面向压缩域数据盲提取的多层循环预测可逆隐藏方案

温文媖[1),2)] 杨育衡[1),2)] 罗新宇[1),2)] 张玉书[1),2)] 方玉明[1),2)]

[1)](江西财经大学计算机与人工智能学院 南昌 330013)

[2)](多媒体智能处理江西省重点实验室 南昌 330013)

摘 要 近年来,压缩感知(Compressive Sensing, CS)域的可逆数据隐藏已得到广泛研究。针对现有CS域可逆数据隐藏方案不能同时实现秘密信息盲提取、测量值直接可用问题,借助CS渐进恢复特性和预测误差扩展方法,本文提出一种面向压缩域数据盲提取的多层循环预测可逆隐藏方案。该方案通过构建多层循环预测嵌入,对CS测量值进行预测,利用直方图平移(Histogram Shifting, HS)对测量值嵌入额外信息,在提取信息阶段可实现信息盲提取和测量值无损还原;此外,为提高测量值可用性,本文提出一种冗余块估计方法,优先在冗余块进行信息嵌入,相比排序前,采样率0.5时平均PSNR最高提升2.8%。该方案结合了缩略图保持加密技术,在测量值中自嵌入图像本身的敏感区域保真值,为不同权限的用户提供不同的可见区域,实现多级预览;同时利用CS的鲁棒性,对测量值外嵌入需要隐藏的秘密信息,使得在不提取秘密信息的前提下,载密测量值重建图像与测量值重建图像保持高度相似(随嵌入率提升,平均PSNR为36 dB~48 dB),保证秘密信息的隐蔽性。实验结果表明,与最新方案相比,本文提出方案能够实现大容量嵌入(0 bit~35 000 bit)、秘密信息盲提取、测量值直接可用以及多级权限隐私保护。

关键词 可逆数据隐藏;压缩感知;循环预测;盲提取;预测误差扩展

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2025.00910

A Multi-Layer Cyclic Predictive Reversible Hiding Scheme for Data Blind Extraction of Compressed Domain

WEN Wen-Ying[1),2)] YANG Yu-Heng[1),2)] LUO Xin-Yu[1),2)] ZHANG Yu-Shu[1),2)] FANG Yu-Ming[1),2)]

[1)](School of Computing and Artificial Intelligence, Jiangxi University of Finance and Economics, Nanchang 330013)

[2)](Jiangxi Provincial Key Laboratory of Multimedia Intelligent Processing, Nanchang 330013)

Abstract Reversible data hiding in compressed sensing (CS) domains has been extensively studied in recent years. The proposal and development of reversible data hiding schemes in this domain have made it possible to hide large-capacity data in CS signals. However, existing reversible data hiding schemes in the CS domain face several challenges and limitations while realizing high-capacity data hiding. First, existing schemes usually lack directly usable measurements, which prevents the secret-carrying measurements from being directly used to reconstruct the original image, and thus can be easily detected during the transmission of the secret information. Second, some schemes generate auxiliary information when hiding the secret information, and these auxiliary information require an additional secure channel for transmission

收稿日期:2024-04-08;在线发布日期:2025-02-18。本课题得到国家自然科学基金青年科学基金项目(62201233)、江西省双千计划(jxsq2023201118)、江西省杰出青年基金项目(20232ACB212004)资助。 **温文媖**(通信作者),教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究方向为图像处理与多媒体安全。E-mail:wenyingwen@sina.cn。 **杨育衡**,硕士研究生,主要研究方向为压缩感知与图像隐藏。**罗新宇**,硕士研究生,主要研究方向为压缩感知与图像隐藏。 **张玉书**,教授,博士生导师,中国计算机学会(CCF)会员,主要研究方向为多媒体安全与人工智能安全。 **方玉明**,教授,博士生导师,中国计算机学会(CCF)杰出会员,主要研究方向为视觉质量评估、计算机视觉、3D图像/视频处理。

to ensure the correct extraction of the secret information, thus these schemes are unable to realize the blind extraction of the secret information. To address these problems, this paper proposes a new scheme, i. e., multi-layer cyclic predictive reversible hiding scheme for data blind-extraction of compressed domain. This new scheme utilizes the asymptotic recovery property of CS and the prediction error expansion technique to hide and extract data through multi-layer cyclic prediction. Specifically, this scheme performs cyclic prediction of CS measurements by CS multilayer cyclic prediction embedding technique and generates sharp histograms of prediction errors, which provide a large-capacity space for secret data embedding. Then, the additional information is embedded in the prediction error and then superimposed on the measurements by employing the histogram shifting method, and finally the auxiliary information is hidden in the lowest significant bit of the measurements in the specified region. In this way, blind extraction of information can also be realized when extracting information, and the lossless restoration of measurement values can be guaranteed. In addition, a redundant block estimation method is proposed in this paper to further improve the usability of the measurement values. The method utilizes the property that compression perception has higher reconstruction quality in redundant regions, image blocks are sorted and the secret information is preferentially embedded in the redundant blocks. On the BSD68 dataset, when the sampling rate is 0.5 and the embedding capacity is 35,000 bits, the average PSNR is improved by 2.8% compared to the unsorted one, which demonstrates the effectiveness and practicality of this approach. Moreover, for different application scenarios, the scheme proposed in this paper also incorporates thumbnail preserving encryption, which can self-embed the fidelity value of the sensitive region of the image itself into the measurement value, thus providing different visible regions for users with different privileges, and realizing the preview of multilevel privileges. At the same time, the additional secret information that needs to be hidden can be embedded into the measurement values by utilizing the robust reconstruction property of CS, so that without extracting the secret information, the reconstructed image after the encrypted measurement values remains highly similar to the reconstructed image after the unencrypted measurement values, ensuring the concealment of the secret information. Experimental results demonstrate that the multi-layer cyclic predictive reversible hiding scheme proposed in this paper can achieves blind extraction of secret information, direct usability of measurements, and privacy protection with multiple levels of permissions, as well as better visualization and embedding capabilities. In the dataset BSD68, compared with other compressed domain data hiding schemes with the same compression rate, this proposed scheme has a higher embedding capability, with more than 8% improvement in embedding capability. These advantages make this scheme will have a wide range of application prospects and important research significance in practical applications.

