合散斑图案和桶测量信号, 进行关联计算才能重建图像 [2–4]. 随后, 学者提出压缩感知算法, 用以提高图像重建质量 [5,6]. 近期, CGI 的图像重建效率得到深入研究 [7–14]. 在伪逆鬼成像中 [7–10], 利用奇异值分解方法获得随机测量矩阵的伪逆矩阵, 可以极大缩短图像重建时间, 提高图像重建质量. Schmidt 正交鬼成像 [11,12] 将测量矩阵逐行正交化, 再进一步对测量矩阵和桶测量信号处理, 可以提高 CGI 的图像重建性能. 将鬼成像与基于卷积神经网络的深度学习相结合, 鬼成像能够以超低采样率重建高质量的图像 [13,14].

鬼成像实验中经常使用随机散斑, 因而鬼成像具有自然的图像加密特点. 加之与图像加密技术相结合, 鬼成像加密获得了广泛的研究 [15–24]. Zhang 等 [15] 提出了一种基于压缩采样的压缩图像加密方法. 结合置换矩阵, Zhang 和 Zhao 等 [18] 研究了随机置换桶测量信号的 CGI 图像加密. Wu 等 [19] 提出了一种位置复用的多图像加密方案. Shi 等 [20] 研究了 CGI 中多幅图像的同时融合成像和加密. Zhu 等 [21] 在 CGI 中使用指纹相位掩模对图像进行加密. Kang 等 [22] 使用公钥加密技术对图像进行加密. Liu 等 [23] 在 CGI 中使用离散余弦变换和正交散斑对图像进行加密. Liu 等 [24] 基于频域扩展技术, 研究了扩频鬼成像加密图像. 这些基于 CGI 的图像加密研究利用了特定的图像变换和随机置换.

* 国家自然科学基金 (批准号: 62105278, 11674273) 资助的课题.

† 通信作者. E-mail: baolongxu@ytu.edu.cn

‡ 通信作者. E-mail: dzcao@ytu.edu.cn

 

本文以图像的二维随机变换为基准, 采用两个随机矩阵和两个置换矩阵, 研究了二维情形下的CGI图像加密方案. 在实验中, 先将两随机矩阵通过Kronecker积获得随机测量矩阵, 然后根据随机矩阵制备一系列投影散斑图. 最后将随机散斑和图像一起加载到空间光调制器 (spatial light modulator, SLM) 上. 具体而言, 激光束照射到SLM上, 以电荷耦合器件 (charge coupled device, CCD) 作为桶探测器, 通过透镜收集物光信号转换为桶测量信号. 由于多个矩阵可以任意排列, 矩阵的排列顺序也是图像加密的关键因素之一, 因此可以实现灵活多变的图像加密方法.

在图像解密过程中, 采用基于截断奇异值分解 (truncated singular value decomposition, TSVD) 的伪逆鬼成像原理, 充分利用两个随机矩阵的伪逆矩阵、置换矩阵以及矩阵顺序, 高效重建二维图像. TSVD方法能够克服噪声, 提高图像质量. 在图像重建过程中, 可以将TSVD应用于两个随机矩阵中的一个或两个, 即可恢复图像. 总之, 只有准确获知随机矩阵、置换矩阵及其序列信息并正确使用, 才能成功地进行图像解密.

## 2 方案理论

在鬼成像实验中, 将一系列散斑图像投影至物体, 探测器收集物光信息并转换为桶测量信号. 一般而言, 为了便于理论处理, 考虑物体分布为一维列向量 $\boldsymbol{x}$, 每一个投影散斑图也考虑成一维行向量, 则所有散斑图像构成测量矩阵 $\boldsymbol{A}$. 这样, 鬼成像的测量过程可表示成为矩阵形式, 桶探测器收集的一维列向量桶测量信号为

$$\boldsymbol{y}_{M\times 1}=\boldsymbol{A}_{M\times N}\boldsymbol{x}_{N\times 1}, \tag{1}$$

其中, 下标表示矩阵和向量的大小.

当考虑物体为二维情形, 则可以通过两个正交变换矩阵的Kronecker积实现基于混合变换的鬼成像[25]. 同样地, 我们采用两个随机矩阵 $\boldsymbol{L}_{M\times M}$ 和 $\boldsymbol{R}_{N\times N}$ 来实现CGI, 桶测量信号亦为二维分布:

$$\boldsymbol{Y}_{M\times N}=\boldsymbol{L}_{M\times M}\boldsymbol{X}_{M\times N}\boldsymbol{R}^{\mathrm{T}}_{N\times N}, \tag{2}$$

其中, $\boldsymbol{X}$ 是二维图像, T表示矩阵转置.

如果将 (2) 式中的二维分布 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 变形为列向量, 则测量矩阵为 $\boldsymbol{L}$ 与 $\boldsymbol{R}$ 的Kronecker积 $\boldsymbol{A}=\boldsymbol{L}\otimes\boldsymbol{R}$. 仿照 (1) 式的形式, (2) 式改写为

$$\boldsymbol{y}=(\boldsymbol{L}\otimes\boldsymbol{R})\,\boldsymbol{x}=\boldsymbol{A}\boldsymbol{x}, \tag{3}$$

其中, 向量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 由二维的 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 向量化得到; $\otimes$ 表示矩阵的Kronecker积. (3) 式中忽略了表示矩阵大小的下标.

本文考虑图像置换加密, 采用两个二维置换矩阵 $\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$, 将它们插入 (2) 式右边 $\boldsymbol{X}$ 的两侧来实现加密. 显然, 这种图像置换加密的方案是非常灵活的, 其特点在于: 1) 矩阵 $\boldsymbol{L}$ 和 $\boldsymbol{R}$ 是随机的, 2) 置换矩阵 $\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 是由单位矩阵随机置换生成的, 3) 在 (2) 式中, 置换矩阵可以被放在矩阵序列中的任何位置.

