

面向秘密共享的逐层残差预测加密域大容量数据隐藏

温文嫒¹, 杨育衡¹, 张玉书^{2,3}, 方玉明¹, 邱宝林¹

¹江西财经大学 信息管理学院 南昌 中国 330032

²南京航空航天大学 计算机科学与技术学院 南京 中国 210016

³中国科学院信息工程研究所 信息安全国家重点实验室 北京 中国 100093

摘要 加密图像中的数据隐藏(Data Hiding in Encrypted Images, DHEI)是一种可行的云端存储方案,但其载体唯一,一旦被破坏就可能导致载体图像无法恢复。DHEI与秘密共享的结合能够在多载体图像中嵌入数据的同时保护原始图像的隐私性和安全性。但现有基于数据隐藏的秘密共享方案主要是利用自然图像像素的相关性为数据隐藏预留空间,嵌入容量受自然图像内容制约。在进行数据嵌入时,若数据量大于载体图像可嵌入容量,则存在数据丢失的可能性。针对该问题,本文基于压缩感知技术(Compressed Sensing, CS),提出一种面向秘密共享的逐层残差预测加密域大容量数据隐藏方案。首先,该方案通过压缩感知逐层预测技术(Layer-by-Layer Prediction Technology base on Compressed Sensing, LLPT-CS)减小测量值之间的冗余性,实现对原始图像进行加密的同时腾出嵌入空间(~4.0bpp);其次,加密图像以秘密图像共享(Secret Image Sharing, SIS)的形式生成 n 个秘密份额,分别发送至 n 个数据隐藏器;接着,数据隐藏器在无图像内容访问权限的情况下向秘密份额嵌入秘密数据;最后,接收端获取 n 个数据隐藏器中的任意 k 个秘密份额后即可依次通过拉格朗日插值法和CS重建算法恢复原始图像。实验结果表明,本文提出方案能实现嵌入率预设,保证数据嵌入的稳定性,并且能较好地保护云端图像存储的隐私性和安全性;与现有的秘密共享数据隐藏方案相比,该方案不仅能很好地为云端图像存储提供稳定的大容量秘密数据嵌入空间,而且还能恢复出在视觉上愉悦的图像,拥有现有方案不具备的逐步恢复功能。

关键词 逐层残差预测; 压缩感知; 数据隐藏; 秘密共享

中图分类号 TP309.7 DOI号 10.19363/J.cnki.cn10-1380/tn.2025.01.05

High-Capacity Data Hiding in Encryption Domain Based on Layer-by-Layer Residual Prediction for Secret Sharing

WEN Wenying¹, YANG Yuheng¹, ZHANG Yushu^{2,3}, FANG Yuming¹, QIU Baolin¹

¹School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330032, China

²College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

³State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract Data Hiding in Encrypted Images (DHEI) is a feasible cloud storage scheme, but its carrier image is unique, and once it is destroyed, the carrier image may be unrecoverable. The combination of data hiding and secret sharing in the encrypted domain can embed data in multiple carrier images while preserving the privacy and security of the original image. However, current secret-sharing schemes based on data hiding primarily employ the correlation of natural image pixels to reserve space for data hiding, and the embedding rate is limited by the natural image content. When embedding data, if the amount of data is greater than the embedding capacity of the carrier image, there is a possibility of data loss. To address this problem, based on compressed sensing(CS), this paper proposes a high-capacity data hiding scheme in encryption domain by employing layer-by-layer residual prediction for secret sharing scheme for secret sharing. First of all, the scheme uses layer-by-layer prediction technology base on compressed sensing(LLPT-CS) to reduce the redundancy between measured values, which can encrypt the original image while freeing up the embedding space(~4.0bpp). Second, the encrypted image creates n secret shares in the form of secret image sharing(SIS) and sends them to each of the n data hid-ers. Next, the data hid-ers embed secret data into the secret shares without having access to the image content. In the end, the receiver receives any of the k secret shares from n data hid-ers and can then recover the original image using Lagran-gian interpolation and CS reconstruction algorithms. The experimental findings demonstrate that the proposed scheme in

通讯作者: 张玉书, 博士, 教授, Email: yushu@nuaa.edu.cn。

本课题得到国家自然科学基金(No. 62201233, No. 61961022)资助、国家信息安全国家重点实验室基金(No. 2022-MS-02)、江西省双千计划(No. jxsq202301118)、江西省杰出青年基金项目(No. 20232ACB212004)、江西省教育厅基金 (No. GJJ210502) 资助。

收稿日期: 2023-02-13; 修改日期: 2023-06-20; 定稿日期: 2024-11-19

this paper provides more stable and large-capacity secret data embedding space for cloud image storage schemes than existing secret sharing data hiding schemes. Additionally, the proposed scheme recovers aesthetically pleasing images with a progressive recovery function that existing schemes lack.

Key words layer-by-layer residual prediction; compressed sensing; data hiding; secret sharing

1 引言

随着信息时代的到来,智能手机和电脑在为用户带来便捷的同时,也产生了大量的隐私数据^[1]。由于设备数据量的增加以及手机、电脑内存的限制,越来越多的用户选择将隐私数据存储至云端^[2-3],但云端是半信任的,这难免会给用户带来云端隐私数据泄露的担忧。图像作为最主要的信息源,一旦云端储存的个人隐私图像被窃取,将会给人们造成严重的危害,因此有必要对图像进行加密后再存储至云端。

传统图像加密算法包括数据加密标准(Data Encryption Standard, DES)、国际数据加密算法(International Data Encryption Algorithm, IDEA)、高级加密标准(Advanced Encryption Standard, AES)等,主要通过将明文图像数据转化为二进制流进行加密^[4]。此外, Pareek 等人^[5]提出利用 Logistic 映射将混沌序列转化为图像加密时使用的密钥流对图像进行加密。然而,上述加密方案仅用于保护图像隐私性,在云端存储场景中,云服务器接收到加密图像后,为实现用户或云端对图像的有效管理,云服务器需要在加密图像中嵌入用户 ID、时间戳、图像索引等数据。因此,云端存储图像既需要考虑图像隐私性,又需要考虑加密图像的数据可嵌入性。

DHEI 是一种有效的解决方案,由于该类方案能够在准确提取嵌入数据的同时保护原始图像的隐私而被应用于云端图像存储中^[6]。DHEI 的思想最早由 Puech 等人^[7]提出,原始图像通过 AES 生成加密图像后,数据隐藏器在每个包含 n 个像素的块中嵌入一个比特数据,证明了加密域数据隐藏的可行性。随后, Zhang^[8]利用流密码加密不改变像素相关性的性质,对原始图像进行加密后,将加密图像分割成若干非重叠块,数据隐藏器通过翻转像素的三个最低有效位(Least Significant Bit, LSB)将秘密信息嵌入到密文块中。项世军等人^[9]将同态加密技术应用于 DHEI 中,提高了数据嵌入安全性,但其数据嵌入率较小。近年来,文献[10]和文献[11]通过中值边缘预测器对像素最高有效位(Most Significant Bit, MSB)进行预测来预留空间,为 DHEI 提升了更理想的嵌入性能。然而,这些方案的载体图像唯一,一旦载体图像遭到恶意攻击,就会对其造成破坏,可能导致载体图像无法恢复。

为解决上述问题,研究人员将秘密共享^[12]与 DHEI 结合^[6,13-16],通过秘密共享将加密图像生成多个秘密份额,并分发给多个云服务器存储,只有在接收端获取大于最低阈值数量的秘密份额才能恢复出原始图像,有效解决了云端图像存储中单载体问题。在文献[13]中, Wu 等人首次将秘密共享应用于 DHEI,通过 Shamir 的秘密共享方案共享图像,并通过差分展开和直方图偏移方法将附加数据嵌入共享图像。受该工作启发, Chen 等人^[14]设计出一种新的数据隐藏器,采用差分展开和加法同态嵌入秘密数据,然而,该项工作嵌入率不高,且大于 250 的像素无法被加密。为提升容量, Chen 等人^[6]提出一种具有多个数据隐藏器的新方法,在数据隐藏阶段,每个数据隐藏器可以通过在每 n 个像素中替换一个像素来嵌入秘密数据,但随着数据隐藏器的数量增加,嵌入率急剧下降。为更好地权衡数据隐藏器数量与嵌入率关系, Hua 等人^[15]采用密码反馈秘密共享(Cipher-Feedback Secret Sharing, CFSS)技术生成加密图像,同时为嵌入数据腾出空间,在保证嵌入率不会随数据隐藏器数量改变而改变的同时,实现较大容量数据嵌入。上述方案利用自然图像像素的相关性为数据隐藏预留空间,从而实现加密图像数据嵌入,但其嵌入率受自然图像内容约束。在实际应用中,这种嵌入率的不可预测性给图像数据嵌入带来不稳定因素,例如当嵌入的数据量超过载体图像可承载的最大容量时,就会出现数据溢出问题,因此现有方案不具有数据嵌入稳定性。

CS 作为一种新颖的数据采样技术,仅使用少量样本即可高效获取和重建信号,一经提出,在众多领域引起高度的关注。它具有同时压缩、加密数据以及渐进恢复的特性,这些特性与密文图像信息隐藏有一定相似之处,这为解决加密领域的图像隐藏提供了新的思路。2020 年, Xiao 等人^[17]首次将 CS 的特性应用于 DHEI,提出一种大容量数据隐藏方案,该方案对原始图像进行压缩感知预测以创建备用空间,然后将图像加密发送到数据隐藏器,数据隐藏器将秘密数据嵌入到相应位置的 MSB 中。此外, Chen 等人^[18]提出基于压缩感知的图像编码方案,大大减少压缩感知测量值之间的冗余性,节省了大量的空间。受文献[17]和文献[18]的启发,本文提出一种基于压缩感知的大容量数据隐藏秘密共享方案。该方