Keywords　reversible data hiding; compressed sensing; cyclic prediction; data blind extraction; prediction error expansion

1　引　言

可逆数据隐藏(Reversible Data Hiding, RDH)作为一种重要的数据隐藏技术,能够从载密图像中提取嵌入的秘密数据的同时无损恢复载体图像,可以广泛应用在医学影像、军事图像处理、法律服务等需要进行覆盖数据恢复的场景中。现有RDH大致可分为三大类:明文域的RDH[1-5]、压缩域的RDH[6-10]和加密域的RDH[11-13]。本文聚焦于压缩域的RDH。

对于压缩域RDH方案,数据往往被嵌入到压缩

系数中，由于压缩域中的冗余远远小于空间域，因此压缩域方法获得的嵌入容量十分有限。JPEG是将数字图像压缩到较小尺寸以节省存储空间和传输时间的最常用压缩技术。目前，基于JPEG压缩的RDH研究已经相当成熟。但JPEG图像依赖于Nyquist-Shannon采样，在一些特殊的应用中，超越Nyquist-Shannon采样可能是必要的，这些应用可能涉及到非常稀疏的信号或需要更高的保真度和细节保留[14]。压缩感知(Compressive Sensing，CS)可以提供一种更好的解决方案。

CS域的RDH已得到广泛研究[15-23]。Sheikh和Baraniuk[15]提出图像变换域中的数据嵌入方案，该方案首先对图像进行离散余弦变换(Discrete Cosine Transform，DCT)和硬阈值处理，通过将隐藏数据散布到稀疏系数上来嵌入隐藏数据，再DCT逆变换得到载密图像；在解码部分，使用L_1范数最小化和线性解码联合解码稀疏DCT系数和嵌入数据。随后，Zhang等人[16]提出具有灵活自恢复质量的新型水印方案，该方案利用载体图像的原始DCT系数生成用于内容恢复的嵌入水印数据，当部分水印图像被篡改时，可以提取未被修改的区域中的水印数据，并利用CS技术和变换系数稀疏性帮助图像恢复，但这种DCT域的系数稀疏表示有限，不能为数据隐藏提供合适条件。为使信号与水印具有更适合的稀疏表示，Hua等人[17]构建了适合数据隐藏的过完备字典，提高了信号与水印的稀疏性，并将水印嵌入稀疏信号中以实现用于图像的数据隐藏。文献[18-19]又提出两种过完备字典的改进扩频水印系统，并对其进行理论分析，证明了其安全性。然而，上述方法均为在压缩前对载体图像进行数据隐藏，在一些场景中，希望将数据嵌入到压缩后的测量值中。例如，在无线生理传感器网络WBSN应用程序中，可能需要在压缩数据中嵌入患者信息。

Yamaç等人[20]提出一种在CS信号中线性嵌入和隐藏数据的方案，该方案将附加信息直接嵌入到CS测量值中，并使用紧缩方法非线性重建压缩信号，实现了压缩后的数据隐藏。但该方案是条件可逆数据隐藏，其精确恢复取决于调制矩阵的受限等距常数。基于水印嵌入的方法能为CS数据隐藏提供较好的恢复精度。Wang等人[21]设计了一种具有身份认证的多数据CS隐私保护方案，该方案通过水印嵌入的方式在测量值中嵌入数据，半授权用户只能使用测量值，而完全授权用户可使用水印嵌入矩阵精确提取隐藏在测量值中的数据，实现了身份认证保护。这种方法虽然提取嵌入数据的精度较高，但需要额外的辅助矩阵，存储和传输这些矩阵时需要额外资源。Xiao等人[22]利用CS逐渐恢复特性，提出一种大容量数据隐藏方案，该方案对原始图像进行CS预测以创建备用空间，将图像加密后发送到数据隐藏器，数据隐藏器将秘密数据嵌入到相应位置的最高有效位(Most Significant Bit，MSB)中，实现数据隐藏的同时无需额外的辅助信息。但该方案重建需要将测量值和秘密信息分离，因此测量值无直接可用性且无法实现盲提取。

直方图平移(Histogram Shifting，HS)是一种可实现盲提取的信息隐藏技术，由于其能无损还原载体图像，已经得到广泛应用[5]。Wang等人[23]提出一种基于CS的联合选择性加密和数据隐藏方案，该方案使用语义安全流密码，在量化阶段选择性地加密CS测量的符号位，并使用基于直方图位移的数据隐藏方案插入身份验证信息，可实现测量值直接可用。但直接在CS域进行信息隐藏嵌入存在嵌入率较小的问题，如图1(b)所示，CS域的直方图趋近于正态分布，不能为数据隐藏提供高容量嵌入空间。

预测误差扩展(Prediction Error Expansion，PEE)[24]能更好地利用图像冗余生成预测误差直方图(Prediction Error Histogram，PEH)，其分布更加尖锐，因此在数据嵌入中具有更卓越的性能。目前常见的预测方法有菱形预测器[25]和中值预测器[26]，但由于CS测量值之间的相关性较弱，现有预测器在CS域中并不能取得理想的预测效果，未能得到理想的尖锐分布预测误差直方图。如图1所示，测量值直方图峰值与菱形预测器和中值预测器的直方图峰值差异较小，因此其嵌入性能较差。

基于上述分析，现有预测方法在CS域中难以有效应用，如何设计一种精确预测方法以提升直方图平移数据隐藏的嵌入性能，成为亟待解决的问题。为此，本文结合CS渐进恢复特性和PEE技术，提出一种基于多层循环预测的盲提取的可逆数据隐藏方案，该方案能确保数据盲提取和测量值的直接可用性，其主要贡献如下：