二维图像置换加密可以按照下列8种方式进行. 如果只使用一个置换矩阵 $\boldsymbol{P}_1$, 可以将物体图像加密为以下两种方式:

$$\boldsymbol{P}_1\boldsymbol{L}\boldsymbol{X}\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_1,\quad \boldsymbol{L}\boldsymbol{P}_1\boldsymbol{X}\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_2. \tag{4}$$

同样地, 如果只使用置换矩阵 $\boldsymbol{P}_2$, 则有

$$\boldsymbol{L}\boldsymbol{X}\boldsymbol{P}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_3,\quad \boldsymbol{L}\boldsymbol{X}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_4. \tag{5}$$

如果两个置换矩阵都使用了, 则有4种加密方式:

$$\begin{aligned}&\boldsymbol{P}_1\boldsymbol{L}\boldsymbol{X}\boldsymbol{P}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_5,\quad \boldsymbol{P}_1\boldsymbol{L}\boldsymbol{X}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_6,\\ &\boldsymbol{L}\boldsymbol{P}_1\boldsymbol{X}\boldsymbol{P}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_7,\quad \boldsymbol{L}\boldsymbol{P}_1\boldsymbol{X}\boldsymbol{R}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_8.\end{aligned} \tag{6}$$

在上述8种加密方式中, 测量矩阵分别为

$$\begin{aligned}&\boldsymbol{A}_1=(\boldsymbol{P}_1\boldsymbol{L})\otimes\boldsymbol{R},\quad \boldsymbol{A}_2=(\boldsymbol{L}\boldsymbol{P}_1)\otimes\boldsymbol{R},\\ &\boldsymbol{A}_3=\boldsymbol{L}\otimes\left(\boldsymbol{R}\boldsymbol{P}_2^{T}\right),\quad \boldsymbol{A}_4=\boldsymbol{L}\otimes\left(\boldsymbol{P}_2^{T}\boldsymbol{R}\right),\\ &\boldsymbol{A}_5=(\boldsymbol{P}_1\boldsymbol{L})\otimes\left(\boldsymbol{R}\boldsymbol{P}_2^{T}\right),\quad \boldsymbol{A}_6=(\boldsymbol{P}_1\boldsymbol{L})\otimes\left(\boldsymbol{P}_2^{T}\boldsymbol{R}\right),\\ &\boldsymbol{A}_7=(\boldsymbol{L}\boldsymbol{P}_1)\otimes\left(\boldsymbol{R}\boldsymbol{P}_2^{T}\right),\quad \boldsymbol{A}_8=(\boldsymbol{L}\boldsymbol{P}_1)\otimes\left(\boldsymbol{P}_2^{T}\boldsymbol{R}\right).\end{aligned} \tag{7}$$

这些测量矩阵可用以形成实验所用投影散斑图, 即将测量矩阵的行向量构造成系列二维分布图.

依据图像加密的反过程, 则可解密得到原图像信息. 以 (4) 式的第一个公式为例, 解密图像可以通过下面公式得到:

$$\boldsymbol{X}_1=\boldsymbol{L}^{-1}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_1\left(\boldsymbol{R}^{\mathrm{T}}\right)^{-1}=\boldsymbol{L}^{-1}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_1\left(\boldsymbol{R}^{-1}\right)^{\mathrm{T}}, \tag{8}$$

其中, $\boldsymbol{L}^{-1}$ 和 $\boldsymbol{R}^{-1}$ 分别是矩阵 $\boldsymbol{L}$ 和 $\boldsymbol{R}$ 的伪逆矩阵. 使用奇异值分解的方法可以将矩阵 $\boldsymbol{L}$ 和 $\boldsymbol{R}$ 展开为 $\boldsymbol{L}=\boldsymbol{U}_L\boldsymbol{S}_L\boldsymbol{V}_L^{\mathrm{T}}$ 和 $\boldsymbol{R}=\boldsymbol{U}_R\boldsymbol{S}_R\boldsymbol{V}_R^{\mathrm{T}}$. 由Moore-Penrose定理[26], 它们的伪逆矩阵为

$$\boldsymbol{L}^{-1}=\boldsymbol{V}_L\boldsymbol{S}_L^{-1}\boldsymbol{U}_L^{\mathrm{T}},\quad \boldsymbol{R}^{-1}=\boldsymbol{V}_R\boldsymbol{S}_R^{-1}\boldsymbol{U}_R^{\mathrm{T}}, \tag{9}$$

其中, $\boldsymbol{U}_L(\boldsymbol{U}_R)$ 和 $\boldsymbol{V}_L(\boldsymbol{V}_R)$ 是幺正矩阵, $\boldsymbol{S}_L(\boldsymbol{S}_R)$ 是一个对角矩阵.

在实验过程中, 噪声会降低重建图像的质量. Chen 等[27] 提出了一种截断奇异值分解与空间滤波相结合的方法来改善伪逆鬼成像. 截断奇异值分解法的核心策略是截断 (9) 式中对角矩阵 $\boldsymbol{S}_L$ 和 $\boldsymbol{S}_R$ 中较小的值, 伪逆矩阵 $\boldsymbol{L}^{-1}$ 和 $\boldsymbol{R}^{-1}$ 可以近似表示为

$$\tilde{\boldsymbol{L}} = \boldsymbol{V}_L\left[\boldsymbol{S}_L^{-1}\right]^{(r_1)}\boldsymbol{U}_L^{\mathrm{T}},\quad \tilde{\boldsymbol{R}} = \boldsymbol{V}_R\left[\boldsymbol{S}_R^{-1}\right]^{(r_2)}\boldsymbol{U}_R^{\mathrm{T}}, \tag{10}$$

其中, $r_1$ 与 $r_2$ 分别小于 $\boldsymbol{S}_L$ 和 $\boldsymbol{S}_R$ 的大小, $(r_1)$ 表示取矩阵 $\boldsymbol{S}_L$ 对角线上前 $r_1$ 个值, $(r_2)$ 表示取矩阵 $\boldsymbol{S}_R$ 对角线上前 $r_2$ 个值. 截断后的对角矩阵为

$$\left[\boldsymbol{S}_L^{-1}\right]^{(r_1)} = \mathrm{diag}\left(s_{L,1}^{-1}, s_{L,2}^{-1}, \cdots, s_{L,r_1}^{-1}\right),$$

$$\left[\boldsymbol{S}_R^{-1}\right]^{(r_2)} = \mathrm{diag}\left(s_{R,1}^{-1}, s_{R,2}^{-1}, \cdots, s_{R,r_2}^{-1}\right).$$