案使用 LLPT-CS 技术, 对图像加密的同时生成残差空间, 并利用压缩感知的鲁棒特性对残差值进一步处理; 在 (k, n) 阈值秘密共享中, 依次根据设定的不同比特数对残差图像进行秘密共享操作, 生成 n 个具有嵌入空间的秘密份额, 并将每个秘密份额发送到云端服务器; 云端服务器向秘密份额嵌入加密数据并存储; 接收端可选择独立提取秘密份额中的加密数据, 或接受到大于阈值的秘密份额后恢复原始图像。本文的主要贡献和创新总结如下:

1) 本文首次提出一种融合压缩感知、数据隐藏和秘密共享的云端图像存储方案, 该方案能很好为云端图像储存方案提供稳定的大容量秘密数据嵌入空间, 在确保图像加密的安全性和隐私性的同时保证加密图像数据嵌入稳定性; 此外, 数据提取和图像恢复是独立的, 在云端图像存储场景中, 可根据不同权限对加密图像执行不同操作。

2) 本文方案利用 LLPT-CS, 通过 CS 渐进恢复的预测策略, 在加密的同时减小测量值之间的冗余性, 为加密图像腾出大容量加密域空间($\sim 4.0\text{bpp}$)用于嵌入秘密数据, 并在预测阶段巧妙运用压缩感知的鲁棒性对超过秘密共享阈值的测量值进行处理, 减小秘密共享的像素损失; 此外, 逐层恢复的结构设计使得该方案具有逐步重建能力。

3) 实验结果表明, 本文方案安全性高, 数据扩展率小; 同时保证重建原始图像具有较高质量, 且在一定条件下, 即使部分秘密份额丢失仍能恢复原始图像。

本文第 1 节介绍压缩感知、基于 CS 渐进恢复的预测策略和秘密共享等相关工作; 第 2 节介绍本文方案的具体实现过程; 第 3 节通过对比实验验证所提方案的可行性和优越性; 最后总结全文。

2 相关工作

2.1 压缩感知

CS 作为一种新兴的采样技术, 打破了传统奈奎斯特采样定律的对采样数目的约束, 能够以较低的采样率在信号采样的同时实现数据压缩, 并以较高的精确度重构原始信号。在压缩感知理论中, 通常需要从一组测量数据中采样数据, 假设一组信号 $x \in R^N$, 它对应的测量值为 $y \in R^M$ ($M \ll N$), 两者关系可以由以下公式表示:

$$y = \Phi x \quad (1)$$

其中, $\Phi \in R^{M \times N}$ 是测量矩阵, 通常为满足等距性质 (Restricted Isometry Property, RIP) 的各种随机矩阵。

例如 Gaussian 随机矩阵^[19]和结构随机 Hadamard 矩阵^[20]已被证明高概率满足 RIP。由于测量矩阵是秩亏的, 因此存在多个满足该方程的解。然而, 如果 x 足够稀疏和不相干, 则精确恢复是可能的。例如在变换域中, $\Psi \in R^{N \times N}$ 是稀疏基, $x = \Psi s$, s 中包含的非 0 元素远远小于 N , 表示为 $\|s\|_0 = k \ll N$ 。可以将公式 (1) 重新定义为:

$$y = \Phi \Psi s = As \quad (2)$$

其中, $A \in R^{M \times N}$ 被定义为感知矩阵。由于公式 (2) 中的解涉及定位 s 中的非零向量, 最简单的方法是 L_0 最小化, 写作

$$\min_x \|s\|_0 \quad \text{s.t. } y = As \quad (3)$$

然而对公式 (3) 的求解, 只能通过穷举所有稀疏组合, 才能找到最稀疏的形式, 其计算复杂, 甚至无法直接求解。因此, 用 L_1 最小化来估计 s 的接近最优解, 将该问题转化为求解一个凸优化的问题, 这是目前较常用的方法, 写成:

$$\min_x \|s\|_1 \quad \text{s.t. } y = As \quad (4)$$

求解公式 (4) 的方法有很多, 常见的方法有: 基追踪算法 (Basis Pursuit, BP)^[21]、贪婪算法 (Matching Pursuits, MP)^[22]、近似消息传递算法 (Approximate Message Passing, AMP)^[23] 以及迭代硬阈值算法 (Iterative Hard Thresholding, IHT)^[24]。本文采用 IHT 算法实现。

2.2 基于 CS 渐进恢复的预测策略

本文主要聚焦于压缩感知测量值的相关性, 利用 CS 逐渐恢复策略来隐藏秘密数据。假设 $y = \Phi x$ ($y \in R^M$), y 是测量值。将 y 分为两部分, 即 $y_{1:t} = (y_1, y_2, \dots, y_t)^T$ 和 $y_{t+1:m} = (y_{t+1}, y_{t+2}, \dots, y_m)^T$, 它们分别是由测量矩阵 Φ 的前 t 行和后 t 行得到:

$$y_{1:t} = \text{CS}(x, \Phi_{1:t}) = \Phi_{1:t} x \quad (5)$$

$$y_{t+1:m} = \text{CS}(x, \Phi_{t+1:m}) = \Phi_{t+1:m} x \quad (6)$$

其中, $\text{CS}(\cdot)$ 表示压缩感知采样操作, $\Phi_{1:t}$ 是 Φ 的前 t 行组成的子矩阵, $\Phi_{t+1:m}$ 为剩余子矩阵。由于压缩感知的逐渐恢复特性, 可以通过部分 y 值恢复出精确度较低的 x 值, 表示为:

$$\tilde{x} = \text{CS}^{-1}(y_z, \Phi_z) \quad (7)$$

其中, \tilde{x} 为恢复图像, $\text{CS}^{-1}(\cdot)$ 是压缩感知重建, y_z 表示 y 中的任意 z 个测量值, Φ_z 代表 y_z 对应索引行数的矩阵。因此, 对 $y_{1:t}$ 和 $y_{t+1:m}$ 分别进行重建, 可以得到 $y_{1:t}$ 和 $y_{t+1:m}$ 的重建图像 \tilde{x} :

$$\tilde{x} \approx CS^{-1}(y_{\dots t}, \Phi_{\dots t}) \approx CS^{-1}(y_{\dots t}, \Phi_{\dots t}) \quad (8)$$

由于 $y_{\dots t}$ 和 $y_{\dots t}$ 都可重建相似的图像, 因此可以通过 $y_{\dots t}$ 重建图像 \tilde{x} 后, 再使用 $\Phi_{\dots t}$ 采样得到对 $y_{\dots t}$ 的预测值 $\hat{y}_{\dots t}$, 即:

$$\hat{y}_{\dots t} = \Phi_{\dots t} \tilde{x} = \Phi_{\dots t} CS^{-1}(y_{\dots t}, \Phi_{\dots t}) \quad (9)$$

用 $\hat{y}_{\dots t} - y_{\dots t}$ 可以得到预测误差值, 预测误差值远远小于测量值, 因此只需保存 $y_{\dots t}$ 和误差值就可减小测量值之间的冗余性, 提升图像压缩效率。受该结论启发, 在加密域数据隐藏时, 需提前创建嵌入空间, 这与该策略有相似之处, 假设差值的最大比特为 b , 则剩余的 $8-b$ 比特可以为数据隐藏创造空间。

2.3 秘密共享

(k, n) 阈值秘密共享方案由 Shamir 提出^[12], 该方案将秘密信息分成 n 份, 由 n 个参与者参与共享, 每个参与者只能得到其中一个份额, 当接收者获取 k 个及 k 个以上的份额时, 秘密消息才能被无损恢复, 但小于 k 个份额无法恢复任何秘密信息。基于算法 [12], Thien 和 Lin 将其用于灰度图像中, 提出秘密图像共享方案^[25], 在该方案中, 将原始图像分为不重叠的若干份, 每份具有 k 个像素。对于每份生成一个

$(k-1)$ 次多项式, 如下所示:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \mod p \quad (10)$$

其中, a_0, a_1, \dots, a_{k-1} 表示每份的像素, $x_i, a_i \in GF(p)$, p 表示不超过 255 的最大素数。对于第 i 个参与者, 计算 $f(x_i)$, 重复上述操作, 得到 n 个秘密份额, 每个份额大小为原图的 $1/k$ 。接收端需要恢复原始图像时, 需要大于等于 k 个秘密份额, 通过拉格朗日插值法求解多项式 $\hat{f}(x)$, 得到恢复像素 a_0, a_1, \dots, a_{k-1} 。循环计算公式(11), 直至恢复原始图像:

$$\begin{aligned} \hat{f}(x) &= \sum_{i=1}^m f(x_i) \prod_{j=1, j \neq i}^m \frac{x - x_j}{x_i - x_j} \\ \text{s.t. } k &\leq m \leq n \\ &= a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \mod p \end{aligned} \quad (11)$$

3 提出方案

本文提出的云端存储方案, 主要由发送端、云服务器、接收端等三个部分组成, 具体的流程框架如图 1 所示。本节将详细描述各部分的具体实现过程。表 1 对本节相关变量作出说明。