(1) 提出一种基于多层循环预测的盲提取的可逆数据隐藏方案，创新性地将PEE技术应用于CS域中数据嵌入，为CS域数据隐藏提供了新思路，并能保证数据盲提取和测量值的直接可用性。此外，还提出了新的嵌入模式，为不同权限用户提供多级

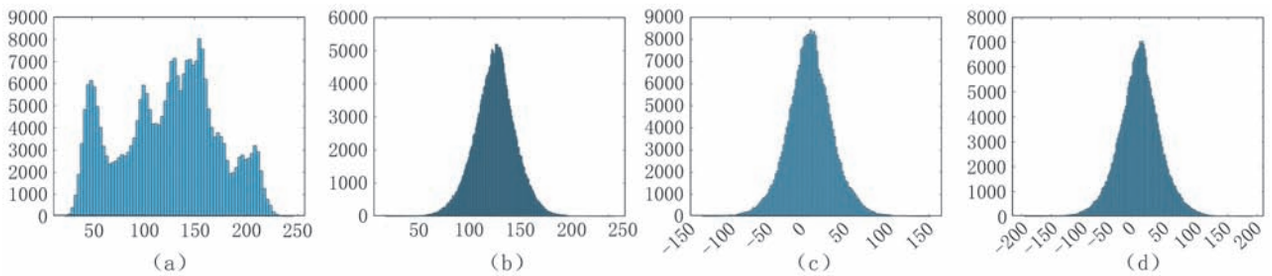

图1　依次为原始图像、测量值、测量值菱形预测和测量值中值预测直方图

预览功能的同时，还保证了秘密信息的隐蔽性。

(2) 提出一种循环预测方法，对测量值进行精确预测，生成尖锐分布预测误差直方图，从而有效提升PEE在CS域的嵌入容量；同时，还利用CS预测对冗余块进行估计，减小嵌入数据带来的图像质量下降，进一步提高测量值的可用性。

(3) 提出自嵌入和外嵌入两种嵌入方式，自嵌入结合缩略图保持加密，在测量值中嵌入图像本身的敏感区域保真值，以保证压缩图像的可用性与图像敏感区域安全性；外嵌入则通过CS循环预测，将秘密信息嵌入到测量值中，在不提取秘密信息的前提下，以提升载密图像的隐蔽性。

(4) 实验结果表明，本文在高容量嵌入的情况下，不仅确保了测量值的直接可用性与秘密信息的忙提取，还在视觉质量上优于现有的JPEG压缩域方案。

2　相关工作

2.1　压缩感知

CS自问世以来，在信号处理领域产生了巨大影响[27]。根据CS理论，只要信号在某些适当的域中是稀疏的或可压缩的，就可以得到比传统的Nyquist-Shannon采样少得多的测量值来对信号进行恢复[24]。具体来说，CS是将采样和压缩同步进行，可有效地降低计算成本。但在信号恢复过程中，其非线性的重建成本较昂贵，计算复杂度由采样端转移到重建端，因此CS在采样端资源受限的情况下格外适用。假设n维信号$\boldsymbol{X}=[x_1,x_2,\cdots,x_n]^T$如果存在某些基$\boldsymbol{\Psi}$使得$\boldsymbol{X}$稀疏：

$$\boldsymbol{X}=\boldsymbol{\Psi s} \tag{1}$$

其中，$\boldsymbol{s}$为稀疏信号，满足$\|\boldsymbol{s}\|_0=k$且$k<<n$，则称$\boldsymbol{X}$是k稀疏。假设$\boldsymbol{\Phi}$是一个大小为$m\times n(m\leqslant n)$的测量矩阵，其采样过程为

$$\boldsymbol{Y}=\boldsymbol{\Phi X}=\boldsymbol{\Phi\Psi s}=\boldsymbol{As} \tag{2}$$

其中，$\boldsymbol{Y}$为测量值，$\boldsymbol{A}=\boldsymbol{\Psi\Phi}$为采样矩阵。图像的恢复根据$\boldsymbol{y}$和$\boldsymbol{A}$重建$\boldsymbol{s}$，然而公式(2)是一个欠定线性方程组，当$rank(\boldsymbol{A})=m\leqslant n$时，可得到近似解$\hat{\boldsymbol{s}}=\boldsymbol{A}^T\left(\boldsymbol{AA}^T\right)^{-1}\boldsymbol{y}$，其重建误差为$\|\boldsymbol{s}-\hat{\boldsymbol{s}}\|_2=\boldsymbol{s}^T\left(\boldsymbol{I}-\boldsymbol{A}^T\left(\boldsymbol{AA}^T\right)^{-1}\boldsymbol{A}\right)\boldsymbol{s}$。因为$\boldsymbol{I}\neq\boldsymbol{A}^T\left(\boldsymbol{AA}^T\right)^{-1}\boldsymbol{A}$，所以实现精确重建并不可能。但因$\|\boldsymbol{s}\|_0=k$，可对添加约束，得到最稀疏解：

$$\min_{\boldsymbol{s}}\|\boldsymbol{s}\|_0,\ \text{s.t.}\ \boldsymbol{Y}-\boldsymbol{As}=0 \tag{3}$$

Donoho等人[28]表明，如果$m\geqslant 2k$，则公式(3)可以得到唯一解。但l_0范数最小化需要组合搜索，是一个NP难题。文献[29]中证明，若$\boldsymbol{A}$满足受限等距性质，则公式(3)的解有极大概率与其凸松弛形式的解相同：

$$\min_{\boldsymbol{s}}\|\boldsymbol{s}\|_1,\ \text{s.t.}\ \boldsymbol{Y}-\boldsymbol{As}=0 \tag{4}$$

可采用一些优化方法来求解[30-33]。

渐进恢复特性是CS的特性之一。具体地，从测量值$\boldsymbol{Y}$中任意取出t行，即$\boldsymbol{Y}_{\cdots t}=\left(y_1,y_2,\cdots,y_t\right)^T$，该值由该$t$行对应的测量矩阵$\boldsymbol{A}_{\cdots t}$采样得到：

$$\boldsymbol{Y}_{\cdots t}=\boldsymbol{A}_{\cdots t}\boldsymbol{s} \tag{5}$$

使用t行测量值对信号进行近似恢复：

$$\tilde{\boldsymbol{s}}=CS^{-1}(\boldsymbol{Y}_{\cdots t},\boldsymbol{A}_{\cdots t}) \tag{6}$$

