基于二维压缩感知的有意义图像加密算法研究

任花[1]，牛少彰[1]，任如勇[1]，岳桢[2]
（1. 北京邮电大学计算机学院，北京 100876；2. 河南师范大学现代教育技术中心，河南 新乡 453007）

摘 要：针对基于压缩感知的有意义图像加密算法存在加密图像视觉安全性不高及重构图像质量不佳的问题，提出了一种基于二维压缩感知的有意义图像加密算法。首先，设计了一种与明文相关联的混沌伪随机序列生成方法，利用全局随机置乱和灰度变换操作进行预加密，改进了重构图像质量。生成的预加密图像作为二维压缩感知的输入，在压缩加密和量化操作后，生成秘密图像。其次，考虑了待嵌入数据和待修改数据之间的关系，利用自适应嵌入方法修改载体系数值，提高了有意义加密图像的视觉安全性。最后，采用二维投影梯度重构方法联合执行解压缩和解密操作，获取重构图像。实验结果表明，与现有算法相比，所提算法不仅提高了加密图像视觉安全性和重构图像质量，而且能抵抗噪声和裁剪攻击。

关键词：图像加密；二维压缩感知；有意义图像加密；嵌入技术
中图分类号：TP309.7
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022101

Research on meaningful image encryption algorithm based on 2-dimensional compressive sensing

REN Hua[1], NIU Shaozhang[1], REN Ruyong[1], YUE Zhen[2]
1. School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Modern Educational Technology Center, Henan Normal University, Xinxiang 453007, China

Abstract: Aiming at the problems that the existing compressive sensing-based meaningful image encryption algorithms have low visual security of the encrypted images and poor quality of the reconstructed images, a 2-dimensional compressive sensing-based (2DCS) meaningful image encryption algorithm was proposed. Firstly, a chaotic pseudo-random sequence generation method associated with plaintext was designed, and the global random permutation and grayscale transformation operations were used for pre-encryption to improve the decrypted image quality. The generated pre-encrypted image was used as the input for 2DCS, and the secret image was generated after the compression encryption and quantization operations. Secondly, the relationship between the hidden and the modified data was considered, and an adaptive embedding method was adopted to modify the carrier coefficient values to improve the visual security of meaningful encrypted image. Finally, the 2-dimensional projection gradient reconstruction method was adopted to decompress and decrypt to obtain the decrypted image. The experimental results show that, compared with the existing algorithms, the proposed algorithm not only improves the visual security of encrypted image and the quality of reconstructed image, but also can resist noise and cropping attacks.

Keywords: image encryption, 2-dimensional compressive sensing, meaningful image encryption, embedding technology

0 引言

随着网络技术的快速发展，海量图像信息正在通过网络快速产生和共享，与此同时，未经授权的访问和滥用问题也随之涌现。作为一种重要的隐私保护技术，加密技术近年来受到了广泛关注[1]。当

收稿日期：2021−10−09；**修回日期：**2022−01−03
基金项目：国家自然科学基金资助项目（No.61370195, No.U1536121）
Foundation Item: The National Natural Science Foundation of China (No.61370195, No.U1536121)

前的图像加密技术通常结合其他技术来提升加密安全性，如混沌理论[1-2]、DNA 编码[3-4]、光变换[5]、细胞自动机[6]等。虽然这些技术可以使密文数据不被直接获取，但是类噪声密文更易暴露被保护内容的重要性，不能确保密文的视觉安全性[7]。因此，如何提高密文的视觉安全性使其在传输时不易被暴露成为当前加密技术亟待解决的问题。

为了解决上述问题，Bao 等[8]在 2015 年首次提出了有意义图像加密概念，通过加密技术和信息隐藏技术将一幅明文图像加密成另一幅有意义的加密图像。具体来说，先通过加密技术将输入明文图像转换成秘密图像，再利用信息隐藏技术将秘密图像嵌入一个较大尺寸的载体图像中。然而，Bao 等算法所生成的加密图像尺寸是明文图像的 4 倍，增加了额外传输负担。幸运的是，压缩感知（CS, compressive sensing）可同步实现信号压缩和加密[9-10]。利用 CS 将明文图像压缩加密成秘密图像，并通过调整采样率控制密文尺寸，有效解决了 Bao 等算法存在的问题。

当前，大量研究已将 CS 技术引入有意义图像加密机制中[11-20]。Chai 等[11]利用 CS 技术将原始明文图像压缩加密成秘密图像，并将秘密图像嵌入离散小波变换（DWT, discrete wavelet transform）后的载体系数中，得到视觉安全的加密图像。由于 DWT 不可逆，对载体图像执行 DWT 会影响秘密信息的正确提取。为了实现无损的信息提取过程，Wang 等[12]和 Chai 等[13]利用整数小波变换（IWT, integer wavelet transform）对载体图像进行无损变换处理，利用最低有效位（LSB, least significant bit）嵌入方法实现了小波系数的可逆修改。此外，为了降低 CS 测量矩阵所占用的空间，Wen 等[14]将半张量积（STP, semi-tensor product）测量矩阵构造方法应用到有意义的加密机制中。为了提高嵌入稳健性，Zhu 等[15]和 Ye 等[16]利用奇异值分解（SVD, singular value decomposition）嵌入方法获得视觉安全的加密图像。为了解决 LSB 嵌入不灵活及 SVD 嵌入强度不高的问题，Wang 等[17]利用贝塞尔曲线嵌入方法实现有意义图像加密。然而，采用一维 CS 压缩感知（1DCS, 1-dimensional compressive sensing）[11-17]处理二维数字图像信号可能导致过高的存储计算负担[18]。基于此，Chai 等[19]和 Huo 等[20]利用二维压缩感知（2DCS, 2-dimensional compressive sensing）技术对明文图像进行压缩加密处理，通过修改载体图像的小波系数矩阵来嵌入秘密图像信息，有效提高了压缩性能和重构图像质量。

上述基于 CS 的有意义图像加密机制[12,14-16,19-20]可归为两类。第一类机制[12,14-16,19]如图 1 所示，发送端依赖持有密钥对明文图像依次执行 CS 压缩−加密−嵌入操作，接收端使用相同密钥逆向执行提取−解密−CS 重构操作来恢复明文图像，此处，将 CS 压缩之前采取的稀疏系数置乱过程视为 CS 稀疏化过程。第二类机制[20]如图 2 所示，发送端依赖持有密钥对明文图像进行加密−CS 压缩−嵌入操作，接收端使用相同密钥提取嵌入信息后，通过联合 CS 解压缩和解密重构算法来恢复明文图像。在一些实际场景中，压缩之前需要执行图像加密过程。例如，当发送端无充足计算资源同时执行压缩和加密操作时，应首先实现加密确保隐私安全，然后将压缩的计算负担转移给计算资源充裕的第三方处理。文献[20]虽利用加密−压缩−嵌入操作，但由发送端完成整个操作不适用于预设资源受限的情况。此外，文献[20]还存在以下问题：1) 加密过程和明文无关联，使用相同置乱向量和相同扩散向量对不同明文图像加密会导致加密安全性不高；2) 预加密过程采取二维随机置乱（2DRP, 2-dimensional random permutation）会导致重构图像质量不佳；3) 没有考虑待嵌入数据和待修改数据之间的关系，直接利用 LSB 替换策略修改载体系数值在一定程度上降低了加密图像视觉安全性。

基于此，本文提出一种基于 2DCS 的有意义图

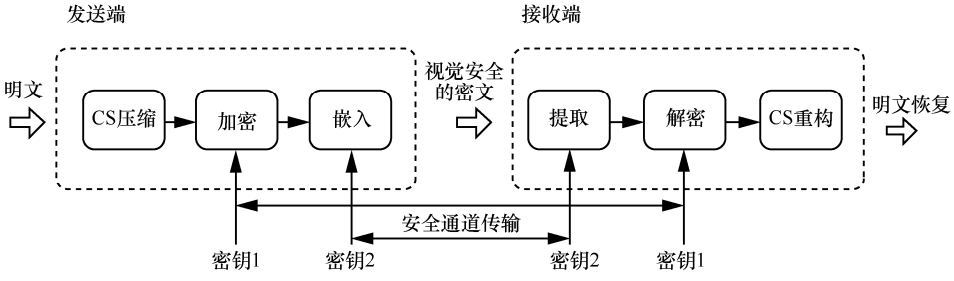


图 1 第一类机制

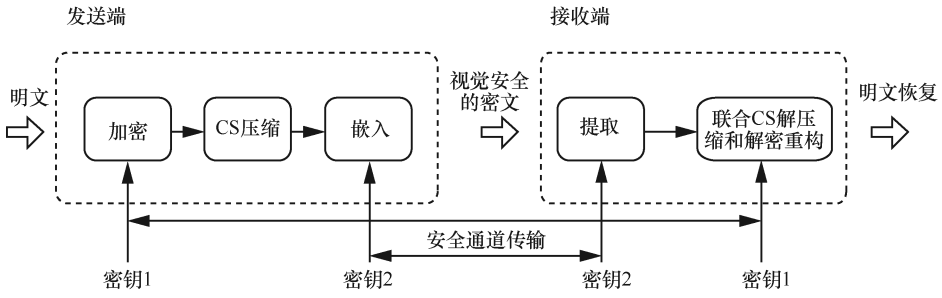


图 2　第二类机制

像加密算法。首先，利用全局随机置乱和灰度变换操作产生预加密图像，以此作为二维压缩感知的输入生成秘密图像，并通过自适应嵌入技术将秘密图像加密成有意义图像。其次，采用二维投影梯度重构方法联合执行解压缩和解密操作，获取重构图像。实验结果验证了所提算法的有效性。