依据截断奇异值的伪逆矩阵 $\tilde{\boldsymbol{L}}$ 和 $\tilde{\boldsymbol{R}}$, 以及 (4) 式—(6) 式, 可以通过 (11) 式对 8 种加密图像分别进行解密, 否则无法复原正确的图像信息:

$$\begin{aligned}
&\boldsymbol{X} = \tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_1\tilde{\boldsymbol{R}}^{\mathrm{T}},\quad \boldsymbol{X} = \boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_2\tilde{\boldsymbol{R}}^{\mathrm{T}},\\
&\boldsymbol{X} = \tilde{\boldsymbol{L}}\boldsymbol{Y}_3\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}},\quad \boldsymbol{X} = \tilde{\boldsymbol{L}}\boldsymbol{Y}_4\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}},\\
&\boldsymbol{X} = \tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_5\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}},\quad \boldsymbol{X} = \tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_6\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}},\\
&\boldsymbol{X} = \boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_7\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}},\quad \boldsymbol{X} = \boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_8\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}.
\end{aligned} \tag{11}$$

## 3 实验系统及测量结果

实验装置图如图 1(a) 所示. 从二极管激光器 (laser diode, LD) 发出的一束激光 (波长为 650 nm) 经过透镜 L1 与 L2 扩束准直后, 照亮 SLM (DHC: GCI-770202), 再由透镜 L3 将被调制激光斑汇聚于 CCD (IMAVISION: MER-132-43GC-P).

SLM 加载的随机散斑、置换矩阵和待加密图像均由计算机 (CPU: Intel Core i7-11700K, RAM: 128 GB) 生成. 图像重构和图像解密也在计算机中实现. CCD 起到桶探测器的作用, 收集激光并转化为桶测量信号. 两偏振片 P 用以调整激光强度, 透镜 L1 焦距为 $f_1 = 1$ cm, L2 焦距为 $f_2 = 10$ cm. 实验所用图像像素 $64 \times 128$, 由“烟台大学”四个字构成, 如图 1(b) 所示. 随机矩阵 $\boldsymbol{L} = \boldsymbol{N}_1$: $64 \times 64$ 和 $\boldsymbol{R} = \boldsymbol{N}_2$: 128×128 由二值数字 (0 和 1) 生成, 它们均满足概率为 0.2 的伯努利分布. 随机矩阵 ($\boldsymbol{L}$ 和 $\boldsymbol{R}$) 和置换矩阵 ($\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$) 也在图 1(b) 中给出.

图 2(a1)、图 2(b1)、图 2(c1) 和图 2(d1) 是根据 (4) 式和 (5) 式中的 4 种图像置换加密方法对图像加密的实验结果, 其他第二、三、四行是解密图像.

以 (4) 式中第一种加密方式为例, 置换加密后的测量矩阵为 $\boldsymbol{A} = (\boldsymbol{P}_1\boldsymbol{L}) \otimes \boldsymbol{R}$. 随机散斑由 $\boldsymbol{A}$ 的行向量 $\boldsymbol{A}_m$ ($m = 1, 2, \cdots, 64 \times 128$) 变形得到. 加载至 SLM 的图案是随机散斑与物体 $\boldsymbol{X}$ 的 Hadamard 积. 空间光调制器由 $1024 \times 768$ 个单元组成, 为了减少将散斑图案加载到 SLM 上时图像的失真, 我们使用 $4 \times 4$ 的单元来表示一个像素. 每个图案的大小为 $64 \times 128$, 包含 $256 \times 512$ 个单元. SLM 播放 $64 \times 128$ 张散斑图案, CCD 依次采集桶测量

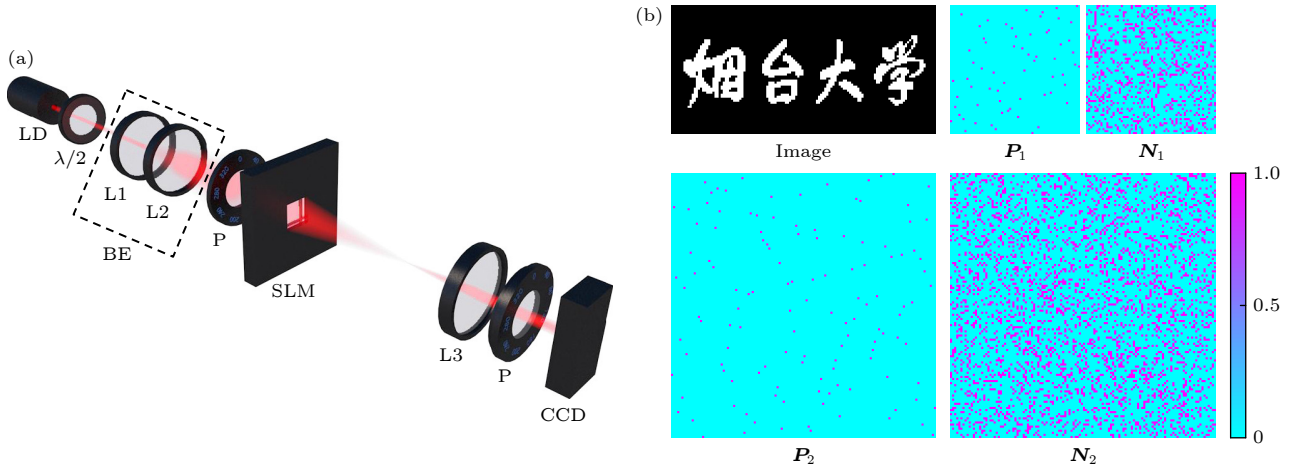


图 1 (a) 实验装置图 (LD, 激光二极管; $\lambda/2$, 半波片; BE, 扩束器; P, 偏振片; L1, L2, L3, 透镜; SLM, 空间光调制器; CCD, 电荷耦合器件); (b) 物体图像 ($\boldsymbol{X}$: $64 \times 128$)、两个随机矩阵 ($\boldsymbol{L} = \boldsymbol{N}_1$: $64 \times 64$ 和 $\boldsymbol{R} = \boldsymbol{N}_2$: $128 \times 128$)、两个置换矩阵 ($\boldsymbol{P}_1$: $64 \times 64$, $\boldsymbol{P}_2$: $128 \times 128$)

Fig. 1. (a) Experimental setup (LD, laser diode; $\lambda/2$, half waveplate; BE, beam expander; P, polarizer; L1, L2, L3, lenses; SLM, spatial light modulator; CCD, charge coupled device); (b) image ($\boldsymbol{X}$: $64 \times 128$), two random matrices ($\boldsymbol{L} = \boldsymbol{N}_1$: $64 \times 64$ and $\boldsymbol{R} = \boldsymbol{N}_2$: $128 \times 128$), and two permutation matrices ($\boldsymbol{P}_1$: $64 \times 64$, $\boldsymbol{P}_2$: $128 \times 128$).