其中，$\tilde{\boldsymbol{s}}$表示恢复信号，$CS^{-1}(\cdot)$为CS重建。

2.2　传统PEE

PEE具有比HS更优越的性能，因为其导出的预测误差直方图分布更加尖锐[5]。PEE充分利用相邻像素的相关性来获得有价值的可用空间，其像素与预测值之间的差异被扩展以用于数据嵌入，因此基于PEE的RDH方法通常有效权衡容量和失真。PEE嵌入过程包含三个步骤：

Step1：在特定的扫描排序下，将载体图像像素变成一维序列$[a_1,a_2,\cdots,a_N]$；然后，使用预测器对像素a_i进行预测，生成预测值$\tilde{a}_i$；可得预测误差为$e_i=a_i-\tilde{a}_i$；最后生成预测误差序列$[e_1,e_2,\cdots,e_N]$。

Step2：通过计算预测误差的频率来生成PEH. 即PEH定义为

$$h(k)=\#\{1\leqslant i\leqslant N: e_i=k\} \tag{7}$$

其中，#表示集合的基数。通常，PEH服从以0或接近0为中心的类拉普拉斯分布。PEH分布越尖锐，嵌入相同数量的比特时失真越小。

Step3：通过扩展和移位修改PEH来嵌入数据。具体来说，对于每个预测误差e_i，它被扩展或移位为

$$e_i'=\begin{cases}2e_i+b, & \text{if } e_i\in[-T, T)\\ e_i+T, & \text{if } e_i\in[T, +\infty)\\ e_i-T, & \text{if } e_i\in(-\infty, -T)\end{cases} \tag{8}$$

其中，T是与容量相关的整数值参数，$b\in\{0,1\}$是二进制嵌入数据。$[-T, T)$之间的预测误差被扩展成嵌入数据，而$[T, +\infty)$和$(-\infty, -T]$中的误差向外移动以创造空间。最后，将载体图像的每个像素修改为$x_i'=\tilde{x}_i+e_i'$，从而生成载密图像。PEE的最大嵌入容量EC为

$$EC=\sum_{k=-T}^{k=T}h(k) \tag{9}$$

2.3 缩略图保持加密

缩略图保持加密（Thumbnail Preserving Encryption，TPE）是一种能较好平衡图像可用性和安全性的隐私保护技术。Gregory[34]的研究表明，人们具有辨别以前浏览过图像的退化版本的能力，也就是说可以辨别出以前看过图像的模糊版本。Wright等人[35]首次提出一种基于先验知识的新图像加密概念，即缩略图保持加密，经缩略图保持加密后的图像保留了大于缩略图块的特征，并且擦除了包含许多敏感细节特征，实现了图像的隐私性和可用性之间的平衡，但该方法已被证实无法抵御统计攻击。Marohn等人[36]提出了两种近似的TPE方案，即动态范围保持加密（Dynamic Range Preserving Encryption，DRPE）和最低有效位TPE。作者声称这两种方案都是安全的，然而，这两种方案生成的密文图像缩略图质量较差，与原始图像缩略图相差较大。此外，利用DRPE生成的密文图像存在解密失败的情况，而采用最低有效位TPE生成的解密图像噪声点过多。为此，Zhang等人[37]提出一种高保真的TPE方案（High-Fidelity TPE，HF-TPE），该方案实现了更高的缩略图感知质量，并且在一定噪声下也能成功解密。

3 本文方案

本文提出的面向压缩域数据盲提取的多层循环预测可逆隐藏方案，如图2所示，包括采样端、嵌入端、接收端三个部分，其过程如下：

（1）采样端：采样端负责图像信号的采样与量化，并将压缩的图像信号传递给嵌入端。

（2）嵌入端：嵌入端分为自嵌入和外嵌入。在自嵌入模式时，嵌入端在接收到信号后，首先重建图像，再对图像敏感区域进行TPE操作，最后通过循环预测嵌入技术将压缩信号与保真信息结合以实现数据隐藏。在外嵌入模式时，将秘密信息进行二进制转换后通过循环预测嵌入技术进行信息嵌入。

（3）接收端：接收端对不同授权用户提供不同操作。对未授权用户，只能重建已模糊敏感区域的图像或只能重建原始图像但无法获取秘密信息；对于全授权用户，通过循环预测提取、重建和解密操作得到重建图像和秘密信息。