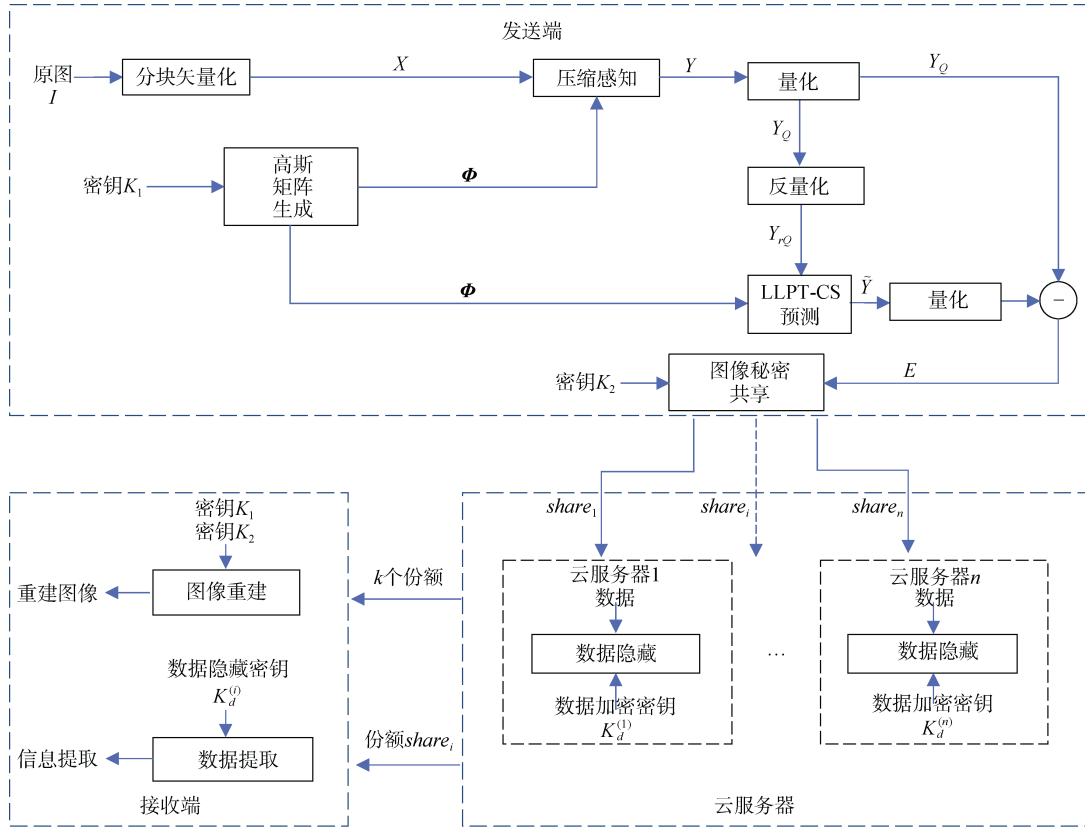


图 1 本文方案流程框架

Figure 1 The program flow framework

表 1 变量及说明

Table 1 Variables and descriptions

变量	说明	变量	说明
I	原始图像	X	分块矢量化后的原始图像
M	原始图像长度	N	原始图像宽度
$CS(\cdot)$	压缩感知采样	y_{\max}	Y 中的最大值
$CS^{-1}(\cdot)$	压缩感知重建	y_{\min}	Y 中的最小值
$divide(\cdot)$	分块器	γ	常数
$vec(\cdot)$	矢量化操作	Y_Q	反量化后的测量值
x_i	矢量化后的第 i 个图像块	$Q^{-1}(\cdot)$	反量化操作
s	x_i 的长度	l	预测层数
K_1	高斯测量矩阵生成密钥	u	每层的测量值长度
K_2	流加密密钥	\tilde{X}_i	预测过程前 i 层测量值恢复结果
Φ	高斯测量矩阵	$K_d^{(i)}$	第 i 个云服务数据加密密钥
Y	测量值	$E(i)$	第 i 层量化测量值与预测值差值
y_i	第 i 块图像测量值	$e_{c,d}^i$	残差 $E(i)$ 中的 c 行 d 列值
Y_Q	量化后的测量值	p_i	第 i 层设定素数值
$Q(\cdot)$	量化操作	b_i	第 i 层设定的最大比特位
$round(\cdot)$	四舍五入函数	$Eshare$	加密秘密份额
$share$	秘密份额	\hat{X}	最终重建图像
$SIS(\cdot)$	秘密图像共享	PR	伪随机字节

3.1 发送端

本文提出方案的主要创新集中在发送端,它由分块矢量化、压缩感知采样、量化与反量化、LLPT-CS 预测和秘密图像共享五部分构成。

3.1.1 分块矢量化

假设原始图像 I 为 8 位灰度图像,其尺寸大小为 $M \times N$ 。本文首先对 I 进行分块,分块的目的是将原始图像分割成 n 个非重叠的块,再把所有的块矢量化,以减小采样操作的复杂度,表示为:

$$X = [x_1, x_2, \dots, x_n] = \text{vec}(\text{divide}(I)) \quad (12)$$

其中, x_i 表示第 i ($1 \leq i \leq n$) 块, $\text{divide}(\cdot)$ 是分块器, $\text{vec}(\cdot)$ 为矢量化操作, x_i 的长度 s 为 $(M \times N)/n$ 。

3.1.2 压缩感知采样

分块后对矢量化像素块进行采样,采样矩阵是由密钥 K_1 控制生成的高斯测量矩阵,首次采样的采样率为 1,因此 $\Phi \in R^{s \times s}$,采样过程表示为:

$$Y = [y_1, y_2, \dots, y_n] = \Phi X = \Phi[x_1, x_2, \dots, x_n] \quad (13)$$

其中, y_i 为对第 i 块的测量值。

3.1.3 量化与反量化

量化的目的是将测量值 Y 映射到指定区间以便传输和存储。本文选择均匀量化器,其量化过程为:

$$Y_Q = Q(Y) = \text{round}\left(\frac{(Y - y_{\min})\gamma}{y_{\max} - y_{\min}}\right) \quad (14)$$

其中, Y_Q 为量化后的测量值, $Q(\cdot)$ 代表量化操作, $\text{round}(\cdot)$ 表示四舍五入函数, y_{\max} 为 Y 中的最大值, y_{\min} 是 Y 中的最小值, γ 为一个常数。反量化则与量化相反,它是为将指定区间的值恢复至原始大小,其还原过程为:

$$Y_Q = Q^{-1}(Y_Q) = Y_Q(y_{\max} - y_{\min})/\gamma + y_{\min} \quad (15)$$

其中, Y_Q 表示反量化后的测量值, $Q^{-1}(\cdot)$ 为反量化操作。测量值经量化和反量化后,会有一定程度的损失,这种损失被称为量化噪声。由于压缩感知技术的鲁棒性,含有噪声的测量值也能实现鲁棒恢复^[26]。

3.1.4 LLPT-CS 预测

预测的目的是为数据嵌入腾出空间,通过保留预测值和真实值的差来提升测量值之间的关联性以减少测量值的冗余。基于 CS 渐进恢复的预测策略是利用部分测量值对剩余测量值预测,本文创新性地改进该策略,将测量值分为多层用于循环预测,进一步提升预测精度以减小测量值冗余。具体地,将 Y_Q 分 l 层,对于第 i ($1 \leq i \leq l$) 层的测量值表示为:

$$Y_{rQ}(i,:) = Y_Q((i-1)u + 1:iu, :) \quad (16)$$

式中, $Y_{rQ}(i,:)$ 表示第 i 层经过量化和反量化后的测量值^①, u 是每层的测量值长度,其大小为 s/l 。

分层结束后进行预测,除第一层外,每层的测量值都可以预测。对于第 i ($2 \leq i \leq l$) 层的预测,使用前 $i-1$ 层的所有测量值以及各层对应的测量矩阵来恢复一个中间的结果:

$$\tilde{X}_{i-1} = CS^{-1}(Y_{rQ}(1:i-1), \Phi(1:i-1)) \quad (17)$$

这里, \tilde{X}_{i-1} 表示用前 $i-1$ 层测量值 $Y_{rQ}(1:i-1)$ 恢复的结果, $\Phi(1:i-1)$ 为该测量值对应的前 $i-1$ 层测量矩阵。可以得到对 i 层测量值的预测结果:

$$\tilde{Y}(i) = CS(\tilde{X}_{i-1}, \Phi(i)) \quad (18)$$

其中, $\tilde{Y}(i)$ 表示对第 i 层的预测值, $\Phi(i)$ 为第 i 层的测量矩阵。在得到对第 i 层的预测测量值之后,将

① 注: 为方便表示,在无特殊解释下后续所有 ij 操作都默认为取第 i 层到第 j 层,而非取第 i 个值到第 j 个值,“:”表示为取所有,后续操作默认取所有列,所以省略该符号。

$\tilde{Y}(i)$ 量化后与 $Y_Q(i)$ 作差得到残差图像 $E(i)$:

$$E(i) = Y_Q(i) - Q(\tilde{Y}(i)) \quad (19)$$

由于 $E(i)$ 值很小, 为方便后续数据嵌入, 本文对 $E(i)$ 中的每个残差值进一步处理, 假设 $E(i)$ 设定的最大比特位为 b_i 位, 则处理操作为:

$$e_{c,d}^i = \begin{cases} 2^{b_i-1} - 1, & e_{c,d}^i > 2^{b_i-1} - 1 \\ 1 - 2^{b_i-1}, & e_{c,d}^i < 1 - 2^{b_i-1} \\ e_{c,d}^i, & \text{else} \end{cases} \quad (20)$$