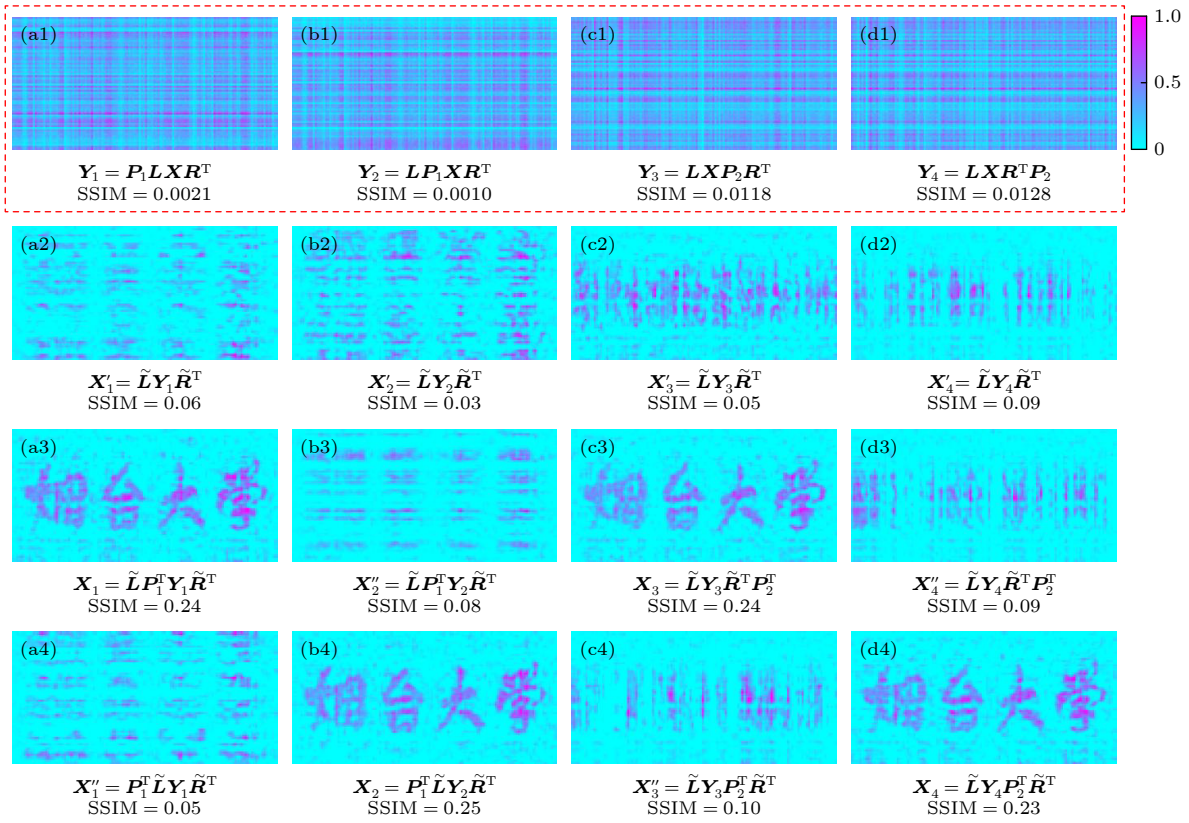


图 2 使用一个置换矩阵时的加密解密图像 (a1)—(d1) 加密图像; (a2)—(d4) 解密图像. 使用的加密或解密公式标在图片下方

Fig. 2. Encrypted and decrypted images with one permutation matrix: (a1)–(d1) Encrypted images; (a2)–(d4) decrypted images. The encryped or decrypted equations are marked below the pictures.

信号 $\boldsymbol{Y}_1$. 此时物体 $\boldsymbol{X}$ 被加密成 $\boldsymbol{Y}_1$. 图 2(a1) 中加密图像的结构相似度 (structural similarity, SSIM)[28] 为 0.0021. 极小的相似度表明了图像加密的可靠性.

解密图像图 2(a2)—(d4) 都是使用截断奇异值方法重构获得的, 截断比均为 $r_1/M = r_2/N = 0.9$, 然后使用 Chen 等 [27] 文中的二次滤波算法对重建图像进行滤波. 该算法通过定义一个点扩散函数对图像进行卷积 (imfilter) 与盲目反卷积 (deconvblind). 我们使用了滤波半径为 1 像素的圆形滤波器, 即

$$h = \begin{pmatrix} 0.0251 & 0.1453 & 0.0251 \\ 0.1453 & 0.3183 & 0.1453 \\ 0.0251 & 0.1453 & 0.0251 \end{pmatrix}.$$

其中, 图 2(a3) 是正确解密获得的图像, 是根据 (11) 式的第一个公式解密的. 如果解密矩阵序列与 (11) 式第一个式子的矩阵序列不一样, 解密后则得到错误的图像. 图 2(a2) 和图 2(a4) 给出了分别由 $\boldsymbol{X}_1' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_1\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 和 $\boldsymbol{X}_1'' = \boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_1\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 所解密的图像. 图 2(a3) 中图像的结构相似度 SSIM = 0.24, 远大于图 2(a2) 和图 2(a4) 中的图像. 因此, 只有在矩阵和序列信息完全已知的情况下, 才能成功解密出正确图像.

图 2(b1) 显示了用 (4) 式中第二个公式加密后的图像 $\boldsymbol{Y}_2$. 图 2(b2)—(b4) 中的解密图像分别用 $\boldsymbol{X}_2' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_2\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_2'' = \tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_2\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_2 = \boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_2\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 得到. 可以看到, 图 2(b2) 和图 2(b3) 中解密错误的图像具有非常低的 SSIM. 图 2(b4) 中的图像是正确解密的, 因为在图像解密中, 随机矩阵、置换矩阵及其序列是正确的.