由于自嵌入过程包含外嵌入部分流程，因此本章节主要对自嵌入进行详细描述。本文涉及到的主要符号及其含义如表1所示。

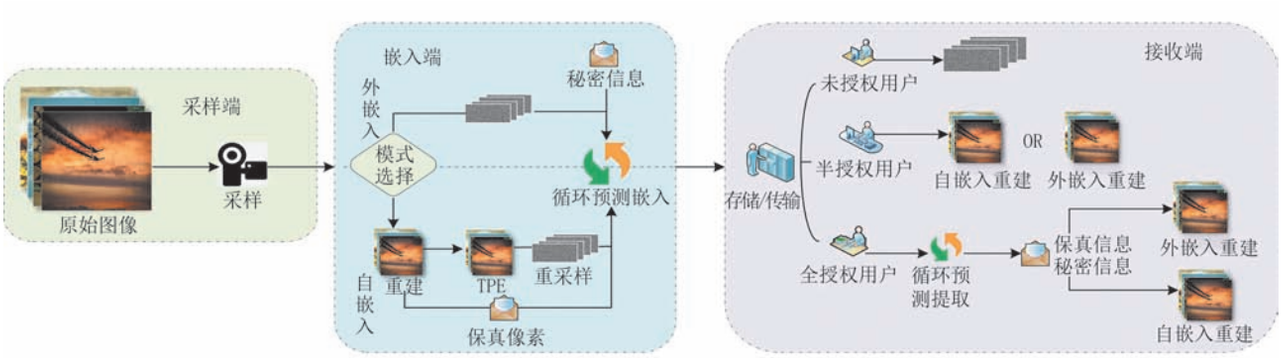

图2 本文提出的多层循环预测RDH方案

表1　主要符号及含义

符号	含义	符号	含义
$\boldsymbol{I}$	原图	$Enc(\cdot)$	HF-TPE加密算法
CR	采样率	K_2	HF-TPE加密秘钥
K_1	高斯采样矩阵生成秘钥	$\tilde{\boldsymbol{X}}_{Enc\Delta}$	HF-TPE加密后的$\tilde{X}_{\Delta}$
$\boldsymbol{X}$	分块矢量化后的原图	R	$\tilde{X}_{\Delta}$的保真信息
$\boldsymbol{A}$	高斯采样矩阵	$\tilde{\boldsymbol{Y}}$	加密测量值
$divide(\cdot)$	分块操作	$\boldsymbol{E}$	预测误差
$vec(\cdot)$	矢量化操作	Q	初始块序列号
$\boldsymbol{Y}$	测量值	$\tilde{Q}$	排序后的序列号
$\tilde{\boldsymbol{X}}$	Y对应重建图像	B	预测零误差块集合
$CS^{-1}(\cdot)$	CS重建算法	$\hat{\boldsymbol{E}}$	块排序后误差
$round(\cdot)$	取整操作	$\boldsymbol{Z}$	各块预测零误差统计集合
$\tilde{\boldsymbol{X}}_{Enc}$	HE-TPE加密后的图像	P	B中对应块MSE集合
$\tilde{\boldsymbol{X}}_{\Delta}$	$\tilde{X}$中ROI区域	$PEE(\cdot)$	预测误差拓展嵌入操作
$\tilde{\boldsymbol{X}}_{\Delta}^{c}$	$\tilde{X}$中非ROI区域	$\hat{\boldsymbol{E}}^{mark}$	嵌入信息后的$\hat{E}$
$\tilde{\boldsymbol{Y}}^{p}$	预测测量值	$\hat{\boldsymbol{Y}}$	嵌入秘密信息后的$\tilde{Y}$
$\tilde{\boldsymbol{X}}_{Enc}$	$\hat{Y}$对应重建图像	$Dec(\cdot)$	HF-TPE解密算法
$\hat{\boldsymbol{X}}_{final\Delta}$	最终还原ROI图像	$\hat{\boldsymbol{X}}_{final}$	最终重建图像

3.1　采样端

假设原始图像$\boldsymbol{I}$的尺寸为$N\times N$，通过采样矩阵对其采样，采样率为CR。若直接对$\boldsymbol{I}$进行采样，采样矩阵的大小为$R^{N^2\times N^2\times CR}$，则采样矩阵的生成和储存会占用较大内存空间。基于块的CS能够极大减小内存空间，并取得较好效果[38-39]，因此，本文采取块采样方法进行采样。

首先将$\boldsymbol{I}$分为m个大小为$n\times n(n<<N)$的非重叠子块并对其矢量化，再通过秘钥K_1生成高斯采样矩阵$\boldsymbol{A}\in R^{n^2\times n^2\times CR}$，最后进行采样，其操作为

$$\boldsymbol{X}=[x_1,x_2,\cdots,x_m]=vec\left(divide(I)\right) \tag{10}$$

其中，x_i表示第$i(1\leqslant i\leqslant m)$块，$divide(\cdot)$为分块操作，$vec(\cdot)$为矢量化操作。分块后对矢量化像素块进行采样：

$$\boldsymbol{Y}=[y_1,y_2,\cdots,y_m]=\boldsymbol{AX} \tag{11}$$

其中，$y_i\in R^{m^2}$为第i块的测量值。

3.2　嵌入端

3.2.1　HF-TPE保持加密与保真值处理

图像隐私保护需要在考虑安全性的同时尽可能提高可用性[40]，CS作为一种轻量级隐私保护技术也应该权衡两者之间的关系。Yamac等人[41]于2021年提出基于CS多级隐私保护方案，通过对敏感区域混淆再结合水印嵌入以实现敏感区域的保护。为提升效率，Suo等人[40]提出可用于物联网场景的类似方案。尽管上述两种方案有效地保护了敏感区域，但其敏感区域是以类噪声形式呈现，对具有图像先验知识的用户来说，这些方案缺乏可用性。为此，Zhang等人[37]提出了高保真缩略图保持加密方案，很好地权衡了图像的安全性和可用性，并且对噪声具有一定的鲁棒性。而CS重建算法是一种近似估计，与真实图像的差异也是一种噪声，HF-TPE可以和CS有效结合。

因此本文结合HF-TPE，实现多级隐私保护。具体地，测量值$\boldsymbol{Y}$在采样端通过CS重建算法还原为重建图像$\tilde{\boldsymbol{X}}$：

$$\tilde{\boldsymbol{X}}=round\left(CS^{-1}(\boldsymbol{Y},\boldsymbol{A})\right) \tag{12}$$

其中，$CS^{-1}(\cdot)$表示CS重建算法，$round(\cdot)$为取整操作。

在有隐私保护需求时，$\tilde{\boldsymbol{X}}$一般包含感兴趣区域(Region-Of-Interest，ROI)区域和非ROI区域。实际应用场景中，可通过自动识别算法来检测ROI边界。将$\tilde{\boldsymbol{X}}$中ROI索引集合表示为Δ，ROI区域为$\tilde{\boldsymbol{X}}_{\Delta}$，非ROI区域为$\tilde{\boldsymbol{X}}_{\Delta}^{c}$。接着，利用HF-TPE对$\tilde{\boldsymbol{X}}_{\Delta}$进行加密：

$$\tilde{\boldsymbol{X}}_{Enc}=\tilde{\boldsymbol{X}}_{\Delta}^{c}+Enc\left(\tilde{\boldsymbol{X}}_{\Delta},K_2\right)=\tilde{\boldsymbol{X}}_{\Delta}^{c}+\tilde{\boldsymbol{X}}_{Enc\Delta} \tag{13}$$