其中, $e_{c,d}^i$ 表示残差 $E(i)$ 中的 c 行 d 列值。由公式(10)知, 秘密共享中的像素值不能大于给定的素数, 否则就无法正确恢复图像。因此, 秘密共享阶段生成秘密份额时需要将大于给定素数的像素值进一步处理, 处理方法为:

$$e_{c,d}^i = \begin{cases} p_i, & (e_{c,d}^i + 2^{b_i-1} - 1) > p_i \\ 0, & (e_{c,d}^i + 2^{b_i-1} - 1) < 0 \\ e_{c,d}^i + 2^{b_i-1} - 1, & \text{else} \end{cases} \quad (21)$$

其中, p_i 表示第 i 层设定的值, 其大小为不超过 b_i 的最大素数。值得注意的是, 由于对残差进行处理会带来一些损失, 会导致压缩感知重建阶段会产生误差, 而且这些误差会随着重建层数的增多逐渐增大, 最后导致重建图像达不到预期效果。本文巧妙地利用压缩感知算法的鲁棒性, 将损失尽可能的减小, 具体操作为: 利用第 i 层经过处理后的残差 $E(i)$ 与测量值 $Y_Q(i)$ 相加后经过反量化后替换 $Y_{rQ}(i)$:

$$Y_{rQ}(i) = Q^{-1}(Y_Q(i) + E(i) + 1 - 2^{b_i-1}) \quad (22)$$

根据式(22), 在下次压缩感知重建时, 利用压缩感知技术的鲁棒性可以降低残差处理给重建带来的影响。对第二层至最后层循环上述操作后, 得到预处理残差图像 E 。第一层为关键层, 未经预测, 因此 $E(1) = Y_Q(1)$ 。算法 1 展示了预测部分的伪代码。

算法 1. 预测.

输入: Y_{rQ}, Y_Q, Φ, b, l

输出: E

```

1  预设:  $E=[]$ ;
2   $E(1) = Y_Q(1)$ ;
3  FOR  $i=2$  TO  $l$ 
4     $b_i = b[i], [L, W] = \text{size}(E(i))$ ;
5     $p_i =$  不超过  $b_i$  的最大素数;
```

```

6     $\tilde{X}_{i-1} = \text{CS}^{-1}(Y_{rQ}(1:i-1), \Phi(1:i-1))$ ;
7     $\tilde{Y}(i) = \text{CS}(\tilde{X}_{i-1}, \Phi(i))$ ;
8     $E(i) = Y_Q(i) - Q(\tilde{Y}(i))$ ;
9    FOR  $c=1$  TO  $L$ 
10   FOR  $d=1$  TO  $W$ 
11     IF  $(e_{c,d}^i + 2^{b_i-1} - 1) > p_i$  THEN
12        $e_{c,d}^i = p_i + 2^{b_i-1} - 1$ ;
13     ELSE  $(e_{c,d}^i + 2^{b_i-1} - 1) < 0$  THEN
14        $e_{c,d}^i = 0$ ;
15     ELSE
16        $e_{c,d}^i = e_{c,d}^i + 2^{b_i-1} - 1$ ;
17     END IF
18   END FOR
19 END FOR
20  $Y_{rQ}(i) = Q^{-1}(Y_Q(i) + E(i) - 2^{b_i-1})$ ;
21 END FOR
22 RETURN  $E$ 
23 算法 1 结束
```

3.1.5 秘密图像共享

共享过程是由残差图像 E 生成具有嵌入空间的秘密份额 $share$ 来实现。根据设定值 (k, n) , 利用秘密图像共享方案, 对不同的层使用不同的素数 p 生成 n 个大小为原始图像 $1/k$ 倍的秘密份额, 即:

$$[share_1, share_2, \dots, share_n] = \text{SIS}(E, p) \quad (23)$$

其中, $share_i$ 表示第 i 个份额, $\text{SIS}(\cdot)$ 为秘密图像共享操作, $p = [p_1, p_2, \dots, p_l]$ 。由于在量化和预测过程对大于 p 的值进行了处理, 因此不会出现像素值溢出。

此外, 由于压缩感知降维投影的线性关系, 攻击者仍然可能获得有关明文 X 的有用信息。如仅通过密文攻击了解明文能量可以推断出其内容^[27], 因此需要对秘密份额进一步加密。本文采用传统的流密码加密方式, 内容所有者通过密钥 K_2 生成伪随机字节 PR , 再异或(XOR)运算对秘密份额的每个像素进行加密生成加密份额 $Eshare$:

$$Eshare = share \oplus PR \quad (24)$$

3.2 云端

为满足云端对秘密份额管理的需求, 云端可以向秘密份额嵌入数据, 且用户可以根据自身需要向秘密份额嵌入额外数据。云端收到加密份额后, 无需获取密钥 K_2 , 仍可通过替换每层加密像素的前 $8-b_i$ 位将数据嵌入加密份额中。实例如图 2 所示, 假设第

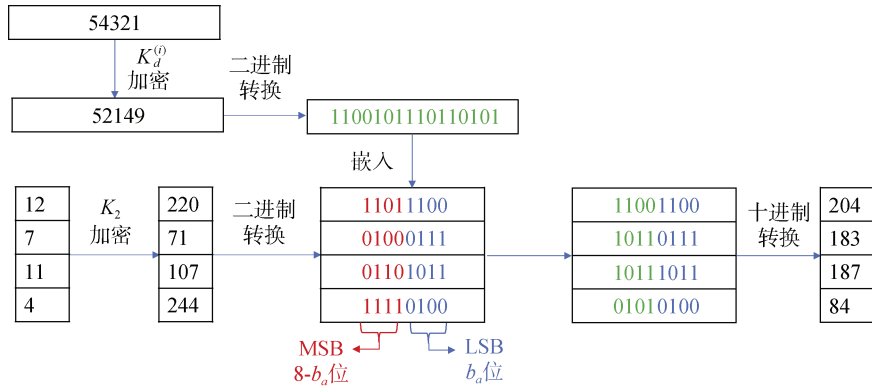


图2 数据嵌入

Figure 2 Data embedding

a 层的最大有效位 b_a 为 4 位, 则不超过 b_a 的最大素数 p_a 为 13, 该层像素值的范围为 $[0, 12]$ 。第 i 个云服务器接受到加密份额后, 向其嵌入图片序号 ‘54321’。首先通过数据加密密钥 $K_d^{(i)}$ 对图片序号加密, 再将加密份额像素值和加密图片序号转换成二进制, 接着根据第 i 层的最大有效位 b_a 判断嵌入空间大小。在该实例中, b_a 为 4, 因此每个像素可嵌入位为 $4=8-4$ 位, 四个像素可嵌入位为 16 位, 加密图片序号转换为二进制 ‘1100101110110101’ 比特数为 16 位, 即 4 个像素的空间可满足嵌入图片序号的需求。因此, 云端按从左到右, 从上到下的顺序依次向像素的 MSB 嵌入二进制数据, 最后将嵌入数据的二进制像素转换为十进制, 得到载密份额。

3.2.1 下载端

在接收端可进行两种操作, 即数据提取和图像重建, 且二者是可分离操作, 无先后次序。

3.2.2 数据提取

数据提取为数据嵌入反操作, K_d 在获取秘密份额各层的最大有效位 b 后, 逐层提取二进制像素的前 $8-b$ 位, 再将其转为十进制得到加密数据; 通过密钥 K_d 解密即可得到嵌入数据。

3.2.3 图像重建

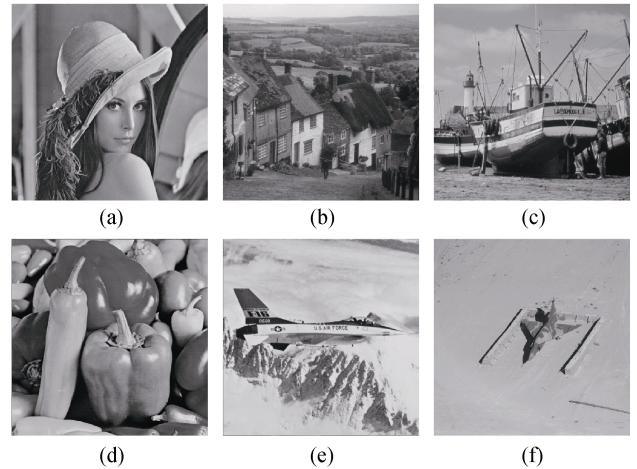
在下载端, 若接收到秘密份额的数量小于 k 个, 则无法重建原始图像。当接收到的秘密份额数量达到阈值 k 时, 首先根据 b 将秘密份额除第一层以外的 MSB 置 0, 再通过密钥 K_2 解密第一层加密份额。提取所有秘密份额后, 利用拉格朗日插值法重建残差图像 E 。由 2.1.4 部分的预测方法可知, 第一层为量化后的测量值, 可以经过反量化后直接重建恢复第一层图像, 其余层为残差层。因此, 在利用 K_1 生成 Φ 后, 逐层重建图像:

$$\hat{X}(i) = \begin{cases} CS^{-1}(Q^{-1}(E(i)), \Phi(i)), & i = 1 \\ CS^{-1} \left(Q^{-1} \begin{pmatrix} E(i) + \hat{X}(i-1) \\ \Phi(i) + 1 - 2^{b_i-1} \end{pmatrix}, \Phi(i) \right), & i > 1 \end{cases} \quad (25)$$