同样, 图 2(c1) 和图 2(d1) 为根据 (5) 式中的两个公式加密后的图像 $\boldsymbol{Y}_3$ 和 $\boldsymbol{Y}_4$. 图 2(c2)—(c4) 中的解密图像分别用 $\boldsymbol{X}_3' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_3\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_3 = \tilde{\boldsymbol{L}}\boldsymbol{Y}_3\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}}$, $\boldsymbol{X}_3'' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_3\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 重建. 图 2(d2)—(d4) 中的解密图像分别用 $\boldsymbol{X}_4' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_4\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_4'' = \tilde{\boldsymbol{L}}\boldsymbol{Y}_4\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}}$, $\boldsymbol{X}_4 = \tilde{\boldsymbol{L}}\boldsymbol{Y}_4\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 重建. 图 2(c3) 和图 2(d4) 解密后的图像 SSIM 值 (0.24 和 0.23) 远大于其他图像, 再次表明图像解密是正确的.

同时使用两个置换矩阵 $\boldsymbol{P}_1$ 和 $\boldsymbol{P}_2$ 的实验结果如图 3 所示. 图 3(a1)、图 3(b1)、图 3(c1)、图 3(d1) 中的加密图像分别由 (6) 式中的第一 ($\boldsymbol{Y}_5$)、第二 ($\boldsymbol{Y}_6$)、第三 ($\boldsymbol{Y}_7$)、第四 ($\boldsymbol{Y}_8$) 个公式定义. 可以发

现所有的加密图像的 SSIM 值都很小. 考虑所有随机矩阵和置换矩阵都已知, 但矩阵序列不清楚的情况. 解密时需要考虑所有可能的解密方式来解密图像. 图 3(a2)—(a6) 是关于加密图像图 3(a1) 的解密图像, 它们分别由 $\boldsymbol{X}_5^{(1)}=\tilde{\boldsymbol{L}}\boldsymbol{Y}_5\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_5^{(2)}=\tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_5\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}}$, $\boldsymbol{X}_5^{(3)}=\tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_5\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$, $\boldsymbol{X}_5^{(4)}=\boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_5\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}}$, $\boldsymbol{X}_5^{(5)}=\boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_5\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 得到. 每幅图像的 SSIM 值标在图像下面. 只有矩阵序列正确时, 如图 3(a3) 所示, 才能成功解密图像. 图 3(a3) 的 SSIM 值 (0.25) 比图 3(a2)—(a6) 更高.

同样, 从图 3(b1) 的加密图像中可能解密的图像如图 3(b2)、图 3(b3)、图 3(b4)、图 3(b5) 和图 3(b6) 所示. 使用 $\boldsymbol{X}_6^{(3)}=\tilde{\boldsymbol{L}}\boldsymbol{P}_1^{\mathrm{T}}\boldsymbol{Y}_6\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 得到的成功的解密图像如图 3(b4) 所示. 对于图 3(c1) 和图 3(d1) 中的加密图像 $\boldsymbol{Y}_7$ 和 $\boldsymbol{Y}_8$, 分别使用 $\boldsymbol{X}_7^{(4)}=\boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_7\tilde{\boldsymbol{R}}^{\mathrm{T}}\boldsymbol{P}_2^{\mathrm{T}}$ 和 $\boldsymbol{X}_8^{(5)}=\boldsymbol{P}_1^{\mathrm{T}}\tilde{\boldsymbol{L}}\boldsymbol{Y}_8\boldsymbol{P}_2^{\mathrm{T}}\tilde{\boldsymbol{R}}^{\mathrm{T}}$ 才能得到成功的解密图像. 所有成功解密图像的 SSIM 值远远大于其他错误解密图像.