其中，$\tilde{\boldsymbol{X}}_{Enc}$表示加密后的图像，$Enc(\cdot)$为HF-TPE加密，$K_2$为加密秘钥，$\tilde{\boldsymbol{X}}_{Enc\Delta}$为HF-TPE加密后的ROI图像。最后，利用公式(10)对$\tilde{\boldsymbol{X}}_{Enc}$再采样得到加密测量值$\tilde{\boldsymbol{Y}}$。值得注意的是，尽管HF-TPE具有一定

鲁棒性，但在采样率较低时，其鲁棒性被破坏，敏感区域无法达到理想恢复效果，影响视觉体验。基于此，本文提取敏感区域保真值以保证重建敏感区域质量，具体操作如下：

$$\boldsymbol{R}_i=\left(\tilde{X}_{\Delta}>>i\right)\&1 \tag{14}$$

其中，$\boldsymbol{R}_i$表示$\tilde{\boldsymbol{X}}_{\Delta}$的第$i$个像素比特保真值，>>为右移运算符，&为按位与运算符。外嵌入不进行保持加密，直接通过3.4节操作将秘密信息嵌入测量值中。

3.2.2 循环预测与信息嵌入

循环预测与信息嵌入是利用CS渐进恢复特性，在对测量值进行预测的同时循环嵌入信息，以提高嵌入容量。如图3所示，循环预测与循环预测提取需经过分层、预测、块排序等步骤。本节将对各步骤进行详细说明。

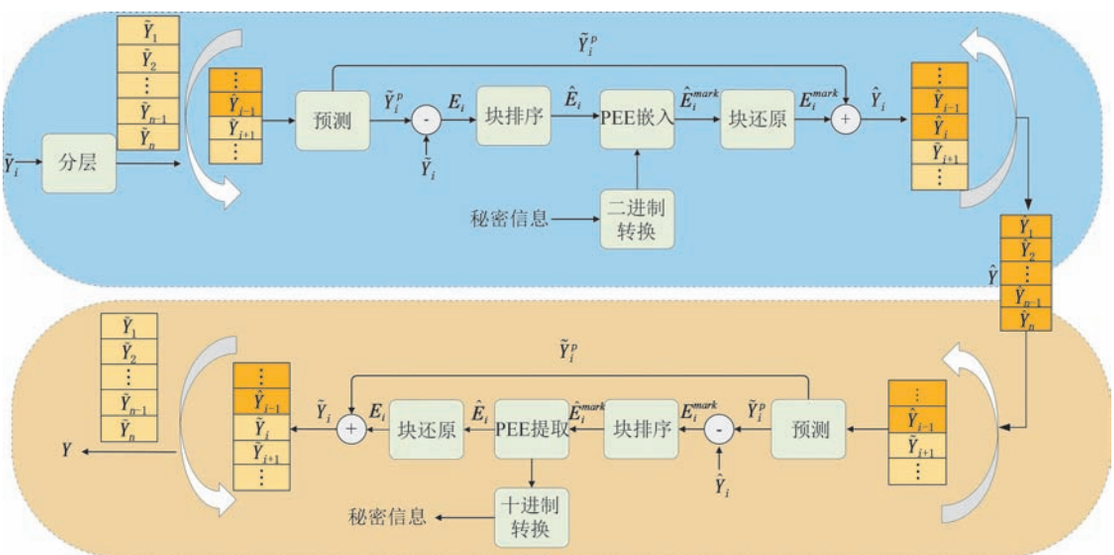

图3 循环预测嵌入与循环预测提取

（1）分层

分层是为后续测量值预测做准备，通过利用$n-1$层测量值预测第n层测量值。如图4所示，以4×4的测量值为例，将测量值$\tilde{\boldsymbol{Y}}$按行分为四层（实际中是多行为一层），测量矩阵$\boldsymbol{A}$采取同样操作。将$\tilde{\boldsymbol{Y}}$和$\boldsymbol{A}$分为l层：

$$\tilde{\boldsymbol{Y}}=\left(\tilde{\boldsymbol{Y}}_1,\tilde{\boldsymbol{Y}}_2\cdots\tilde{\boldsymbol{Y}}_i,\cdots,\tilde{\boldsymbol{Y}}_l\right)^T \tag{15}$$

$$\boldsymbol{A}=\left(\boldsymbol{A}_1,\boldsymbol{A}_2\cdots\boldsymbol{A}_i,\cdots,\boldsymbol{A}_l\right)^T \tag{16}$$

其中$\tilde{\boldsymbol{Y}}_i$表示第i层测量值，$\boldsymbol{A}_i$表示第i层测量矩阵，T为转置运算。

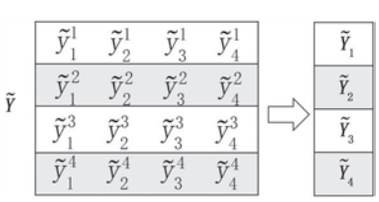

图4 测量值分层

（2）预测

通过2.1节中的CS渐进恢复特性对测量值进行分层预测，预测结果的精确性决定PEE嵌入容量。假设对第i层测量值$\tilde{\boldsymbol{Y}}$进行预测，则前$i-1$层已嵌入秘密信息，表示为$\tilde{\boldsymbol{Y}}_{1;\,i-1}^{mark}$，后$l-i$层表示为$\tilde{\boldsymbol{Y}}_{i+1;\,l}$，除去第$i$层的集合为$\tilde{\boldsymbol{Y}}_{exc(i)}=\left(\tilde{\boldsymbol{Y}}_{1;\,i-1}^{mark},\tilde{\boldsymbol{Y}}_{i+1;\,l}\right)^T$，除去第$i$层的测量矩阵为$\boldsymbol{A}_{exc(i)}=\left(\boldsymbol{A}_{1;\,i-1},\boldsymbol{A}_{i+1;\,l}\right)^T$。利用$\tilde{\boldsymbol{Y}}_{exc(i)}$和$\boldsymbol{A}_{exc(i)}$进行CS重建：

$$\tilde{\boldsymbol{X}}_{exc(i)}=CS^{-1}\left(\tilde{\boldsymbol{Y}}_{exc(i)},\boldsymbol{A}_{exc(i)}\right) \tag{17}$$