1　基础知识

1.1　压缩感知

假设二维图像和二维稀疏基为 $\boldsymbol{X}\in R^{N\times N}$ 和 $\boldsymbol{\Psi}\in R^{N\times N}$，对 $\boldsymbol{X}$ 进行稀疏化，即

$$\boldsymbol{D}=\boldsymbol{\Psi}\boldsymbol{X}\boldsymbol{\Psi}^{\mathrm{T}} \tag{1}$$

其中，$(\cdot)^{\mathrm{T}}$ 是转置操作，$\boldsymbol{D}\in R^{N\times N}$ 是稀疏基 $\boldsymbol{\Psi}$ 上的系数矩阵。当 $\boldsymbol{D}$ 中的大多数元素为 0 时，$\boldsymbol{X}$ 可视为二维稀疏信号。通常来说，CS 用于一维信号采样。当 CS 采样二维信号时，需将二维信号转换为一维信号后再采样，即

$$\boldsymbol{y}=\boldsymbol{\Phi}\mathrm{vec}(\boldsymbol{X})=\boldsymbol{\Phi}\boldsymbol{x} \tag{2}$$

其中，vec(·) 是一维向量函数，$\boldsymbol{x}$ 是 $1\times N^2$ 的一维向量，$\boldsymbol{\Phi}\in R^{M^2\times N^2}$ 和 $\boldsymbol{y}\in R^{M^2}$ 分别为测量矩阵和测量值向量。将二维图像数据转换为一维向量的采样过程称为 1DCS。根据式(2)可知，1DCS 测量矩阵所占据的存储空间大小为 $M^2\times N^2$，压缩过程的时间复杂度为 $O(M^2N^2)$。

与 1DCS 相比，2DCS 的存储空间和时间复杂度更高效[21]。假设 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是大小为 $M\times N$ 的 2 个不同测量矩阵，利用 2DCS 生成测量值 $\boldsymbol{Y}\in R^{M\times M}$ 的过程如下

$$\boldsymbol{Y}=\boldsymbol{A}\boldsymbol{X}\boldsymbol{B}^{\mathrm{T}} \tag{3}$$

采样率 SR 定义为

$$\mathrm{SR}=\frac{M^2}{N^2} \tag{4}$$

由式(3)可知，2DCS 的时间复杂度为 $O(MN^2)$，只需 $2MN$ 个存储单元即可存储测量矩阵。

1.2　混沌系统

混沌是确定性非线性系统中普遍存在的一种现象，具有类随机行为，对初始条件和控制参数极为敏感[22]。与低阶混沌系统相比，超混沌是一类高阶混沌系统，在保密性、密钥空间及非线性行为方面比低阶混沌系统更具优势。因此，本文利用式(5)定义的超混沌系统生成混沌伪随机数序列[23]，即

$$\begin{cases} y_{i+1}=c_1y_i+c_1z_i \\ z_{i+1}=c_2y_i+c_2z_i+w_i-y_iu_iv_i \\ u_{i+1}=-c_3z_i-c_4u_i-c_5v_i+y_iz_iv_i \\ v_{i+1}=-c_6v_i+y_iz_iu_i \\ w_{i+1}=-c_7y_i-c_7z_i \end{cases} \tag{5}$$

当五阶超混沌系统的控制参数设置为 $[c_1,c_2,c_3,c_4,c_5,c_6,c_7]=[30,10,15.7,5,2.5,4.45,38.5]$ 时，式(5)处于混沌状态。

2　本文算法

本文提出的基于 2DCS 的有意义图像加密算法框架如图 3 所示。发送端借助外部密钥和明文图像的哈希值计算五阶超混沌系统的初始值，根据初始值生成伪随机序列，实现图像预加密过程；云服务器端对预加密图像执行 2DCS 操作得到秘密图像，利用平滑函数[24]自适应地将秘密图像嵌入载体图像中，生成有意义加密图像；接收端提取嵌入信息后，通过二维投影梯度（2DPG, 2-dimensional projected gradient）重构方法[21,25]同时进行解压缩和解密操作获取重构图像。2DPG 的每次迭代包括 3 个过程：空域采用梯度下降法降低图像全变差（TV, total variation）[26]过程；小波变换域利用双变量收缩增强图像稀疏性过程；将迭代解投影到二维解空间过程。接下来将逐一讨论所提框架内容。

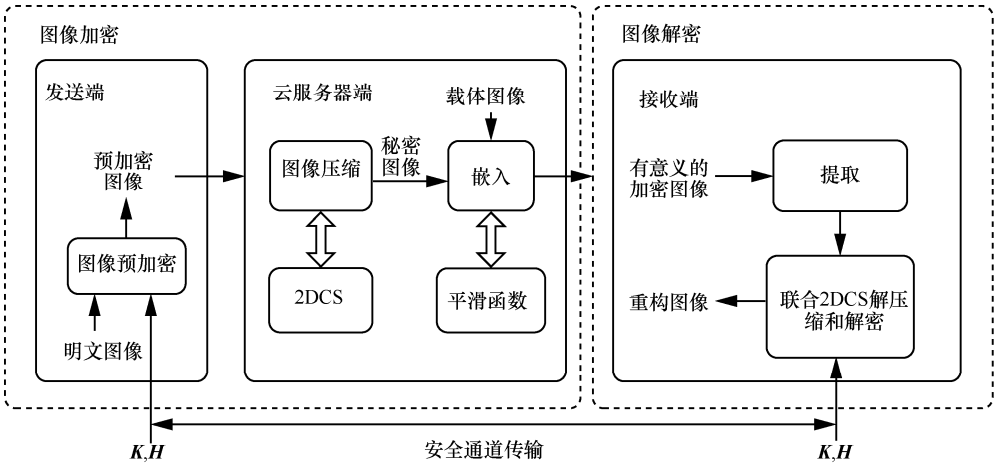


图 3 算法框架

2.1 图像加密

2.1.1 混沌伪随机序列生成

哈希函数因其不可逆性在图像加密系统中扮演着重要角色。MD5 和 SHA-256 是 2 种常用的哈希函数，分别生成 128 位和 256 位哈希值。为了提高加密安全性，本节的混沌伪随机序列由 MD5 和 SHA256 哈希函数控制生成。

首先，将 256 位的外部密钥 $\boldsymbol{K}$ 分成 32 块，即

$$\boldsymbol{K}=\{k_1,k_2,\cdots,k_{32}\} \tag{6}$$

在式(6)的基础上，通过 MD5 和 SHA256 哈希函数，计算明文图像 $\boldsymbol{P}_0$ 和外部密钥 $\boldsymbol{K}$ 的 256 位哈希值 $\boldsymbol{H}$ 为

$$\boldsymbol{H}=\mathrm{SHA256}\big(\mathrm{MD5}(\boldsymbol{S}_1),\mathrm{MD5}(\boldsymbol{S}_2),\mathrm{MD5}(\boldsymbol{S}_3),\mathrm{MD5}(\boldsymbol{K})\big) \tag{7}$$

其中，$\boldsymbol{S}_1$、$\boldsymbol{S}_2$ 和 $\boldsymbol{S}_3$ 分别计算 $\boldsymbol{P}_0$ 的每一行像素和、每一列像素和以及对角像素和。

其次，将哈希值 $\boldsymbol{H}$ 划分成 32 块 $\boldsymbol{H}=\{h_1,h_2,\cdots,h_{32}\}$，利用 $\boldsymbol{K}$ 和 $\boldsymbol{H}$ 生成更新密钥 $\boldsymbol{K}'=\{k'_1,k'_2,\cdots,k'_{32}\}$ 和 k_{xor}，即

$$k'_i=h_i\oplus k_i,\quad 1\leqslant i\leqslant 32 \tag{8}$$

$$k_{\mathrm{xor}}=k'_1\oplus k'_2\oplus\cdots\oplus k'_{32} \tag{9}$$

最后，根据 $\boldsymbol{K}'$ 和 k_{xor} 生成五阶混沌系统的初始值和伪随机序列，具体步骤如下。

1) 根据式(5)的默认方式设置五阶混沌系统的控制参数，利用 k_{xor} 和 $\boldsymbol{K}'$ 计算五阶混沌系统的初始值 y_0、z_0、u_0、v_0 和 w_0 为

$$\begin{cases}y_0=\dfrac{k'_1\oplus k'_2\oplus k'_3\oplus k'_4\oplus k'_5\oplus k'_6\oplus k_{\mathrm{xor}}}{256}\\ z_0=\dfrac{k'_7\oplus k'_8\oplus k'_9\oplus k'_{10}\oplus k'_{11}\oplus k'_{12}\oplus k_{\mathrm{xor}}}{256}\\ u_0=\dfrac{k'_{13}\oplus k'_{14}\oplus k'_{15}\oplus k'_{16}\oplus k'_{17}\oplus k'_{18}\oplus k_{\mathrm{xor}}}{256}\\ v_0=\dfrac{k'_{19}\oplus k'_{20}\oplus k'_{21}\oplus k'_{22}\oplus k'_{23}\oplus k'_{24}\oplus k_{\mathrm{xor}}}{256}\\ w_0=\dfrac{k'_{25}\oplus k'_{26}\oplus k'_{27}\oplus k'_{28}\oplus k'_{29}\oplus k'_{30}\oplus k_{\mathrm{xor}}}{256}\end{cases} \tag{10}$$