从图 2 和图 3 的实验结果可以看出, 置换矩阵及其在矩阵序列中的位置在图像解密中都很重

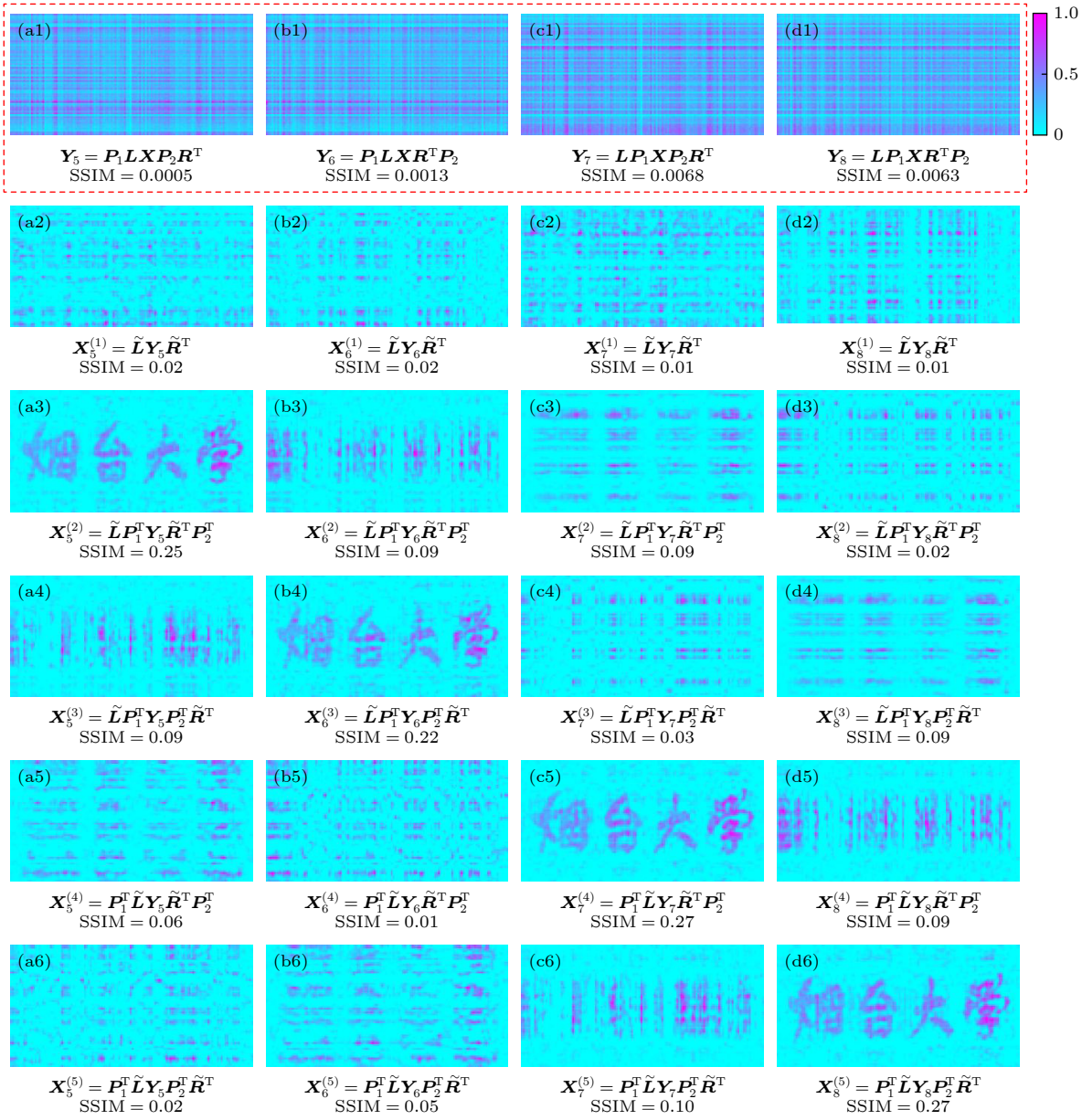


图 3 使用两个置换矩阵时的加密解密图像 (a1)—(d1) 加密图像; (a2)—(d6) 解密图像. 使用的加密或解密公式标在图片下方

Fig. 3. Encrypted and decrypted images with two permutation matrices: (a1)–(d1) Encrypted images; (a2)–(d6) decrypted images. The encryped or decrypted equations are marked below the pictures.

要. 该方案为 CGI 中的图像加密提供了灵活多变的方法.

解密图像的质量可用峰值信噪比 (peak signal-to-noise ratio, PSNR) 和相关系数 (correlation coefficient, CC) 来进一步评估:

$$\mathrm{PSNR} = 10\lg\frac{X_{\boldsymbol{k},\max}^2}{\Delta \boldsymbol{X}_k^2}, \tag{12}$$

$$\mathrm{CC} = \frac{\mathrm{Cov}(\boldsymbol{X}_k, \boldsymbol{X})}{\sqrt{\Delta \boldsymbol{X}_{\boldsymbol{k}}^2 \Delta \boldsymbol{X}^2}}, \tag{13}$$

其中, $X_{k,\max}$ 是解密图像 $\boldsymbol{X}_k$ 中的最大值, $\Delta \boldsymbol{X}^2 = \overline{\boldsymbol{X}^2 - \bar{\boldsymbol{X}}^2}$ 是解密图像的均方误差, $\bar{\boldsymbol{X}}$ 是图像的均值, 协方差为

$$\mathrm{Cov}(\boldsymbol{X}_k, \boldsymbol{X}) = \overline{(\boldsymbol{X}_k - \bar{\boldsymbol{X}}_k)(\boldsymbol{X} - \bar{\boldsymbol{X}})}.$$

图 2 和图 3 解密图像的 PSNR 分别绘制在图 4(a) 和图 4(b) 中. 由图 4(a) 和图 4(b) 可以发现, 在每一组中, 成功解密的图像的 PSNR 都远大于错误解密的图像. 例如, 图 2(a2)—(a4) 的 PSNR 分别为 8.48 dB, 12.14 dB 和 8.31 dB. 解密图像的 CC 绘制在图 4(c) 和图 4(d) 中. 由图 4(d) 可以看出, 对于成功解密的图像, CC 值分别为 0.8427, 0.8127, 0.8470, 0.8468. 很明显, 它们和其他的截然不同. 可以认为, 一旦图像被成功解密, 图像的 PSNR, SSIM 和 CC 可以保持在一个较好的水平.

实验中多个随机矩阵和置换矩阵的应用, 表明了本文提出的图像加密方案具有较好灵活性. 这种加密方式在其他图像处理如水印 [29]、图像隐藏 [30] 等方面也有一定的应用前景. 除此之外, 本方案与其他加密方式, 如 Arnold 置乱 [31]、RSA 加密 [32] 等相结合, 将会形成保密性更高, 加密方式更加巧妙的加密方法, 这也是我们未来工作的研究内容.

## 4 结 论

本文研究了一种基于 CGI 的灵活的二维图像加密方案, 该方案使用两个随机矩阵和两个置换矩阵. 这些矩阵的 Kronecker 积作为测量矩阵. 在实验中, 将投影的散斑和图像加载到 SLM 上. 采用 8 种方式对图像进行加密, 显示了图像加密的灵活性. 在每种加密方式中, 加密后的图像与原始图像的结构相似度都很小. 在图像解密过程中, 矩阵序列是非常重要的. 只有当随机矩阵、置换矩阵及其序列信息完全已知时, 图像才能成功解密. 为了对解密后的图像进行去噪处理, 采用截断奇异值分解