对所有层依次重复上述步骤, 最后整体压缩感知重建图像 \hat{X} 。

4 仿真结果与性能分析

为展示本文提出方案的优越性, 选取六幅具有不同特征的常用图像作为测试, 如图 3 所示。同时, 对本文所提算法的安全性和数据扩展率进行分析, 并与最新的基于秘密共享的加密域数据隐藏方案, 如 Chen 等人^[6]、Wu 等人^[13]、Hua 等人^[15]和 Qin 等人^[16], 进行实验对比。本文实验环境是在 AMD R5-3600 和 16GB RAM, 利用 MATLAB 2020A 软件进行仿真实验。



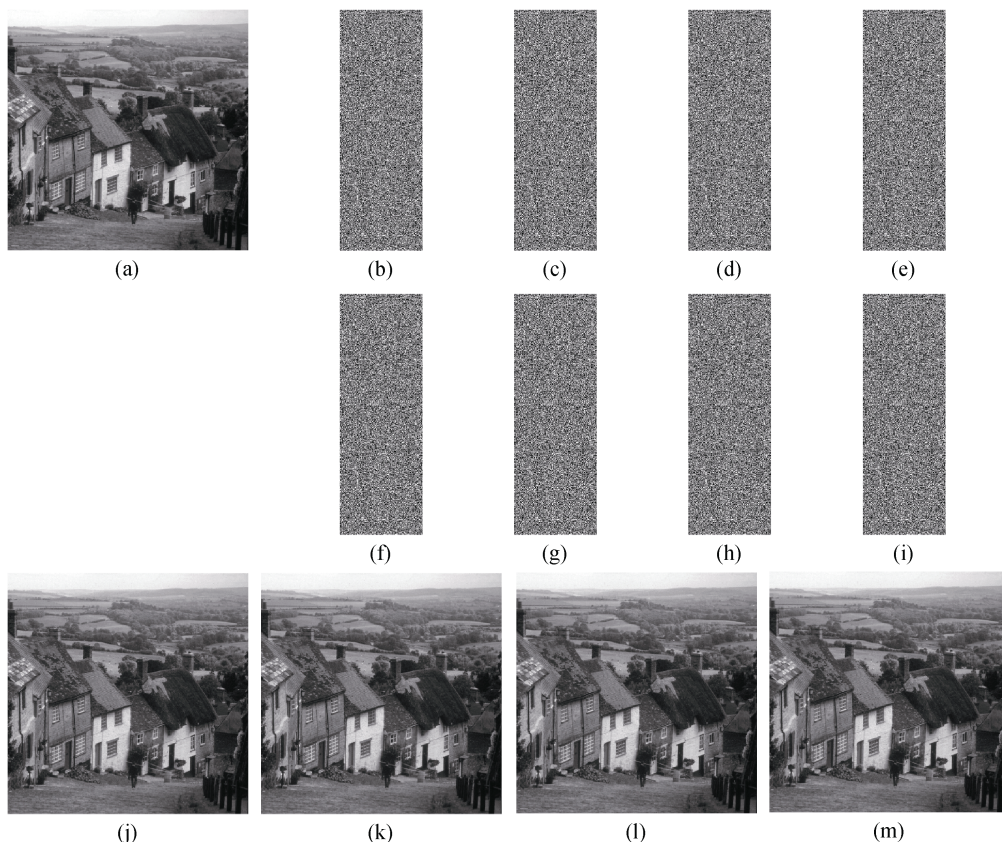
(a) Lena; (b) Goldhill; (c) Boat; (d) Peppers; (e) Jetplane; (f) Airplane

图3 大小为 512×512 的六幅测试图像Figure 3 Six test images of size 512×512

4.1 仿真结果

图 4 以图片 Goldhill 为例, (k, n) 阈值设定为(3, 4), 嵌入率为 3bpp, 层数设定 $l=4$, 对应层设定素数为 $p=[251, 63, 13, 7]$ 的实验仿真结果。(a)为原始图像 Goldhill, (b)~(e)为加密份额, (f)~(i)为嵌入数据后的秘密份额, (j)~(m)是从四个载密份额中任意选择三个进行差值重建并采用逐层重建算法恢复的图像。视

觉不可感知性是数据隐藏的重要指标之一, 因为数据被嵌入到图像中, 不同嵌入策略可能会对图像产生不同的视觉效果。如图 4 (b)~(e)与(f)~(i)所示, 加密份额与载密份额都以类噪声图像存储。因此, 本文提出方案具有较强的视觉不可感知性。值得注意的是, 本文方案还具有其他方案不具备的渐进恢复功能, 如图 5 所示。



(a) 512×512 尺寸的 Goldhill 原始图像; (b)~(e) 四个加密份额; (f)~(i) 四个载密份额; (j) 为 (f)、(g) 和 (h) 的 PSNR = 41.6 dB 的重建图像; (k) 为 (f)、(g) 和 (i) 的 PSNR = 41.6 dB 的重建图像; (l) 为 (f)、(h) 和 (i) 的 PSNR = 41.6 dB 的重建图像; (m) 为 (g)、(h) 和 (i) 的 PSNR = 41.6 dB 的重建图像

图 4 (3, 4) 阈值图像共享仿真结果

Figure 4 (3, 4) threshold image sharing simulation results



(a) 第一次重建图像 PSNR=28.3 dB; (b) 第二次重建图像 PSNR=31.1 dB; (c) 第三次重建图像 PSNR=34.30 dB; (d) 第四次重建图像 PSNR=41.6 dB;

图 5 以 Goldhill 为例, $l=4$ 渐层恢复图

Figure 5 Taking Goldhill as an example, the progressive recovery diagram of $l=4$

4.2 数据扩展

数据扩展意味着加密图像或载密图像在尺寸上

比原始图像大。如文献[13]中所定义, 数据扩展通过扩展速率进行评估, 其计算公式为:

$$\text{Expansion rate} = \frac{\text{Total bits of the encrypted image}}{\text{Total bits of the original image}} \quad (26)$$

对于本文方案, 内容所有者使用多层残差预测方法将原始图像转换为残差图像, 残差图像比特为原始图像的 $(1/8l) \sum_{i=1}^l (8-b_i)$ 倍, 残差图像生成原图 $1/k$ 倍的秘密份额, 并对秘密份额加密, 加密过程不会使数据扩展; 在云端, 云服务器将数据嵌入到秘密份额中, 数据嵌入同样不会产生数据扩展, 因此 n 个载密图像的总大小为原始图像的 n/k 。表 2 展示了发送端、云服务器和接收端在不同秘密共享策略下的扩展率。传统加密^[28-30]的方案不会发生数据扩展, 但安全性较

差; 同态加密的方案^[31-35]虽然具有高安全性, 但数据扩展严重, 加密图像为原始图像的百十倍。与基于同态的方案相比, 本文方案的数据扩展可接受。当数据隐藏器损坏时, 无法重建原始图像, 而本文方法可以保证, 即使 $n-k$ 个云服务器被损坏, 原始图像仍可被重建。此外, 各个云服务器中存储有不同的载密份额, 接收者需要 k 个载密份额来恢复原始图像, 这意味着即使 n 个载密份额中的任意 $k-1$ 个载密份额被泄露, 原始图像仍不能被恢复, 保证原始图像安全性。总之, 通过适当的数据扩展, 本文方案解决了潜在的数据隐藏器损坏问题, 而且还降低了原始图像泄漏概率。

表 2 嵌入率为 4bpp 时发送端、云服务器和接收端的图像扩展速率

Table 2 Image expansion rates of the sender, cloud end, and receiver when the embedding rate is 4bpp

	$n=2$	$n=3$	$n=4$	$n=5$
$k=2$	1, 1/2, 1	3/2, 1/2, 1	2, 1/2, 1	5/2, 1/2, 1
$k=3$	/	(1, 1/3, 1)	4/3, 1/3, 1	5/3, 1/3, 1
$k=4$	/	/	1, 1/4, 1	5/4, 1/4, 1
$k=5$	/	/	/	1, 1/5, 1

4.3 嵌入率与重建图像质量

本文方案的嵌入性能主要是通过云端接收到的加密图像的嵌入量来体现, 而有效嵌入容量是指通过数据隐藏器将秘密数据嵌入到加密图像中的最大数量, 嵌入性能通常用嵌入率(Embedding Rate, ER)来评估, 它表示为每个像素的平均可嵌入容量, 例如嵌入率为 4 bpp, 原始像素为 8 位, 则平均每个像素中的 4 位可用于嵌入信息, 其计算公式为:

$$\text{ER} = \frac{\text{Effective embedding capacity}}{\text{Pixel bits of each encrypted image}} \quad (27)$$

在本文的方案中, 嵌入率取决于层数 l 和比特数 b , 嵌入率表示为:

$$\text{ER} = \sum_{i=1}^l (8-b_i) / l \quad (28)$$

表 3 列出图像 *Lena* 作为测试图像, 在接收端获取的相应加密图像在不同层数下的比特数、嵌入率以及重建图像的 PSNR 值。本文选取 2、4、8、16 层进行大量实验。结果表明, 层数越多, 可嵌入的比特数越小, 嵌入率也就越大; 低层的 b_i 取值越大, 其图像的恢复效果越好。值得注意的是, 为保证该方案的高安全性, 需生成较多秘密份额, 本文设定 $b \geq 3$, 因此生成的秘密份额最少为 7。

为证实本文方案具有稳定的嵌入率以及较高的嵌入容量, 选取图 3 中的六张图像进行测试, 并与目前主流秘密嵌入方法, 如 Chen 等人^[6]、Wu 等人^[13]、