2) 为了消除混沌暂态效应，根据式(10)的初始值，循环迭代五阶混沌系统 $k'_{31}+k'_{32}+k_{\mathrm{xor}}$ 次，最后一次的迭代结果充当更新的初始值。

3) 使用更新的初始值再次迭代该系统 $1\times\dfrac{N^2}{8}$ 次，获取长度为 $1\times\dfrac{N^2}{8}$ 的序列 $\boldsymbol{Y}$、$\boldsymbol{Z}$、$\boldsymbol{U}$、$\boldsymbol{V}$ 和 $\boldsymbol{W}$。

4) 通过式(11)，生成 2 个长度均为 $1\times N^2$ 的混沌伪随机序列 $\boldsymbol{E}_P$ 和 $\boldsymbol{E}_D$，即

$$\begin{cases}\boldsymbol{E}_P=[\boldsymbol{Y},\boldsymbol{Z},\boldsymbol{Y}-\boldsymbol{Z},\boldsymbol{U},\boldsymbol{V},\boldsymbol{U}-\boldsymbol{V},\boldsymbol{W},\boldsymbol{W}-\boldsymbol{Y}]\\ \boldsymbol{E}_D=[\boldsymbol{V},\boldsymbol{Z},\boldsymbol{V}+\boldsymbol{Z},\boldsymbol{U},\boldsymbol{Y},\boldsymbol{U}+\boldsymbol{Y},\boldsymbol{W},\boldsymbol{W}+\boldsymbol{Y}]\end{cases} \tag{11}$$

2.1.2 图像预加密

生成一维置乱序列 $\boldsymbol{E}_P$ 和扩散序列 $\boldsymbol{E}_D$ 后，发送端对明文图像执行全局随机置乱（GRP, global random permutation）操作和灰度变换操作，生成预加密图像。

首先，发送端将 $N\times N$ 的明文图像 $\boldsymbol{P}_0$ 转换为 $1\times N^2$ 的一维向量 $\mathrm{vec}(\boldsymbol{P}_0)$；同时，利用内置排序函数排序一维置乱序列 $\boldsymbol{E}_P$，得到 $1\times N^2$ 的位置向量 **POS**。根据位置向量 **POS**，对 $\mathrm{vec}(\boldsymbol{P}_0)$ 执行全局随

机置乱操作，即

$$\boldsymbol{P}_1 = \mathrm{GRP}\left(\mathbf{POS}, \mathrm{vec}(\boldsymbol{P}_0)\right) \tag{12}$$

其中，$\boldsymbol{P}_1$ 是置乱后的一维向量，GRP(·) 是全局随机置乱函数。

随后，将置乱向量 $\boldsymbol{P}_1$ 转换为二维矩阵，通过式(13)的灰度变换操作对 $\boldsymbol{P}_1$ 完成扩散操作，即

$$\boldsymbol{P}_2(i,j) = \begin{cases} 255 - \boldsymbol{P}_1(i,j), & \boldsymbol{B}(i,j) = 1 \\ \boldsymbol{P}_1(i,j), & \boldsymbol{B}(i,j) = 0 \end{cases} \tag{13}$$

其中，矩阵 $\boldsymbol{P}_2$ 是预加密结果；二值矩阵 $\boldsymbol{B}$ 由扩散矩阵 $\boldsymbol{E}_D$ 计算，且 $\boldsymbol{B} = \mathrm{mod}(\boldsymbol{E}_D \times 10^{14}, 2)$，$\boldsymbol{E}_D$ 是已转换为二维矩阵的伪随机序列值。

2.1.3 压缩嵌入

云服务器端通过 2DCS 操作将预加密图像 $\boldsymbol{P}_2$ 压缩加密成测量值 $\boldsymbol{P}_3$，将测量值 $\boldsymbol{P}_3$ 量化到整数值[0,255]，生成秘密图像 $\boldsymbol{P}_4$，再通过平滑函数嵌入方法将秘密图像自适应地嵌入载体系数矩阵中。具体步骤如下。

1) 构造 $M \times N$ ($M < N$)的高斯随机测量矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$，并利用 2DCS 将 $\boldsymbol{P}_2$ 压缩加密成测量值 $\boldsymbol{P}_3$，即

$$\boldsymbol{P}_3 = \boldsymbol{A}\boldsymbol{P}_2\boldsymbol{B}^{\mathrm{T}} \tag{14}$$

2) 利用非线性函数 Sigmoid 将 $\boldsymbol{P}_3$ 量化到[0,255]，得到秘密图像 $\boldsymbol{P}_4$ 为

$$\boldsymbol{P}_4 = \mathrm{round}\left(a_1\left(1 + \mathrm{e}^{-a_2(\boldsymbol{P}_3 - a_3)}\right)\right) \tag{15}$$

其中，round(·) 为四舍五入函数，$a_1 = 255$，$a_2 = \max - \min$，$a_3 = \dfrac{\max + \min}{2}$，max 和 min 是测量值 $\boldsymbol{P}_3$ 中的最大值和最小值。

3) 将秘密图像 $\boldsymbol{P}_4$ 排列成一维向量 $\boldsymbol{P}_r = \{p_i\}_{i=1}^{\frac{N^2}{4}}$。

4) 对 $N \times N$ 的载体图像执行提升整数小波变换（LIWT, lifting integer wavelet transform），生成低频子带系数矩阵 **LL**、中频子带系数矩阵 **LH** 和 **HL**、高频子带系数矩阵 **HH**。将 **LH**、**HL** 和 **HH** 这 3 个子带重新排列成一维向量 $\mathbf{lh}=\{\mathrm{lh}_i\}_{i=1}^{i=\frac{N^2}{4}}$、$\mathbf{hl}=\{\mathrm{hl}_i\}_{i=1}^{i=\frac{N^2}{4}}$ 和 $\mathbf{hh}=\{\mathrm{hh}_i\}_{i=1}^{i=\frac{N^2}{4}}$。

5) 将一维待嵌入向量 $\boldsymbol{P}_r$ 及系数向量 **lh** 和 **hl** 的每个元素分割成 8 位。利用平滑函数将 $p_{i8}p_{i7}p_{i6}$ 嵌入 $\mathrm{lh}_{i3}\mathrm{lh}_{i2}\mathrm{lh}_{i1}$ 中，将 $p_{i5}p_{i4}p_{i3}$ 嵌入 $\mathrm{hl}_{i3}\mathrm{hl}_{i2}\mathrm{hl}_{i1}$ 中，记为 $\mathrm{lh}_{i3}\mathrm{lh}_{i2}\mathrm{lh}_{i1} \leftarrow p_{i8}p_{i7}p_{i6}$ 和 $\mathrm{hl}_{i3}\mathrm{hl}_{i2}\mathrm{hl}_{i1} \leftarrow p_{i5}p_{i4}p_{i3}$；利用 LSB 位替换方式将 $p_{i2}p_{i1}$ 嵌入 $\mathrm{hh}_{i2}\mathrm{hh}_{i1}$ 中，记为 $\mathrm{hh}_{i2}\mathrm{hh}_{i1} = p_{i2}p_{i1}$。将 $p_{i8}p_{i7}p_{i6}$ 自适应地嵌入 $\mathrm{lh}_{i3}\mathrm{lh}_{i2}\mathrm{lh}_{i1}$ 的过程如下

$$v_i = 4p_{i8} + 2p_{i7} + p_{i6} - (\mathrm{lh}_i - \mathrm{mod}(\mathrm{lh}_i, 8)) \tag{16}$$

$$\mathrm{lh}_i' = \begin{cases} \mathrm{lh}_i + v_i & ,|v_i| < 5 \\ \mathrm{lh}_i + v_i + 8 & ,v_i \leqslant -5 \\ \mathrm{lh}_i + v_i - 8 & ,v_i \geqslant 5 \end{cases} \tag{17}$$