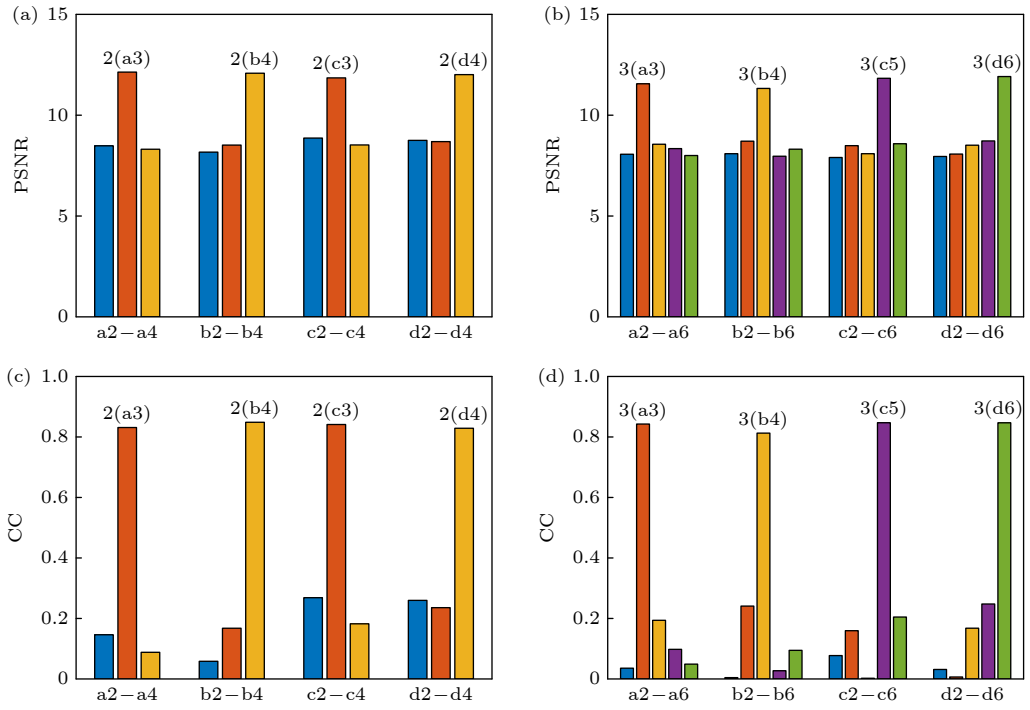


图 4 解密图像的 PSNR 和 CC 值 (a) 图 2 中解密图像的 PSNR 值; (b) 图 3 中解密图像的 PSNR 值; (c) 图 2 中解密图像的 CC 值; (d) 图 3 中解密图像的 CC 值

Fig. 4. PSNRs and CCs of the decrypted images: (a) PSNRs of the decrypted images in Fig. 2; (b) PSNRs of the decrypted images in Fig. 3; (c) CCs of the decrypted images in Fig. 2; (d) CCs of the decrypted images in Fig. 3.

方法. SSIM, PSNR, CC 都表明成功解密的图像具有较好的质量. 这一方法为鬼成像的图像加密提供了一种新的思路, 在其他图像处理如水印、图像隐藏、Arnold 置乱、RSA 加密等方面也有潜在的应用前景.

## 参考文献


[1] Shapiro J H 2008 *Phys. Rev. A* **78** 061802
[2] Cao D Z, Xiong J, Zhang S H, Lin L F, Gao L, Wang K 2008 *Appl. Phys. Lett.* **92** 201102
[3] Chan K W C, O'Sullivan M N, Boyd R W 2009 *Opt. Lett.* **34** 3343
[4] Bromberg Y, Katz O, Silberberg Y 2009 *Phys. Rev. A* **79** 053840
[5] Romberg J 2008 *IEEE Signal Process. Mag.* **25** 14
[6] Katz O, Bromberg Y, Silberberg Y 2009 *Appl. Phys. Lett.* **95** 131110
[7] Zhang C, Guo S, Cao J, Guan J, Gao F 2014 *Opt. Express* **22** 30063
[8] Gong W 2015 *Photonics Res.* **3** 234
[9] Zhang X, Meng X, Yang X, Wang Y, Yin Y, Li X, Peng X, He W, Dong G, Chen H 2018 *Opt. Express* **26** 12948
[10] Lü X, Guo S, Wang C, Yang C, Zhang H, Song J, Gong W, Gao F 2018 *IEEE Photonics J.* **10** 3900708
[11] Luo B, Yin P, Yin L, Wu G, Guo H 2018 *Opt. Express* **26** 23093
[12] Nie X, Zhao X, Peng T, Scully M O 2022 *Phys. Rev. A* **105** 043525
[13] Lyu M, Wang W, Wang H, Wang H, Li G, Chen N, Situ G 2017 *Sci. Rep.* **7** 17865
[14] Barbastathis G, Ozcan A, Situ G 2019 *Optica* **6** 921
[15] Zhang X, Ren Y, Feng G, Qian Z 2011 *Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing* Dalian, China, October 14–16, 2011 pp222–225
[16] Kong L J, Li Y, Qian S X, Li S M, Tu C, Wang H T 2013 *Phys. Rev. A* **88** 013852
[17] Chen W, Chen X 2013 *Appl. Phys. Lett.* **103** 221106
[18] Zhang Y, Zhao S 2017 *Chin. Phys. B* **26** 054205
[19] Wu J, Xie Z, Liu Z, Liu W, Zhang Y, Liu S 2016 *Opt. Commun.* **359** 38
[20] Shi D, Huang J, Wang Y, Yuan K, Xie C, Liu D, Zhu W 2017 *Sci. Rep.* **7** 13172
[21] Zhu J, Yang X, Meng X, Wang Y, Yin Y, Sun X, Dong G 2018 *Opt. Commun.* **420** 34
[22] Kang Y, Zhang L, Zhang D 2018 *Opt. Lasers Eng.* **111** 58
[23] Liu Y, Zheng P, Liu H C 2022 *Opt. Express* **30** 14073
[24] Liu J F, Dong Y, Wang L, Zhao S M 2023 *Chin. Phys. B* **32** 074202
[25] Zhao Y N, Chen L S, Chen L Y, Kong L, Wang C, Ren C, Zhang S H, Cao D Z 2024 *Opt. Lasers Eng.* **181** 108408
[26] Albert A 1972 *Regression and the Moore-Penrose pseudoinverse* (New York: Academic Press)
[27] Chen L Y, Wang C, Xiao X Y, Ren C, Zhang D J, Li Z, Cao D Z 2022 *Opt. Express* **30** 6248
[28] Zhou W, Bovik A C, Sheikh H R, Simoncelli E P 2004 *IEEE Trans. Image Process.* **13** 600
[29] Qu G, Meng X, Yang X, Wu H, Wang P, He W, Chen H 2021 *Opt. Lasers Eng.* **137** 106376
[30] Wang L, Zhao S, Cheng W, Gong L, Chen H 2016 *Opt. Commun.* **366** 314
[31] Qu G, Meng X, Yin Y, Wu H, Yang X, Peng X, He W 2021 *Opt. Lasers Eng.* **137** 106392
[32] Huang H, Han Z 2024 *Results Phys.* **56** 107282