表 3 不同层数下的比特数、嵌入率以及 PSNR 值

Table 3 Number of bits, embedding rate and PSNR value under different layers

2 层	嵌入率 bpp	0~1.5	2	2.5	/
	PSNR	44.2	44	42.7	/
	比特数 b	8, 8~5	8, 4	8, 3	/
4 层	嵌入率 bpp	2	2.5	3	3.5
	PSNR	43.9	43.9	43.9	42.6
	比特数 b	8, 6, 6, 4	8, 6, 5, 3	8, 5, 4, 3	8, 4, 3, 3
8 层	嵌入率 bpp	2.5	3	3.5	4
	PSNR	43.5	43.3	43	42.1
	比特数 b	8, 6, 6, 6, 6, 5, 4, 3	8, 6, 6, 5, 5, 4, 3, 3	8, 6, 5, 4, 4, 3, 3, 3	8, 5, 4, 3, 3, 3, 3, 3, 3
16 层	嵌入率 bpp	3	3.5	4	4.5
	PSNR	43.2	42.7	42	38
	比特数 b	8, 6, 6, 6, 6, 6, 6, 6, 6, 3, 3, 3, 3, 3, 3	8, 6, 6, 6, 6, 6, 6, 4, 3, 3, 3, 3, 3, 3, 3	8, 6, 6, 6, 5, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3	8, 5, 4, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3

Hua 等人^[15]和 Qin 等人^[16], 在不同 (k, n) 阈值下的嵌入率进行比较, 如图 6 所示。实验表明, 四种对比算法中, Wu 等人^[15]和 Qin 等人^[16]不仅嵌入容量较低, 而且嵌入率不稳定; 与 Wu 等人^[13]和 Qin 等人^[15]相比, Hua

等人^[16]具有较高的嵌入率, 但是其嵌入率也不稳定; Chen 等人^[6]方法虽然有较好的嵌入稳定性, 但随着 n 值的增加嵌入率下降。而本文方法, 在不同 k 值和 n 值的情况下, 都具有较高且稳定的嵌入率。

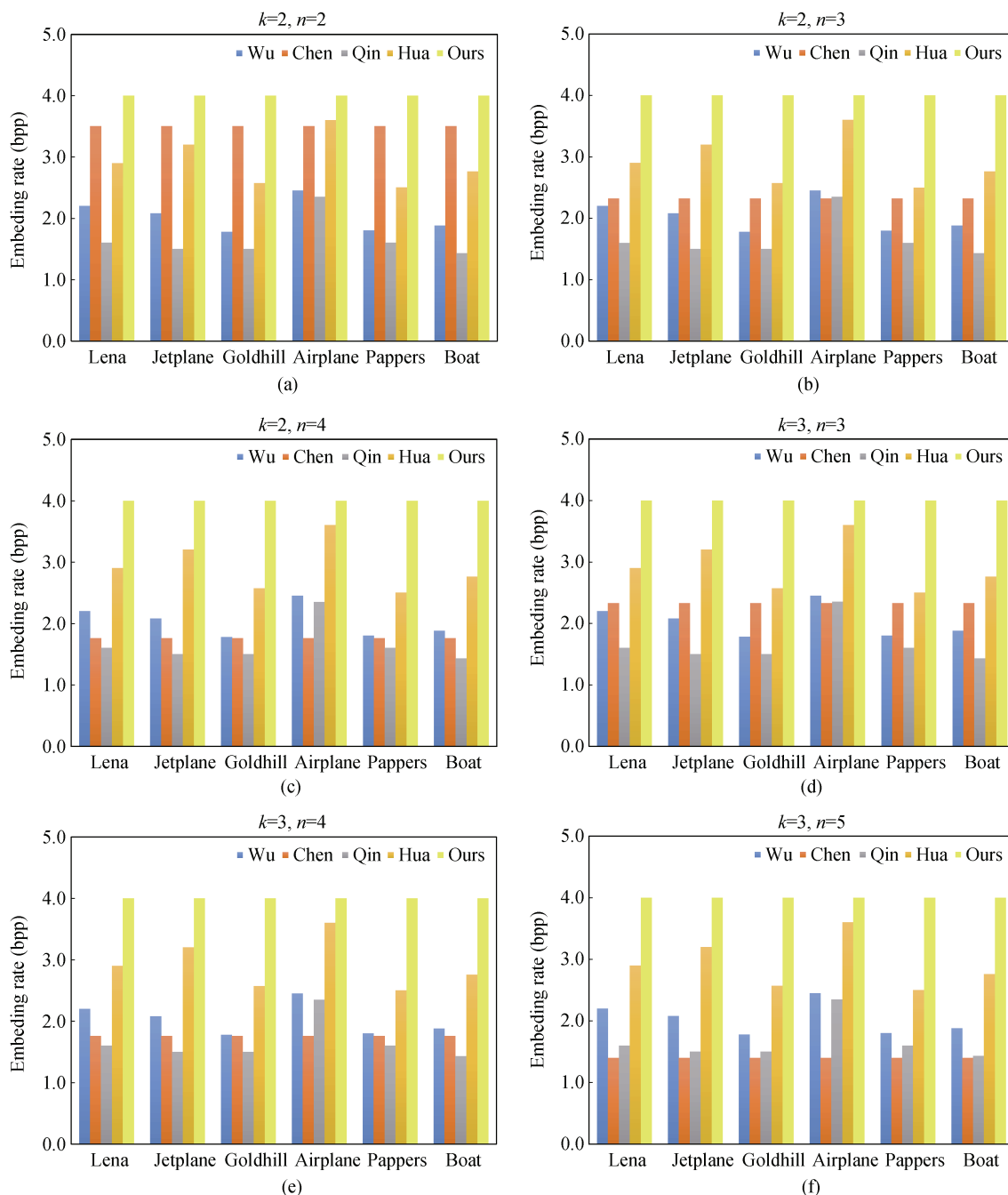


图 6 不同秘密共享方案在不同 (k, n) 阈值下的嵌入率

Figure 6 Embedding rates of different secret sharing schemes under different (k, n) thresholds

峰值信噪比(Peak Signal to Noise Ratio, PSNR)是评价图像重建质量的客观指标, 用来描述图像之间的差异。本文以 PSNR 为指标评价六幅测试图像在层数为 8, 最大嵌入容量为 4 bpp 时的重建图像, 如图 7 所示。从图 7 可以看出, 随着预设嵌入率提高,

图像 PSNR 逐渐下降; 此外, 由于不同图像的纹理细节的差异, 其重建图像的质量也有所不同。尽管经过 LLPT-CS 的图像质量有所下降, 但利用本文方案重建的图像 PSNR 值均高于 35 dB。因此, 本文方案在实现高嵌入率的同时也能恢复出不影响视觉体验的

高质量载体图像。为进一步证实提出方案恢复图像具有较高视觉质量, 本文在文献[36]和文献[37]提供的 196 张灰度图像(内容包括风景、人物、文字、动物、昆虫、植物、物品等)进行测试, 由于数据集图片尺寸大小不一, 因此统一裁剪并缩放为 512×512 , 实验结果的平均 PSNR 分别为 40.2 dB 和 36.8 dB, 证明本文方案用于不同类型图像都具有较好的恢复质量。

4.4 安全性

为证明本文方案具有高安全性, 本节将使用不同的统计指标, 包括水平和垂直相关系数、信息熵、密钥分析、以及直方图分析。

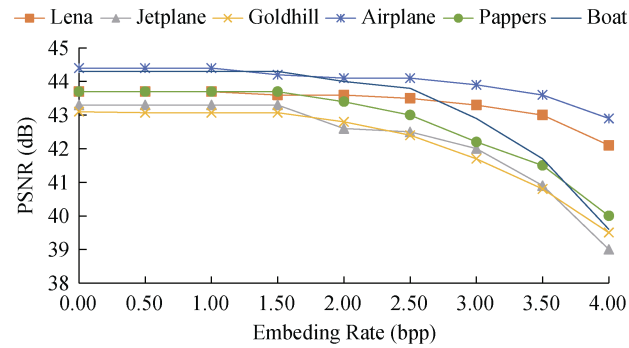


图 7 六幅测试图像在 $l=8$ 时预设嵌入率与 PSNR 关系
Figure 7 Relationship between preset embedding rate and PSNR for six test images of $l=8$

4.4.1 密钥分析

假设攻击者已获得大于 k 个秘密份额后对图像进行蛮力攻击。为抵抗蛮力攻击, 密钥空间应该足够大。本文算法的密钥主要来源于两个方面: 一是用于生成高斯测量矩阵 Φ 的初始参数 K_1 ; 二是对秘密份

额加密的密钥 K_2 。因此, 本文算法密钥空间为 $10^{16} \times 10^{24} = 10^{40} \approx 2^{120} (>> 2^{100})$, 足以抵御蛮力攻击。

4.4.2 直方图分析

直方图展示的是图像在每个灰度上像素值的分布情况, 加密图像的直方图应该满足均匀分布以防止攻击者获取直方图信息来抵抗统计分析攻击。本节选取 Lena 为原始图像, 阈值设定为(2, 2), 对其原图、秘密份额以及载密份额进行直方图分析。如图 8 所示, 秘密份额和载密份额均平坦而均匀, 与明文图像直方图具有较大差异, 证明本文的加密方案可以防止攻击者通过直方图获取有用信息。

4.4.3 相关性分析

相邻像素间的相关性是评价加密方案安全性的重要指标。本文为研究相邻像素的相关性, 从原始图像 Lena、秘密份额和嵌入数据的载密份额中随机选取 3000 对相邻像素, 分别计算其水平、垂直和对角线三个方向的相关系数。相关性计算公式为:

$$Corr = \frac{\sum_{i=1}^L \left(S_i - \frac{1}{N} \sum_{i=1}^N S_i \right) \left(O_i - \frac{1}{N} \sum_{i=1}^N O_i \right)}{\sqrt{\sum_{i=1}^L \left(S_i - \frac{1}{N} \sum_{i=1}^N S_i \right)^2 \times \sum_{i=1}^L \left(O_i - \frac{1}{N} \sum_{i=1}^N O_i \right)^2}} \quad (29)$$