其中，$v_i \left(1 \leqslant i \leqslant \dfrac{N^2}{4}\right)$ 是第 i 个待嵌入值和待修改系数值之间的差值，lh_i' 是第 i 个已修改的载体系数值。当所有系数向量按式(16)和式(17)修改后，待嵌入向量 $\boldsymbol{P}_r$ 的高 3 位 $p_{i8}p_{i7}p_{i6}$ 就已经完全嵌入 **LH** 中。

6) 将含嵌入信息的系数向量转换为二维矩阵，利用 LIWT 的逆变换过程将二维矩阵变换到空域，得到有意义加密图像 $\boldsymbol{P}_5$。

2.2 图像解密

解密是加密的逆过程，主要包括秘密图像提取和明文图像重构过程。

2.2.1 秘密图像提取

在秘密图像提取过程，接收端需从加密图像 $\boldsymbol{P}_5$ 中提取秘密图像。首先，对 $\boldsymbol{P}_5$ 执行 LIWT 操作，获取 4 个系数矩阵 **LL**、**LH′**、**HL′** 和 **HH′**。随后，将系数矩阵 **LH′**、**HL′** 和 **HH′** 排列成一维向量 $\{\mathrm{lh}_i'\}_{i=1}^{i=\frac{N^2}{4}}$、$\{\mathrm{hl}_i'\}_{i=1}^{i=\frac{N^2}{4}}$ 和 $\{\mathrm{hh}_i'\}_{i=1}^{i=\frac{N^2}{4}}$，按式(18)来提取嵌入信息。

$$\begin{cases} p_{i1}p_{i2} = \mathrm{hh}_{i1}'\mathrm{hh}_{i2}' \\ p_{i3}p_{i4}p_{i5} = \mathrm{hl}_{i1}'\mathrm{hl}_{i2}'\mathrm{hl}_{i3}' \\ p_{i6}p_{i7}p_{i8} = \mathrm{lh}_{i1}'\mathrm{lh}_{i2}'\mathrm{lh}_{i3}' \end{cases} \tag{18}$$

其中，$p_{i1}p_{i2}$、$p_{i3}p_{i4}p_{i5}$ 和 $p_{i6}p_{i7}p_{i8}$ 表示分别从 hh_i'、hl_i' 和 lh_i' 的第 i 个像素中提取的秘密信息位，且 $1 \leqslant i \leqslant \dfrac{N^2}{4}$。将所提取的信息转换为十进制 $p_i = [p_{i8}, p_{i7}, p_{i6}, p_{i5}, p_{i4}, p_{i3}, p_{i2}, p_{i1}]$，并将 p_i 转换为二维矩阵，获取秘密图像 $\boldsymbol{P}_4$。

2.2.2 明文图像重构

在图像重构阶段，以往有意义图像加密算法通常先根据解密密钥解密所提取的信息，再利用 CS 重构算法获取重构图像内容。与以往算法不同的是，本文采取二维投影梯度 2DPG 重构方法[21,25]同时进行解压缩和解密操作生成重构图像。在图像重构前，通过安全通道将外部密钥 $\boldsymbol{K}$ 和哈希值 $\boldsymbol{H}$ 传

输至接收端。

首先，利用逆 Sigmoid 函数对所提取的秘密图像 $\boldsymbol{P}_4$ 进行逆量化。

$$\boldsymbol{P}_3 = \text{round}\left(\log \frac{\frac{a_1}{\boldsymbol{P}_4} - 1}{-a_2} + a_3 \right) \tag{19}$$

为方便后续理解和描述，将测量值 $\boldsymbol{P}_3$ 赋给矩阵 $\boldsymbol{Y}$。紧接着，需对二维投影梯度迭代过程初始化，而 $\boldsymbol{Y} = \boldsymbol{P}_3 = \boldsymbol{A}\boldsymbol{P}_2\boldsymbol{B}^{\mathrm{T}}$ 的最小 L_2 范式解可视为初始值 $\boldsymbol{X}_0$。

$$\boldsymbol{X}_0 = \boldsymbol{A}^*\boldsymbol{P}(\boldsymbol{B}^*)^{\mathrm{T}} = \boldsymbol{A}^*\boldsymbol{Y}(\boldsymbol{B}^*)^{\mathrm{T}} \tag{20}$$

其中，$\boldsymbol{A}^* = \boldsymbol{A}^{\mathrm{T}}(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}})^{-1}$ 和 $\boldsymbol{B}^* = \boldsymbol{B}^{\mathrm{T}}(\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}})^{-1}$ 分别表示 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 的伪逆矩阵。

然后，分别从梯度下降、双变量收缩和解投影 3 个过程实现图像重构。首先，利用梯度下降法降低空域图像的 TV。

$$\hat{\boldsymbol{X}}_n = \boldsymbol{X}_n - r\frac{\partial \mathrm{TV}(\boldsymbol{X}_n)}{\partial \boldsymbol{X}_n} \tag{21}$$

其中，$r = \mu\alpha\lambda$ 是步长，$\dfrac{\partial \mathrm{TV}(\boldsymbol{X}_n)}{\partial \boldsymbol{X}_n}$ 是导数结果，将 $\dfrac{\partial \mathrm{TV}(\boldsymbol{X}_n)}{\partial \boldsymbol{X}_n}$ 定义为

$$\begin{aligned}\frac{\partial \mathrm{TV}(\boldsymbol{X}_n)}{\partial \boldsymbol{X}_n} = &\\ &\frac{2\boldsymbol{X}_{i,j} - \boldsymbol{X}_{i-1,j} - \boldsymbol{X}_{i,j-1}}{\sqrt{(\boldsymbol{X}_{i,j} - \boldsymbol{X}_{i-1,j})^2 + (\boldsymbol{X}_{i,j} - \boldsymbol{X}_{i,j-1})^2 + \delta}} + \\ &\frac{\boldsymbol{X}_{i,j} - \boldsymbol{X}_{i+1,j}}{\sqrt{(\boldsymbol{X}_{i+1,j} - \boldsymbol{X}_{i,j})^2 + (\boldsymbol{X}_{i+1,j} - \boldsymbol{X}_{i+1,j-1})^2 + \delta}} + \\ &\frac{\boldsymbol{X}_{i,j} - \boldsymbol{X}_{i,j+1}}{\sqrt{(\boldsymbol{X}_{i,j+1} - \boldsymbol{X}_{i,j})^2 + (\boldsymbol{X}_{i,j+1} - \boldsymbol{X}_{i-1,j+1})^2 + \delta}}\end{aligned} \tag{22}$$

其中，参数 δ 用来避免分母为 0，在本文实验中 $\delta = 10^{-7}$。

梯度下降后，可以得到一个比过去迭代解更小的解 $\hat{\boldsymbol{X}}_n$，但 $\hat{\boldsymbol{X}}_n$ 在小波域中不够充分稀疏。为了增强 $\hat{\boldsymbol{X}}_n$ 的稀疏性，将双树离散小波变换（DDWT, dual-tree discrete wavelet transform）视为稀疏基，采用双变量硬阈值收缩方法[27]对 $\hat{\boldsymbol{X}}_n$ 稀疏化，稀疏后的系数矩阵 $\hat{\boldsymbol{D}}_n$ 可表示为

$$\hat{\boldsymbol{D}}_n = \boldsymbol{\Psi}\hat{\boldsymbol{X}}_n\boldsymbol{\Psi}^{\mathrm{T}} \tag{23}$$

接下来，对稀疏系数矩阵 $\hat{\boldsymbol{D}}_n$ 进行双变量收缩，即

$$\tilde{\boldsymbol{D}}_n = \mathrm{Th}(\hat{\boldsymbol{D}}_n, \eta) = \frac{\left(\sqrt{\hat{\boldsymbol{D}}_n^2 + f_p^2} - \eta\dfrac{\sqrt{3\sigma^n}}{\sigma_f} \right)}{\sqrt{\hat{\boldsymbol{D}}_n^2 + f_p^2}} + \hat{\boldsymbol{D}}_n \tag{24}$$

其中，$\mathrm{Th}(\cdot)$ 是阈值函数，$\tilde{\boldsymbol{D}}_n \in R^{N\times N}$ 是双变量收缩后的小波系数矩阵，η 是常量，f_p 是 $\hat{\boldsymbol{D}}_n$ 的双亲系数，$\sigma^n = \dfrac{\mathrm{median}\left(\mathrm{vec}\left(\hat{\boldsymbol{D}}_n\right)\right)}{0.674\,5}$，$\mathrm{median}(\cdot)$ 是中值函数，σ_f 是边界方差。对系数矩阵完成双变量收缩后，执行双树离散小波的逆变换过程，得到系数解 $\tilde{\boldsymbol{X}}_n = \boldsymbol{\Psi}^{\mathrm{T}}\tilde{\boldsymbol{D}}_n\boldsymbol{\Psi}$。