# Ghost imaging based on two-dimensional permutational encryption*

ZHAO Yining CHEN Linshan KONG Lingxin WANG Chong
REN Cheng XU Baolong† CAO Dezhong‡

(*Department of Physics, Yantai University, Yantai* 264005, *China*)

( Received 3 May 2025; revised manuscript received 30 May 2025 )

**Abstract**

Ghost imaging is closely related to image encryption, since the random speckle patterns are often utilized. In the two-dimensional (2D) case, computational ghost imaging can be realized through $\boldsymbol{LXR}^{\mathrm{T}}=\boldsymbol{Y}$, where $\boldsymbol{X}$ is a 2D object, $\boldsymbol{Y}$ is the bucket detection signals reshaped into a 2D form, and $\boldsymbol{L}$ and $\boldsymbol{R}$ are two random matrices. In this work, a scenario of flexible image encryption in ghost imaging in the 2D case is proposed. The image is encrypted into the bucket detection signals by arbitrarily arranging the two random matrices ($\boldsymbol{L}$ and $\boldsymbol{R}$) and other two permutation matrices ($\boldsymbol{P}_1$ and $\boldsymbol{P}_2$). The permutation matrices are used to disrupt the distribution of the bucket signals. Considering that the specific size of the image may not be square but rectangle, eight ways of image encryption are investigated in this work. Four of them use only one permutation matrix ($\boldsymbol{P}_1$ or $\boldsymbol{P}_2$), and they are $\boldsymbol{P}_1\boldsymbol{LXR}^{\mathrm{T}}=\boldsymbol{Y}_1$, $\boldsymbol{LP}_1\boldsymbol{XR}^{\mathrm{T}}=\boldsymbol{Y}_2$, $\boldsymbol{LXP}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_3$, $\boldsymbol{LXR}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_4$. The other four use two permutation matrices ($\boldsymbol{P}_1$ and $\boldsymbol{P}_2$), and they are $\boldsymbol{P}_1\boldsymbol{LXP}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_5$, $\boldsymbol{P}_1\boldsymbol{LXR}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_6$, $\boldsymbol{LP}_1\boldsymbol{XP}_2\boldsymbol{R}^{\mathrm{T}}=\boldsymbol{Y}_7$, and $\boldsymbol{LP}_1\boldsymbol{XR}^{\mathrm{T}}\boldsymbol{P}_2=\boldsymbol{Y}_8$.

Specifically, in experiment, the measurement matrix is generated by the Kronecker product of the random matrices and permutation matrices. According to the 8 ways of image encryption, the 8 measurement matrices are $\boldsymbol{A}_1=(\boldsymbol{P}_1\boldsymbol{L})\otimes\boldsymbol{R}$, $\boldsymbol{A}_2=(\boldsymbol{LP}_1)\otimes\boldsymbol{R}$, $\boldsymbol{A}_3=\boldsymbol{L}\otimes\left(\boldsymbol{RP}_2^{\mathrm{T}}\right)$, $\boldsymbol{A}_4=\boldsymbol{L}\otimes\left(\boldsymbol{P}_2^{\mathrm{T}}\boldsymbol{R}\right)$, $\boldsymbol{A}_5=(\boldsymbol{P}_1\boldsymbol{L})\otimes\left(\boldsymbol{RP}_2^{\mathrm{T}}\right)$, $\boldsymbol{A}_6=(\boldsymbol{P}_1\boldsymbol{L})\otimes\left(\boldsymbol{P}_2^{\mathrm{T}}\boldsymbol{R}\right)$, $\boldsymbol{A}_7=(\boldsymbol{LP}_1)\otimes\left(\boldsymbol{RP}_2^{\mathrm{T}}\right)$, and $\boldsymbol{A}_8=(\boldsymbol{LP}_1)\otimes\left(\boldsymbol{P}_2^{\mathrm{T}}\boldsymbol{R}\right)$. These measurement matrices are used to form the random speckle patterns which are then projected onto the object. A spatial light modulator (SLM) is employed to load the objects and random speckle patterns. A charge coupled device (CCD) is used to obtain the bucket detection signals.

As truncated singular value decomposition (TSVD) is an effective denoising method, it is used to obtain the pseudoinverse matrices of the random matrices used in the decryption process. Only when the pseudoinverse matrices of the random matrices, as well as the correct sequences of the random and permutation matrices, are known in each way, can the image be successfully decrypted. Otherwise, image decryption will not be successful. The structural similarity (SSIM), peak signal-to-noise ratio (PSNR), and correlation coefficient (CC) are used to evaluate the quality of the decrypted images. The SSIMs of object and the 2D bucket detection signals are very low, indicating the successfully encryption. The PSNRs and CCs of the successfully decrypted images are better than those of unsuccessful images. The successfully decrypted images clearly reconstruct the image of the object, while the unsuccessful images are in a mess.

Our method provides a new idea of image encryption in ghost imaging, and image encryption is therefore enhanced and made flexible. Moreover, the present protocol can be combined with other image encryption techniques to form a more flexible protocol, which also has some application prospects in other image processing such as watermarking and image hiding.

**Keywords:** ghost imaging, permutation encryption, Kronecker product

**PACS:** 42.15.Eq, 42.30.–d, 42.30.Va **DOI:** 10.7498/aps.74.20250592

**CSTR:** 32037.14.aps.74.20250592

* Project supported by the National Natural Science Foundation of China (Grant Nos. 62105278, 11674273).

† Corresponding author. E-mail: baolongxu@ytu.edu.cn

‡ Corresponding author. E-mail: dzcao@ytu.edu.cn

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

# 基于二维置换加密鬼成像研究

赵一宁 陈琳珊 孔令鑫 王翀 任承 徐宝龙 曹德忠

# Ghost imaging based on two-dimensional permutational encryption

ZHAO Yining CHEN Linshan KONG Lingxin WANG Chong REN Cheng XU Baolong CAO Dezhong

引用信息 Citation: Acta Physica Sinica, 74, 164201 (2025) DOI: 10.7498/aps.74.20250592
CSTR: 32037.14.aps.74.20250592
在线阅读 View online: https://doi.org/10.7498/aps.74.20250592
当期内容 View table of contents: http://wulixb.iphy.ac.cn

---