其中 S_i 和 O_i 表示相邻像素的像素值, L 为像素对数, 图 9 展示的是明文、秘密份额以及载密份额在水平、垂直和对角线三个方向的相关性, 其相应的相关系数如表 4 所示。从图 9 和表 4 可以看出, 本文方案会极大减小图像的相邻像素相关性, 明文图像在水平、垂直和对角线的相邻像素具有较大相关性, 而秘密份额和载密份额则表现出较低相关性, 进一

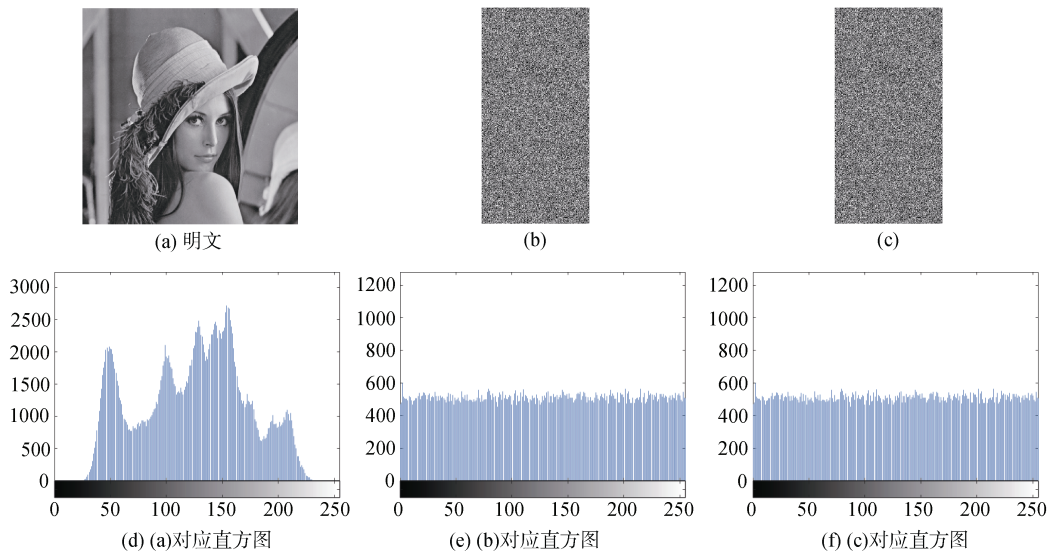


图 8 明文、秘密份额和载密份额直方图

Figure 8 Histogram of plaintext, secret share, and carrier share

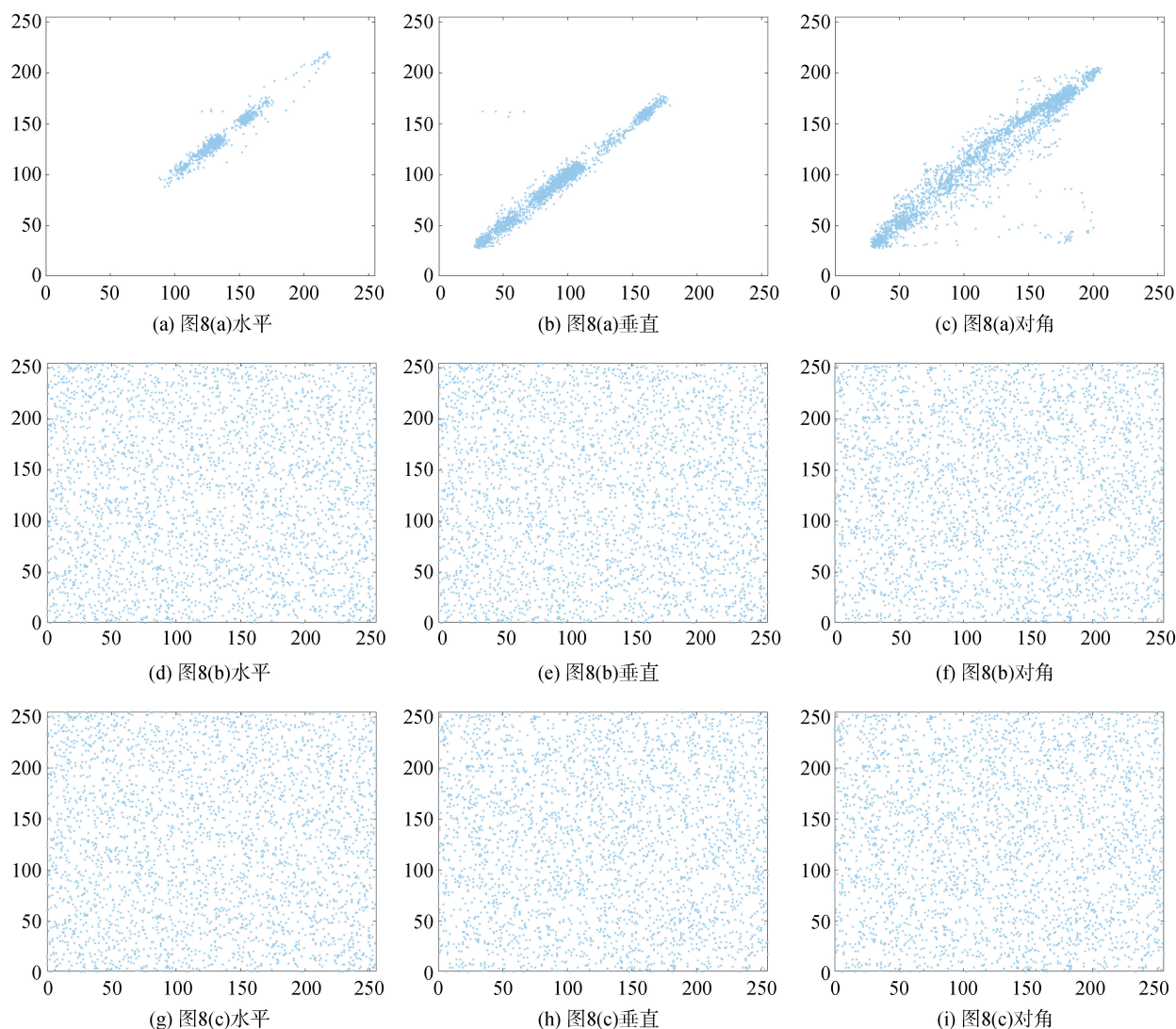


图 9 明文、秘密份额和载密份额相关性分析

Figure 9 Correlation analysis of clear text, secret share, and carrier share

表 4 明文、秘密份额和载密份额相关系数

Table 4 Correlation coefficient of clear text, secret share, and carrier share

名称	水平方向	垂直方向	对角方向
Lena	0.9844	0.9749	0.9364
秘密份额	0.0023	0.0242	-0.0136
载密份额	0.0035	-0.0083	-0.0085

步验证所提方案在云端存储中能较好保护图像的隐私性。

4.4.4 熵分析

熵是用于检测图像像素分布的重要指标。加密图像应具有均匀分布的像素以抵御基于统计的攻击。在理想状态下,所有像素值具有相等概率,图像熵定义如下:

$$H = -\sum_{i=1}^{N_a} P(S_i) \log_2(S_i) \quad (30)$$

其中, N_a 表示可能的像素值, $P(S_i)$ 表示像素值 S_i ($1 \leq S_i \leq N_a$) 出现的概率。对于一幅 8-bit 灰度图像, $N_a=256$, 并且当每个可能像素值具有相同概率时获得理论最大熵, 即 $P(S_i)=1/256$ 。因此理论最大熵值 H_{\max} 为: $H_{\max} = -\sum_{i=1}^{256} 1/256 \times \log(1/256) = 8$ 。加密图像的熵值越接近 8, 表示其图像像素分布更均匀。表 5 列出了 6 张测试图片的原始图像, 以及在本文方案中设定(2, 2)阈值后的各个份额的熵值。结果表明本文方案可以生成非常接近理论最大熵值 8 的加密图像, 这表明本文加密方案具有较高的像素随机性。

5 总结

为提高云端密文图像数据嵌入的稳定性, 本文提出一种面向秘密共享的逐层残差预测加密域大容量数据隐藏方案。该方案基于压缩感知渐进恢复特性,

表 5 六幅图像及对应加密图像的熵

Table 5 Entropy of six images and corresponding encrypted images

	原图	秘密份额 1	秘密份额 2	载密份额 1	载密份额 2
Lena	7.4455	7.9985	7.9986	7.9985	7.9985
Goldhill	7.2925	7.9986	7.9987	7.9988	7.9985
Boat	7.1914	7.9985	7.9985	7.9986	7.9986
Peppers	6.7624	7.9985	7.9987	7.9986	7.9987
Jetplane	6.7135	7.9985	7.9984	7.9987	7.9986
Airplane	4.0045	7.9987	7.9986	7.9987	7.9986

通过压缩感知逐层预测技术, 在对载体图像进行加密的同时腾出大容量嵌入空间, 此外巧妙利用压缩感知的鲁棒性解决秘密共享中像素值溢出问题。实验结果表明, 本文提出方案在嵌入率大小和嵌入率稳定性方面都优于现有方案, 且具有较高的安全性, 此外还具备现有方案不具有的逐步恢复能力。但本文方案多次使用传统压缩感知重建算法, 因此重建时间较长。接下来的工作考虑结合深度学习, 用深度学习方法做预测与重建, 以提高本文方案的性能。