最后，得到稀疏解 $\tilde{\boldsymbol{X}}_n$，但梯度下降和双变量收缩后的解 $\tilde{\boldsymbol{X}}_n$ 偏离了解空间，需将迭代解 $\tilde{\boldsymbol{X}}_n$ 投影至二维解空间中。假设 $\tilde{\tilde{\boldsymbol{X}}}_n$ 是已投影到解空间后的矩阵，$\tilde{\boldsymbol{X}}$ 是待求解变量，投影过程就是解优化函数过程，即求解 $\tilde{\boldsymbol{X}}$，使 $\tilde{\boldsymbol{X}}$ 满足 $\boldsymbol{Y} = \boldsymbol{A}\tilde{\boldsymbol{X}}(\boldsymbol{B})^{\mathrm{T}}$ 且 $\left\|\tilde{\boldsymbol{X}} - \tilde{\boldsymbol{X}}_n\right\|_{\mathrm{F}}^2$ 最小。

$$\begin{aligned}&\tilde{\tilde{\boldsymbol{X}}}_n = \arg\min_{\tilde{\boldsymbol{X}}} \left\|\tilde{\boldsymbol{X}} - \tilde{\boldsymbol{X}}_n\right\|_{\mathrm{F}}^2 \\ &\text{s.t.}\,\boldsymbol{Y} = \boldsymbol{A}\tilde{\boldsymbol{X}}(\boldsymbol{B})^{\mathrm{T}}\end{aligned} \tag{25}$$

而式(25)的优化过程可通过拉普拉斯方法求解，即

$$\tilde{\tilde{\boldsymbol{X}}}_n = \tilde{\boldsymbol{X}}_n - \boldsymbol{A}^*(\boldsymbol{A}\tilde{\boldsymbol{X}}_n\boldsymbol{B}^{\mathrm{T}} - \boldsymbol{Y})(\boldsymbol{B}^*)^{\mathrm{T}} \tag{26}$$

式(26)的 $\tilde{\boldsymbol{X}}_n$ 和 $\boldsymbol{Y}$ 在前文已经求解，$\boldsymbol{A}$ 和 $\boldsymbol{B}$ 是已知测量矩阵，最终可以求解 $\tilde{\tilde{\boldsymbol{X}}}_n$，最终解 $\tilde{\tilde{\boldsymbol{X}}}_n$ 就是重构图像 $\boldsymbol{P}_0$。

3 实验结果及对比

本节给出所提算法的仿真结果，所有实验均在 64 位 Windows7 PC 16.0 GB 和 Inter(R) Core(TM) i7-4770CPU @ 3.40 GHz 上进行，平台为 MATLAB R2012b。在混沌伪随机序列生成阶段，外部密钥为 $\boldsymbol{K}$ = 6b679b3c77826d30a79e612114a8c18df984c176f4e529f684748ad052241b17。在 2DCS 压缩和重构阶段，正交高斯随机矩阵作为测量矩阵，采样率固定为 $\dfrac{1}{4}$，重构过程采取 DDWT 作为稀疏基。利用峰值信噪比（PSNR, peak signal-to-noise ratio）和平均结构相似性（MSSIM, mean structural similarity）

测量加密图像的视觉安全性和重构图像质量。

3.1　实验结果

本节以大小为 256 像素×256 像素的标准测试图像 Parrots、Monarch、Camera、Boats 和 Barbara 作为明文图像，Lena 作为载体图像，对所提算法进行测试。图 4 给出了 Parrots 和 Monarch 的测试结果。由图 4 可知，秘密图像已经压缩加密成了原始明文图像的$\frac{1}{4}$，倘若在不安全通道直接传输，秘密图像的类噪声外观易引起攻击者的注意；如果传输加密图像，可以看出不同明文图像对应的最终加密图像视觉上类似，与载体图像 Lena 无法用肉眼区分，因此可以在不引起攻击者注意下实现加密图像的安全传输。

需要说明的是，在有意义加密图像生成过程中，发送端只需要对二维图像进行预加密，此过程的时间复杂度为$O(MN)$；云服务器端需要先对预加密图像进行 2DCS 处理，随后完成嵌入操作，此过程的复杂度为$O(MN^2)$；接收端采取二维投影梯度重构方法解压缩解密加密图像，此过程的复杂度为$O(MN)$。因此，本文所涉及的加密算法的计算复杂度为$O(MN^2)$。

接下来，分别从直方图分析、相关性分析、信息熵分析、差分攻击及选择明文攻击（CPA, chosen plaintext attack）5 个方面验证所提算法的有效性。

3.1.1　直方图分析

图像直方图用来描述离散灰度值的概率密度分布。利用 Lena 为载体图像，对 5 幅明文图像进行加密，图 5 给出了载体图像和加密图像的直方图结果。不难发现，不同明文图像所对应的加密图像具有相似的直方图分布，且与载体图像 Lena 的直方图分布相似，这说明所提加密算法有效地隐藏了原始明文图像信息，攻击者难以通过加密图像的直方图分布分析明文关联信息。

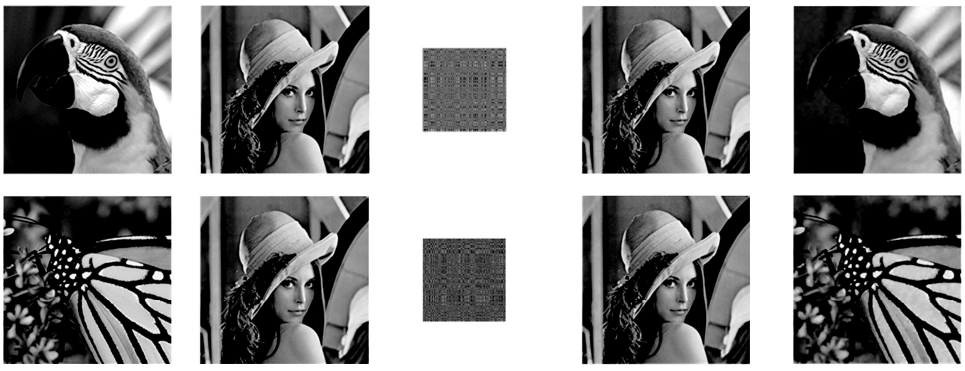
3.1.2　相关性分析

对于视觉有意义的明文图像而言，相邻像素相关系数应接近于 1。本文算法将输入明文图像加密成外观类似于载体图像的加密图像，所生成的加密图像的相邻像素相关系数值理论上应接近于载体图像的相邻像素相关系数值。相邻像素相关系数值的计算式为

$$C_{xy}=\frac{L_s\sum_{i=1}^{L_s}(x_iy_i)-\sum_{i=1}^{L_s}x_i\sum_{i=1}^{L_s}y_i}{\sqrt{\left(L_s\sum_{i=1}^{L_s}x_i^2-\left(\sum_{i=1}^{L_s}x_i\right)^2\right)\left(L_s\sum_{i=1}^{L_s}y_i^2-\left(\sum_{i=1}^{L_s}y_i\right)^2\right)}} \tag{27}$$

其中，x_i和y_i是 2 个相邻像素值，L_s是随机所选的总像素对数。本节随机从水平方向、垂直方向以及对角线方向上选择$L_s=2\ 000$对像素进行测试。

图 6 给出了 Parrots 为明文图像、Lena 为载体图像的测试结果。图 6(a)～图 6(c)为载体图像 Lena 在水平方向、垂直方向以及对角线方向的相关性，图 6(d)～图 6(f)为加密图像在水平方向、垂直方向以及对角线方向的相关性。从图 6 可以看出，加密图像在水平方向、垂直方向及对角线方向上的相关性近似于载体图像，很难用肉眼逐一区分。进一步地，表 1 列出了 5 幅不同明文图像所对应的秘密图像、载体图像和加密图像在 3 个方向上的相关系数值结果。从表 1 中可以看出，加密图像的相关系数值接近于载体图像的相关系数值，这说明所提算法能够很好地将明文图像加密成外观类似载体图像的加密图像。