其中，$\tilde{\boldsymbol{X}}_{exc(i)}$为使用除$i$层测量值重建结果。再通过二次采样对$\tilde{\boldsymbol{Y}}_i$进行预测：

$$\tilde{\boldsymbol{Y}}_i^p=\boldsymbol{A}_i\tilde{\boldsymbol{X}}_{exc(i)} \tag{18}$$

其中，$\tilde{\boldsymbol{Y}}_i^p$表示$\tilde{\boldsymbol{Y}}_i$的预测值。利用$\tilde{\boldsymbol{Y}}_i$和$\tilde{\boldsymbol{Y}}_i^p$作差得到预测误差$E_i$。

（3）块排序

在本文中，将数据嵌入过程中可嵌入数据的测量值称为“可嵌入测量值”，将可嵌入测量值以外的值称为“不可嵌入测量值”。为尽可能减小嵌入失真，需估计每个测量值所在块的平滑度，优先在平滑度较高的块中嵌入数据。CS具有可以利用部分测量值预测其余测量值的特性，预测的误差集中在

像素变化尖锐区域，也就是非平滑区域。受此启发，本文利用CS预测特性对图像块进行平滑度估计。

首次预测测量值$\tilde{\boldsymbol{Y}}_1^p$与原测量值$\tilde{\boldsymbol{Y}}_1$作差生成第一层预测误差$\boldsymbol{E}_1=(e_1^1,e_1^2,\cdots,e_1^m)$。对$E_1$中的零值预测误差进行统计：

$$z_i=\#\{e_1^i\in\boldsymbol{E}_1:e_1^i==0\} \tag{19}$$

$$\boldsymbol{Z}=(z_1,z_2,\cdots,z_m) \tag{20}$$

其中，z_i表示第i块预测误差e_1^i中的零值预测误差个数。得到每个块的零预测数量后，以Z为参考对预测误差$\boldsymbol{E}_1$进行从大到小排序：

$$(\tilde{Q},\tilde{\boldsymbol{E}}_1)=sort(Q,\boldsymbol{Z},\boldsymbol{E}_1)=(\tilde{e}_1^1,\tilde{e}_1^2,\cdots,\tilde{e}_1^m) \tag{21}$$

其中$\tilde{\boldsymbol{E}}_1=(\tilde{e}_1^1,\tilde{e}_1^2,\cdots,\tilde{e}_1^m)$表示排序后的预测误差，$Q$为初始块序列号，$\tilde{Q}$为排序后的序列号，在后续用于恢复初始排序。但仅根据零误差个数进行平滑度估计可能会出现错误。如图5所示，采样率为0.5，层数为4，块数为256时，对第一层的预测零误差频数统计。可以观察到，四幅测试图像的最大零误差频数都超过10，最高可达16块，因此有必要对相同数量的零误差块进行再排序。均方误差(Mean Squared Error，MSE)是一种常用的衡量预测值与真实测量值之间差异的指标，本文使用MSE对具有相同预测零误差块进行再排序。将具有i个相同预测零误差块的集合表示为：$B_i=\{\tilde{e}_1^i\in\tilde{\boldsymbol{E}}_1:z_i==i\}$，$\tilde{\boldsymbol{E}}_1=(B_{\max},\cdots,B_i,\cdots,B_{\min})$。其中，$B_{\max}$和$B_{\min}$分别表示具有最大和最小数量的预测零误差块的集合。对于图5中的Goldhill，$\#\{B_{\max}\}=\#\{B_{73}\}=4$对应Goldhill图像最右侧中具有73个零预测误差的块数为4块；而$\#\{B_{\min}\}=\#\{B_{13}\}=1$，对应Goldhill图像最左侧中具有13个零预测误差的块数为1块。对块数大于等于2的集合，计算其中每个块的MSE：

$$P_i=\{\tilde{e}_1^i\in B_i:MSE(e_j),\ 1\leqslant j\leqslant k\} \tag{22}$$

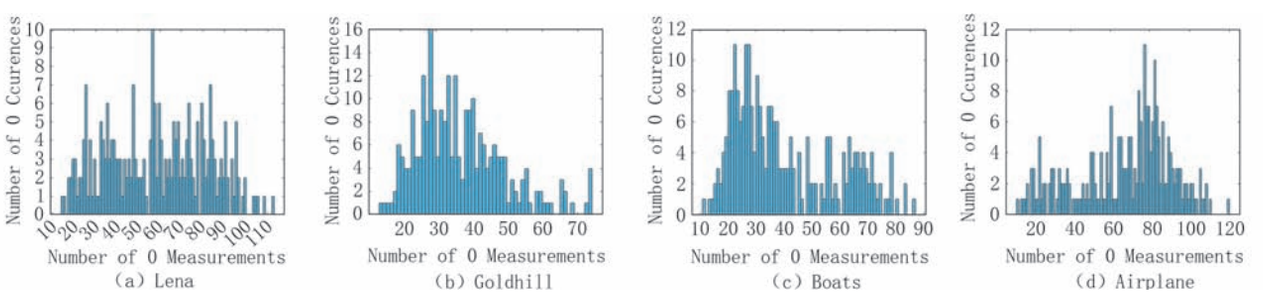

图5　预测零误差块数量统计直方图

其中，P_i表示B_i对应每个块的MSE的集合，$k=\#\{B_i\}$为集合B_i内的块个数，$P=(P_{\max},\cdots,P_i,\cdots,P_{\min})$。以$P$为参考，对$B_i$集合进行排序：

$$(\hat{Q}_i,\hat{B}_i)=sort(\tilde{Q}_i,P_i,B_i) \tag{23}$$

其中，$\tilde{Q}_i$为第i个集合对应的序列号，$\hat{Q}_i$为$\tilde{Q}_i$排序后的序列号，$\hat{B}_i$为排序后的B_i，得到排列预测误差$\hat{\boldsymbol{E}}_1=(\hat{B}_{\max},\cdots,\hat{B}_i,\cdots,\hat{B}_{\min})$。块还原为块排序还原初始顺序操作。其算法如下：