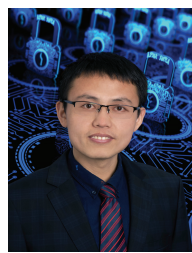
参考文献

- [1] Wang H, Huang F J. Attack and Improvement of an Authentication Scheme Based on Reversible Data Hiding[J]. *Journal of Cyber Security*, 2022, 7(1): 56-65.
(王泓, 黄方军. 基于可逆信息隐藏技术的认证方案的攻击与改进[J]. *信息安全学报*, 2022, 7(1): 56-65.)
- [2] Wu T Y, Huang F J. Adaptive JPEG Reversible Data Hiding Method Based on Pairwise Coefficients[J]. *Journal of Software*, 2022, 33(2): 725-737.
(吴桃宇, 黄方军. 基于系数配对的自适应 JPEG 可逆信息隐藏方法[J]. *软件学报*, 2022, 33(2): 725-737.)
- [3] Malik A, Wang H X, Chen Y L, et al. A Reversible Data Hiding in Encrypted Image Based on Prediction-Error Estimation and Location Map[J]. *Multimedia Tools and Applications*, 2020, 79(17): 11591-11614.
- [4] Akkar M L, Giraud C. An Implementation of DES and AES, Secure Against Some Attacks[M]. Koç Ç K, Naccache D, Paar C, eds. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 309-318.
- [5] Pareek N K, Patidar V, Sud K K. Image Encryption Using Chaotic Logistic Map[J]. *Image and Vision Computing*, 2006, 24(9): 926-934.
- [6] Chen B, Lu W, Huang J W, et al. Secret Sharing Based Reversible Data Hiding in Encrypted Images with Multiple Data-Hiders[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(2): 978-991.
- [7] Puech W, Chaumont M, Strauss O. A Reversible Data Hiding Method for Encrypted Images[C]. *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 2008: 534-542.
- [8] Zhang X P. Reversible Data Hiding in Encrypted Image[J]. *IEEE Signal Processing Letters*, 2011, 18(4): 255-258.
- [9] Xiang S J, Luo X R. Reversible Data Hiding in Encrypted Image Based on Homomorphic Public Key Cryptosystem[J]. *Journal of Software*, 2016, 27(6): 1592-1601.
(项世军, 罗欣荣. 同态公钥加密系统的图像可逆信息隐藏算法[J]. *软件学报*, 2016, 27(6): 1592-1601.)
- [10] Wu Y Q, Ma W J, Yin Z X, et al. Reversible Data Hiding in Encrypted Image Based on Bit-Plane Compression of Prediction Error[J]. *Journal on Communications*, 2022, 43(8): 219-230.
(吴友情, 马文静, 殷赵霞, 等. 基于预测误差位平面压缩的密文图像可逆信息隐藏[J]. *通信学报*, 2022, 43(8): 219-230.)
- [11] Ma W J, Wu Y Q, Yin Z X. High-Capacity Reversible Data Hiding in Encrypted Images Using Adaptive Encoding[J]. *Journal of Software*, 2022, 33(12): 4746-4757.
(马文静, 吴友情, 殷赵霞. 自适应编码的高容量密文可逆信息隐藏算法[J]. *软件学报*, 2022, 33(12): 4746-4757.)
- [12] Shamir A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612-613.
- [13] Wu X T, Weng J, Yan W Q. Adopting Secret Sharing for Reversible Data Hiding in Encrypted Images[J]. *Signal Processing*, 2018, 143: 269-281.
- [14] Chen Y C, Hung T H, Hsieh S H, et al. A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(12): 3332-3343.
- [15] Hua Z Y, Wang Y X, Yi S, et al. Reversible Data Hiding in Encrypted Images Using Cipher-Feedback Secret Sharing[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2022, 32(8): 4968-4982.
- [16] Qin C, Chanyu J, Mo Q, et al. Reversible Data Hiding in Encrypted Image via Secret Sharing Based on GF(p) and GF(2⁸)[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2022, 32(4): 1928-1941.
- [17] Xiao D, Li F, Wang M D, et al. A Novel High-Capacity Data Hiding in Encrypted Images Based on Compressive Sensing Progressive Recovery[J]. *IEEE Signal Processing Letters*, 2020, 27: 296-300.
- [18] Chen Z, Hou X S, Shao L, et al. Compressive Sensing Multi-Layer Residual Coefficients for Image Coding[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2020, 30(4): 1109-1120.
- [19] Baraniuk R G. Compressive Sensing [Lecture Notes][J]. *IEEE Signal Processing Magazine*, 2007, 24(4): 118-121.
- [20] Gan L, Do T T, Tran T D. Fast Compressive Imaging Using

- Scrambled Block Hadamard Ensemble[C]. *2008 16th European Signal Processing Conference*, 2008: 1-5.
- [21] Chen S S, Donoho D L, Saunders M A. Atomic Decomposition by Basis Pursuit[J]. *SIAM Review*, 2001, 43(1): 129-159.
- [22] Mallat S G, Zhang Z F. Matching Pursuits with Time-Frequency Dictionaries[J]. *IEEE Transactions on Signal Processing*, 1993, 41(12): 3397-3415.
- [23] Metzler C A, Maleki A, Baraniuk R G. From Denoising to Compressed Sensing[J]. *IEEE Transactions on Information Theory*, 2016, 62(9): 5117-5144.
- [24] Blanchard J D, Tanner J, Wei K. Conjugate Gradient Iterative Hard Thresholding: Observed Noise Stability for Compressed Sensing[J]. *IEEE Transactions on Signal Processing*, 2015, 63(2): 528-537.
- [25] Thien C C, Lin J C. Secret Image Sharing[J]. *Computers & Graphics*, 2002, 26(5): 765-770.
- [26] Dai Q H, Fu C J, Ji X Y. Research on Compressed Sensing[J]. *Chinese Journal of Computers*, 2011, 34(3): 3425-3434.
(戴琼海, 付长军, 季向阳. 压缩感知研究[J]. *计算机学报*, 2011, 34(3): 3425-3434.)
- [27] Zhang Y S, Wang P, Fang L M, et al. Secure Transmission of Compressed Sampling Data Using Edge Clouds[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(10): 6641-6651.
- [28] Puteaux P, Puech W. An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(7): 1670-1681.
- [29] Wu H T, Yang Z Y, Cheung Y M, et al. High-Capacity Reversible Data Hiding in Encrypted Images by Bit Plane Partition and MSB Prediction[J]. *IEEE Access*, 2019, 7: 62361-62371.
- [30] Yi S, Zhou Y C. Adaptive Code Embedding for Reversible Data Hiding in Encrypted Images[C]. *2017 IEEE International Conference on Image Processing*, 2017: 4322-4326.
- [31] Zhang X P, Long J, Wang Z C, et al. Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography[J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2016, 26(9): 1622-1631.
- [32] Chen B, Wu X T, Wei Y S. Reversible Data Hiding in Encrypted Images with Private-Key Homomorphism and Public-Key Homomorphism[J]. *Journal of Visual Communication and Image Representation*, 2018, 57: 272-282.
- [33] Chen B, Wu X T, Lu W, et al. Reversible Data Hiding in Encrypted Images with Additive and Multiplicative Public-Key Homomorphism[J]. *Signal Processing*, 2019, 164: 48-57.
- [34] Zheng S L, Wang Y Z, Hu D H. Lossless Data Hiding Based on Homomorphic Cryptosystem[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(2): 692-705.
- [35] Wen W Y, Fan J C, Zhang Y S, et al. APCAS: Autonomous Privacy Control and Authentication Sharing in Social Networks[J]. *IEEE Transactions on Computational Social Systems*, 2023, 10(6): 3169-3180.
- [36] Kulkarni K, Lohit S, Turaga P, et al. ReconNet: Non-Iterative Reconstruction of Images from Compressively Sensed Measurements[C]. *2016 IEEE Conference on Computer Vision and Pattern Recognition*, 2016: 449-458.
- [37] Guo J M, Sankarasrinivasan S. Digital Halftone Database (DHD): A Comprehensive Analysis on Halftone Types[C]. *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference*, 2018: 1091-1099.



温文嫒 于重庆大学获得博士学位。江西财经大学教授, 博士生导师, 研究领域为图像处理与加密、多媒体信息安全、人工智能安全、大数据与物联网、区块链。Email: wenyingwen@sina.cn



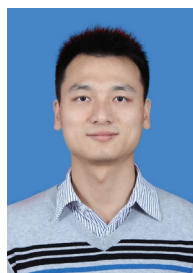
张玉书 于重庆大学获得博士学位。南京航空航天大学教授, 博士生导师, 研究领域为多媒体安全、区块链等。Email: yu-shu@nuaa.edu.cn



杨育衡 于江苏理工学院获得机械设计制造及自动化学士学位。现于江西财经大学电子信息专业攻读硕士学位。研究领域为图像处理与加密、压缩感知、多媒体信息安全。Email: 515951143@qq.com



方玉明 于南洋理工大学获得博士学位。江西财经大学教授, 博士生导师, 研究领域为、视频图像处理、计算机视觉、机器学习。Email: leo.fangyuming@foxmail.com



邱宝林 于北京邮电大学获得博士学位。江西财经大学讲师, 硕士生导师, 研究领域为神经网络动力学, 图像隐私保护。Email: qiubaolin_bupt@foxmail.com