(a) 明文图像　(b) 载体图像　(c) 秘密图像　(d) 加密图像　(e) 重构图像

图 4　Parrots 和 Monarch 的测试结果

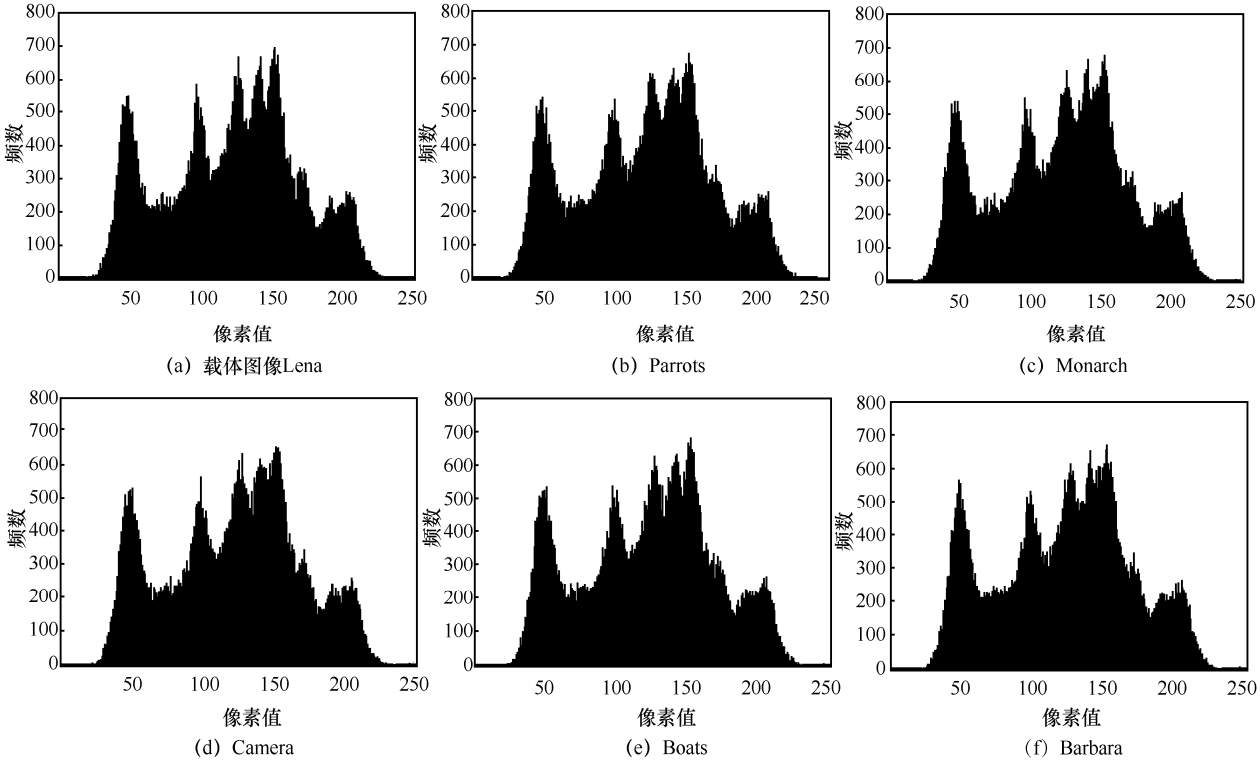


图 5　载体图像和加密图像的直方图结果

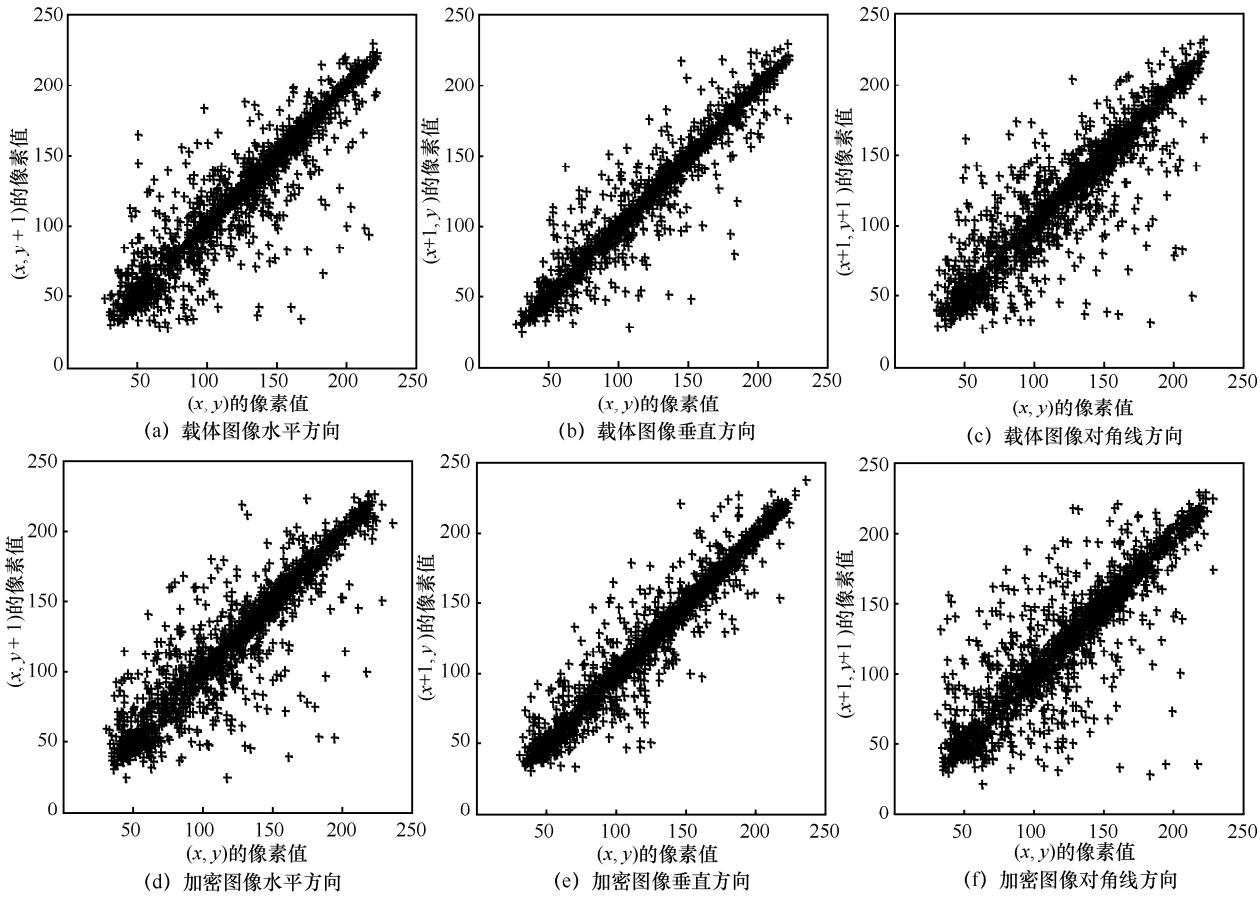


图 6　Parrots 为明文图像、Lena 为载体图像的测试结果

表 1　　相关系数值结果

图像	方向	秘密图像	载体图像	加密图像
Parrots	水平	0.031 4	0.944 0	0.948 0
	垂直	0.011 1	0.971 3	0.971 6
	对角线	0.012 4	0.915 7	0.931 4
Monarch	水平	−0.054 5	0.947 9	0.939 0
	垂直	0.109 0	0.974 8	0.965 5
	对角线	0.016 9	0.928 7	0.911 0
Camera	水平	0.072 9	0.943 3	0.944 1
	垂直	0.061 5	0.971 0	0.972 1
	对角线	−0.013 1	0.917 1	0.923 2
Boats	水平	−0.029 4	0.941 8	0.937 7
	垂直	0.058 6	0.969 9	0.969 3
	对角线	0.022 9	0.920 9	0.920 7
Barbara	水平	0.093 3	0.944 1	0.944 5
	垂直	0.034 7	0.968 9	0.970 1
	对角线	−0.007 6	0.920 0	0.924 4

3.1.3　信息熵分析

信息熵是评估加密安全性的重要指标之一。对于有意义加密图像而言，加密图像的信息熵越靠近载体图像信息熵，则加密效果越好。图像信息熵的计算式为

$$\hat{H}(x)=-\sum_{i=1}^{N}p(x_i)\mathrm{lb}p(x_i) \tag{28}$$

其中，$p(x_i)$ 是 x_i 的发生概率。表 2 列出了将不同明文图像嵌入相同载体图像 Lena 后的信息熵结果。

从表 2 可知，加密图像的信息熵与载体图像的信息熵相关，随着载体图像的信息熵改变，加密图像的信息熵随之改变，这说明攻击者很难通过加密图像的信息熵来分析原始明文信息。

表 2　　信息熵结果

图像	明文图像	载体图像	加密图像	重构图像
Parrots	7.414 1	7.444 2	7.456 1	7.525 4
Monarch	7.471 6	7.444 2	7.455 0	7.572 7
Camera	7.009 7	7.444 2	7.455 9	7.046 4
Boats	7.145 6	7.444 2	7.455 8	7.403 1
Barbara	7.525 2	7.444 2	7.455 5	7.563 6

3.1.4　差分攻击

差分攻击指攻击者通过改变明文图像中的一个像素值，分析两幅加密图像之间的差异，建立明文图像和加密图像之间的关联，并尝试在未知密钥信息的前提下恢复明文图像。通常使用像素变化率（NPCR, number of pixels change rate）和统一平均变化强度（UACI, unified average changing intensity）来分析加密系统抵抗差分攻击的能力，计算式为

$$\mathrm{NPCR}=\frac{1}{N^2}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\% \tag{29}$$

$$\mathrm{UACI}=\frac{1}{N^2}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100\% \tag{30}$$

其中，C_1 和 C_2 为在明文图像上稍加修改而获得的 2 个加密图像。如果 $C_1(i,j)=C_2(i,j)$，则 $D(i,j)=0$，否则 $D(i,j)=1$。

本文算法通过改变明文图像 Parrots 的 1 bit 像素和 2 bit 像素，分别计算所生成的加密图像的 NRCR 和 UACI，结果如表 3 所示。从表 3 不难发现，1 bit 像素改变和 2 bit 像素改变所生成的加密图像差异不大，最大 NPCR 差异为 0.43%，最大 UACI 差异仅 0.01%，暗示了通过差分攻击来攻破加密系统是无效的。

表 3　　NPCR 和 UACI 结果

图像	1 bit 像素改变		2 bit 像素改变	
	NPCR	UACI	NPCR	UACI
Parrots	83.28%	0.76%	83.71%	0.76%
Monarch	83.48%	0.76%	83.11%	0.76%
Camera	83.79%	0.76%	83.87%	0.77%
Boats	83.59%	0.76%	83.36%	0.76%
Barbara	83.55%	0.76%	83.54%	0.76%

3.1.5　选择明文攻击

已知明文攻击（KPA, known plaintext attack）指攻击者在事先了解明文和相应密文的情况下试图揭露密钥关联信息的密码分析模型。与 KPA 相比，选择明文攻击具有更强大的能力，攻击者可以选择任意明文并生成相应密文，以揭示密钥相关信息。如果一种加密方案能够抵抗 CPA，则该方案也能抵抗 KPA。基于此，安全的图像加密机制应该能够抗 CPA。在本文算法中，虽然明文图像只改变了 1 bit 信息，但所生成的秘密图像存在明显差异，这是由于加密过程的密钥由哈希值控制，而哈希值对明文极其敏感，微小改变的明文图像都会生成完全不同的预加密图像，从而生成完全不同的秘密图像。基于以上分析，本文算法可以抵制 CPA。

3.2　比较

3.2.1　噪声和裁剪攻击

加密图像在不安全通道中传输时容易遭到噪声干扰，安全的加密算法应具备抗噪声干扰能力。本节将分析本文算法和文献[20]算法在抗噪声攻击方面的能力。在实验过程中，本文算法和文献[20]算法均采用二维投影梯度重构方法[21,25]重构原始明文图像。图 7 给出了遭受不同强度椒盐噪声攻击后的加密图像以及重构图像结果。由图 7 可知，当噪声强度从 0.000 1 增加到 0.001 0 时，文献[20]算法的重构图像 PSNR 依次为 29.142 8 dB、21.758 5 dB 和 18.423 5 dB，而本文算法的重构图像 PSNR 依次为 32.158 2 dB、26.522 0 dB 和 20.382 2 dB。显然，本文算法的抗噪声干扰能力优于文献[20]算法。

为了测试抗裁剪攻击能力，将文献[20]算法和本文算法的加密图像的不同区域的像素值设置为 0，相应结果如图 8 所示。随着裁剪区域的逐渐增大，文献[20]算法的重构图像 PSNR 依次为 23.423 7 dB、20.142 6 dB 和 16.854 8 dB，而本文算法的重构图像 PSNR 依次为27.288 9 dB、24.272 8 dB 和 18.354 2 dB。因此，无论是抗噪声干扰能力还是抗裁剪攻击能力，本文算法均优于文献[20]算法。

3.2.2　加密图像视觉安全性比较

为了进一步验证加密图像的视觉安全性，本节计算本文算法的加密图像和载体图像之间的 PSNR 和 MSSIM，并和文献[12,13,15,17,20]算法进行比较。在实验中，除上文测试图像 Parrots、Monarch、Camera、Boats、Barbara 和 Lena 外，对常用测试图像 Peppers、Jet、Baboon、Girl、Goldhill 和 Bridge 也进行了测试。同时，明文图像和载体图像实现一一对应，即不同的明文图像将生成不同的加密图像。表 4 和表 5 分别给出了本文算法和文献[12,13,15, 17,20]算法的加密图像 PSNR 和 MSSIM。从表 4 和表 5 可知，本文算法的加密图像 PSNR 和 MSSIM 均高于其他算法。这是因为其他算法采取直接位替换操作修改载体

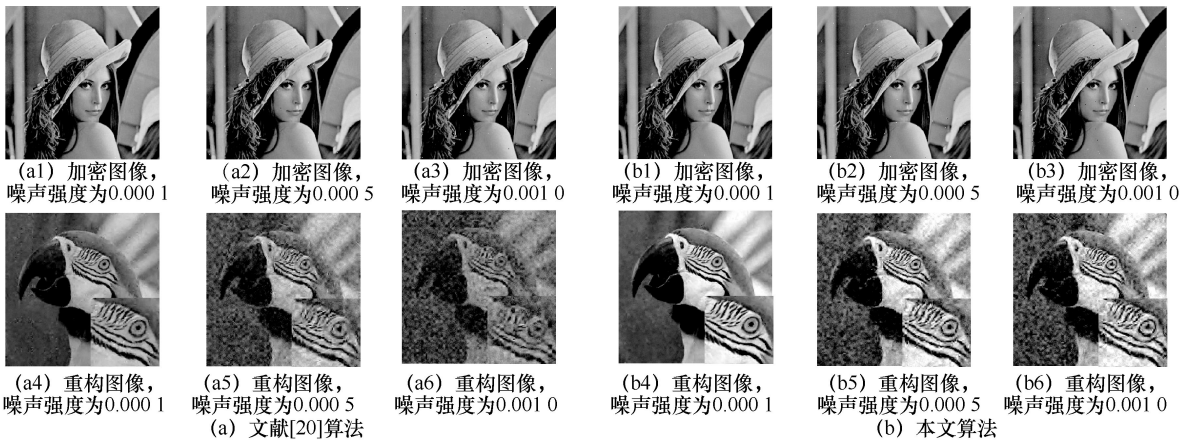


图 7　本文算法和文献[20]算法椒盐噪声攻击结果

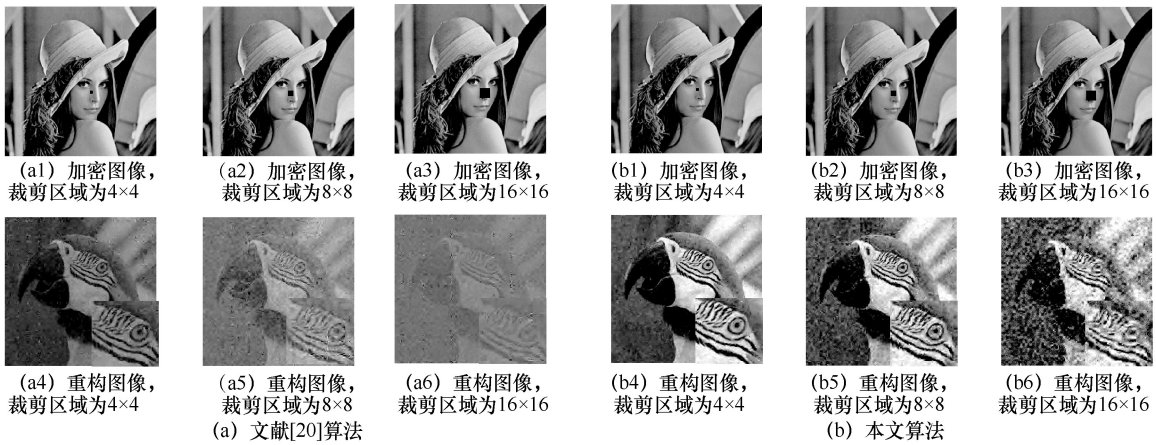


图 8　本文算法和文献[20]算法裁剪攻击结果

表 4　加密图像 PSNR 比较

明文图像	载体图像	文献[12]算法	文献[13]算法	文献[15]算法	文献[17]算法	文献[20]算法	本文算法
Len	Peppers	32.351 3	34.513 4	31.798 6	35.143 5	41.667 3	42.320 7
Jet	Baboon	37.105 8	35.156 7	32.597 6	32.456 5	41.505 9	42.325 4
Girl	Goldhill	36.112 5	34.254 3	32.064 7	32.224 3	41.601 6	42.323 4
Barbara	Bridge	35.562 9	36.113 4	31.739 7	33.435 5	41.490 3	42.249 3
平均	—	35.283 1	35.009 5	32.050 2	33.315 0	41.566 3	42.304 7

表 5　加密图像 MSSIM 比较

明文图像	载体图像	文献[12]算法	文献[13]算法	文献[15]算法	文献[17]算法	文献[20]算法	本文算法
Lena	Peppers	0.925 7	0.995 2	0.990 3	0.991 8	0.996 7	0.998 3
Jet	Baboon	0.983 3	0.995 6	0.995 5	0.979 7	0.997 6	0.998 3
Girl	Goldhill	0.966 6	0.997 3	0.994 2	0.964 1	0.997 2	0.997 5
Barbara	Bridge	0.978 3	0.998 2	0.994 6	0.988 9	0.998 6	0.999 4
平均	—	0.963 5	0.996 6	0.993 7	0.981 1	0.997 5	0.998 4

系数值，而本文算法考虑了待嵌入数据和待修改载体系数之间的关系，有效降低了由于嵌入而造成的载体数据的修改幅度，从而提高了加密图像的视觉安全性。

3.2.3　重构图像质量比较

为了分析重构图像效果，使用 512 像素×512 像素的相同明文图像 Barbara 及等大小的不同载体图像 Lena、Boat、Je 和 Peppers 进行测试，计算重构图像和原始明文图像之间的 PSNR 和 MSSIM，并和文献[12,13,15,17,20]算法进行比较。具体实验过程中，文献[12,13,15,17]算法采用 1DCS 先压缩明文图像再加密，对提取信息解密后利用正交匹配追踪（OMP, orthogonal matching pursuit）进行图像重构；而文献[20]算法和本文算法采用 2DCS 压缩加密明文图像，利用二维投影梯度 2DPG 方法同时进行解压缩和解密得到重构图像。表 6 列出了不同算法的 PSNR 和 MSSIM 结果。从表 6 中可以看出，文献[20]算法和本文算法的重构图像质量明显优于文献[12,13,15,17]算法，主要原因是利用基于 2DPG 的图像重构效果优于 OMP 图像重构。此外，文献[20]算法的重构图像的 PSNR 和 MSSIM 不如本文算法所生成的结果，

表 6　重构图像 PSNR 和 MSSIM 比较

明文图像	载体图像	文献[12]算法		文献[13]算法		文献[15]算法		文献[17]算法		文献[20]算法		本文算法	
		PSNR/dB	MSSIM	PSNR/dB	MSSIM	PSNR/dB	MSSIM	PSNR/dB	MSSIM	PSNR/dB	MSSIM	PSNR/dB	MSSIM
Barbara（512 像素×512 像素）	Lena（512 像素×512 像素）	28.443 5	0.812 8	28.553 4	0.993 2	27.123 2	0.814 5	32.118 5	0.867 0	35.778 4	0.985 8	36.145 0	0.986 1
	Boats（512 像素×512 像素）	28.443 5	0.812 8	28.553 4	0.993 2	26.987 5	0.801 6	31.672 1	0.828 9	35.753 8	0.985 8	36.279 5	0.986 3
	Jet（512 像素×512 像素）	28.443 5	0.812 8	28.553 4	0.993 2	26.714 5	0.793 4	31.982 1	0.896 7	35.103 1	0.983 4	35.894 6	0.985 3
	Peppers（512 像素×512 像素）	28.443 5	0.812 8	28.553 4	0.993 2	27.014 5	0.803 4	29.960 2	0.784 5	35.485 4	0.984 1	35.969 1	0.985 5

这是因为文献[20]算法采取二维随机置乱 2DRP 操作进行加密，而本文算法采取全局随机置乱 GRP 操作进行加密，利用 GRP 加密在一定程度上提升了重构图像质量。

综上，本文算法具有更优的重构图像质量。

4 结束语

本文提出了一种基于二维压缩感知的有意义图像加密算法。首先，设计了一种与明文相关联的混沌伪随机数生成方法，在此基础上，利用 GRP 操作加密明文图像，提高了加密安全性且改进了重构图像质量。其次，利用平滑函数嵌入方法自适应地将秘密图像嵌入载体图像中，有效提高了加密图像的视觉安全性。然而，由于 2DCS 的输入是预加密图像而非原始明文图像，当遭受噪声干扰时，在解压缩图像上进行解密会对重构图像质量造成一定的影响。下一步工作将考虑在压缩之前引入矢量量化操作，将量化后的误差矩阵作为 2DCS 的输入，图像重构由矢量量化矩阵和重构误差矩阵联合完成，以提高有意义加密算法的稳健性。

参考文献：

[1] REN H, NIU S Z. Separable reversible data hiding in homomorphic encrypted domain using POB number system[J]. Multimedia Tools and Applications, 2022, 81(2): 2161-2187.

[2] 印曦, 黄伟庆. 基于混沌理论的彩色 QR 编码水印技术研究[J]. 通信学报, 2018, 39(7): 50-58.
YIN X, HUANG W Q. Research on color QR code watermarking technology based on chaos theory[J]. Journal on Communications, 2018, 39(7): 50-58.

[3] CHAI X L, FU X L, GAN Z H, et al. A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 2019, 155: 44-62.

[4] WU J H, LIAO X F, YANG B. Image encryption using 2D Hénon-Sine map and DNA approach[J]. Signal Processing, 2018, 153: 11-23.

[5] WANG Y, QUAN C, TAY C J. Asymmetric optical image encryption based on an improved amplitude-phase retrieval algorithm[J]. Optics and Lasers in Engineering, 2016, 78: 8-16.

[6] 吴颖芝, 郝立波, 陈炬桦. T 型邻居细胞自动机的分组加密方法[J]. 通信学报, 2009, 30(S2): 52-60.
WU Y Z, HAO L B, CHEN J H. Block cipher based on T-shaped cellular automata[J]. Journal on Communications, 2009, 30(S2): 52-60.

[7] KADHIM I J, PREMARATNE P, VIAL P J, et al. Comprehensive survey of image steganography: techniques, evaluations, and trends in future research[J]. Neurocomputing, 2019, 335: 299-326.

[8] BAO L, ZHOU Y C. Image encryption: generating visually meaningful encrypted images[J]. Information Sciences, 2015, 324: 197-207.

[9] DONOHO D L. Compressed sensing[J]. IEEE Transactions on Information Theory, 2006, 52(4): 1289-1306.

[10] BARANIUK R G. Compressive sensing[J]. IEEE Signal Processing Magazine, 2007, 24(4): 118-121.

[11] CHAI X L, GAN Z H, CHEN Y R, et al. A visually secure image encryption scheme based on compressive sensing[J]. Signal Processing, 2017, 134: 35-51.

[12] WANG H, XIAO D, LI M, et al. A visually secure image encryption scheme based on parallel compressive sensing[J]. Signal Processing, 2019, 155: 218-232.

[13] CHAI X L, WU H Y, GAN Z H, 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.

[14] WEN W Y, HONG Y K, FANG Y M, et al. A visually secure image encryption scheme based on semi-tensor product compressed sensing[J]. Signal Processing, 2020, 173: 107580.

[15] ZHU L Y, SONG H S, ZHANG X, et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding[J]. Signal Processing, 2020, 175: 107629.

[16] YE G D, PAN C, DONG Y X, et al. Image encryption and hiding algorithm based on compressive sensing and random numbers insertion[J]. Signal Processing, 2020, 172: 107563.

[17] WANG X Y, REN Q, JIANG D H. An adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing[J]. Nonlinear Dynamics, 2021, 104(4): 4543-4567.

[18] ZHOU N R, PAN S M, CHENG S, et al. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing[J]. Optics & Laser Technology, 2016, 82: 121-133.

[19] CHAI X L, WU H Y, GAN Z H, et al. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing[J]. Information Sciences, 2021, 556: 305-340.

[20] HUO D M, ZHU Z L, WEI L S, et al. A visually secure image encryption scheme based on 2D compressive sensing and integer wavelet transform embedding[J]. Optics Communications, 2021, 492: 126976.

[21] ZHANG B, XIAO D, XIANG Y. Robust coding of encrypted images via 2D compressed sensing[J]. IEEE Transactions on Multimedia, 2021, 23: 2656-2671.

[22] ZHANG X C, HAN F, NIU Y. Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding[J]. Computational Intelligence and Neuroscience, 2017, 2017: 6919675.

[23] SOLAMI A E, AHMAD M, VOLOS C, et al. A new hyperchaotic

system-based design for efficient bijective substitution-boxes[J]. Entropy, 2018, 20(7): 525.

[24] LEE T Y, LIN S D. Dual watermark for image tamper detection and recovery[J]. Pattern Recognition, 2008, 41(11): 3497-3506.

[25] CHEN G, LI D F, ZHANG J S. Iterative gradient projection algorithm for two-dimensional compressive sensing sparse image reconstruction[J]. Signal Processing, 2014, 104: 15-26.

[26] RUDIN L I, OSHER S, FATEMI E. Nonlinear total variation based noise removal algorithms[J]. Physica D: Nonlinear Phenomena, 1992, 60(1/2/3/4): 259-268.

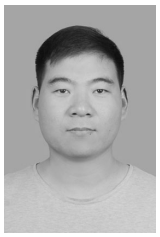
[27] SENDUR L, SELESNICK I W. Bivariate shrinkage functions for wavelet-based denoising exploiting interscale dependency[J]. IEEE Transactions on Signal Processing, 2002, 50(11): 2744-2756.

[作者简介]

任花（1992− ），女，河南信阳人，北京邮电大学博士生，主要研究方向为信息隐藏、图像加密和图像认证等。

牛少彰（1965− ），男，北京人，博士，北京邮电大学教授、博士生导师，主要研究方向为信息隐藏、图像取证等。

任如勇（1993− ），男，山东聊城人，北京邮电大学博士生，主要研究方向为数字取证、计算机视觉等。



岳桢（1988− ），男，河南新乡人，博士，河南师范大学实验师，主要研究方向为信息隐藏、多媒体教学等。