算法1.　块排序算法

输入：第一层预测误差$\boldsymbol{E}_1$

输出：排序后序列号$\hat{Q}$

1. 排序后第一层预测误差$\hat{\boldsymbol{E}}_1$
2. 统计E_1中各列0值个数生成$\boldsymbol{Z}$
3. 以Z为参考，根据0的数量对$\boldsymbol{E}_1$从大到小排序生成$\tilde{\boldsymbol{E}}_1$与$\tilde{Q}$
4. 将0数量相同的列归为一个集合，生成B。
5. FOR i=1 to m
6. 计算B_i集合中各列的MSE，生成P_i
7. 以P_i为参考，根据各列MSE对B_i从小到大排序，生成$\tilde{B}_i$和$\hat{Q}$
8. END FOR

(4) PEE嵌入

在本节利用预测误差直方图位移方法在测量值中嵌入秘密信息，秘密信息$\boldsymbol{W}$由保真值R和从最后几行测量值的最低有效位(Least Significant Bit，LSB)像素(为辅助信息嵌入预留空间)组成。在进行PEE嵌入前，首先将秘密信息$\boldsymbol{W}$平均分为l份，表示为$\boldsymbol{W}=(w_1,w_2,\cdots,w_l)$，再通过公式(8)在预测误差$\hat{\boldsymbol{E}}_i$中嵌入$w_i$：

$$\hat{\boldsymbol{E}}_i^{mark}=PEE(T,\hat{\boldsymbol{E}}_i,w_i) \tag{24}$$

其中，$\hat{\boldsymbol{E}}_i^{mark}$为嵌入秘密信息后的第$i$层预测误差，$PEE(\cdot)$为预测误差拓展嵌入操作。

(5) 块还原

直接将$\hat{\boldsymbol{E}}_i^{mark}$与$\tilde{\boldsymbol{Y}}_i^p$作和可能导致重建图像质量

较低，因此需要将$\hat{\boldsymbol{E}}_i^{mark}$还原，以减轻图像失真率：

$$\boldsymbol{E}_i^{mark}=sort^{-1}(\hat{\boldsymbol{Q}},\hat{\boldsymbol{E}}_i^{mark}) \tag{25}$$

其中，$\boldsymbol{E}_i^{mark}$表示还原后的$\hat{\boldsymbol{E}}_i^{mark}$，$sort^{-1}(\cdot)$为根据$\hat{\boldsymbol{Q}}$进行初始序列排序操作。最后将$\boldsymbol{E}_i^{mark}$与$\tilde{\boldsymbol{Y}}_i^p$相加得第$i$层嵌入秘密信息的测量值$\hat{\boldsymbol{Y}}_i$。

对上述过程进行i次循环后，将辅助信息嵌入最后两列测量值的最低有效位中。最后将测量值传输至接收端。循环预测与嵌入如算法2所示：

算法2. 循环预测与嵌入

输入：加密后的测量值$\tilde{\boldsymbol{Y}}$

测量矩阵$\boldsymbol{A}$

输出：嵌入秘密信息后的测量值$\hat{\boldsymbol{Y}}$

1. 排序后序列号$\hat{\boldsymbol{Q}}$
2. 秘密信息二进制转换，并分为l份
3. 对$\tilde{\boldsymbol{Y}}$和$\boldsymbol{A}$进行分层
4. FOR i=1 to l
5. 预测生成第i层预测测量值$\tilde{\boldsymbol{Y}}_i^p$
6. $\tilde{\boldsymbol{Y}}_i$与$\tilde{\boldsymbol{Y}}_i^p$作差生成预测误差$\boldsymbol{E}_i$
7. IF i==1
8. 块排序后生成序列号$\hat{\boldsymbol{Q}}$与预测误差$\hat{\boldsymbol{E}}_1$
9. ELSE
10. 根据$\hat{\boldsymbol{Q}}$对E_i进行排序生成$\hat{\boldsymbol{E}}_i$
11. END IF
12. PEE嵌入生成$\hat{\boldsymbol{E}}_i^{mark}$
13. 根据$\hat{\boldsymbol{Q}}$进行块还原生成$\boldsymbol{E}_i^{mark}$
14. $\tilde{\boldsymbol{Y}}_i^p$与$\boldsymbol{E}_i^{mark}$作和生成$\hat{\boldsymbol{Y}}_i$
15. END FOR

3.3 接收端

在接收端，不同权限的用户在接收到载密测量值后可进行不同权限操作。其中，未授权用户得不到任何有用信息；半授权用户可恢复除敏感区域外的加密图像，且不会察觉到嵌入信息的存在；全授权用户可完全重建图像，并获取测量值中的隐藏秘密信息。

3.3.1 半授权用户

半授权用户在接收到载密测量值后，在指定区域的测量值中提取最低有效位的部分辅助信息转换为秘钥K_1和图像尺寸信息，再通过K_1和图像尺寸信息生成高斯采样矩阵$\boldsymbol{A}$，最后利用CS重建图像：

$$\check{\boldsymbol{X}}_{Enc}=CS^{-1}\left(\hat{\boldsymbol{Y}},\boldsymbol{A}\right) \tag{26}$$

其中，$\check{\boldsymbol{X}}_{Enc}$表示重建图像.

3.3.2 全授权用户

全授权用户对载密测量值可以进行秘密信息提取和图像还原操作。首先，从指定位置LSB处提取全部辅助信息，再根据辅助信息进行循环预测提取（循环预测嵌入反过程）秘密信息$\boldsymbol{W}$，将秘密信息中的原指定区域的LSB像素进行替换，恢复测量值$\tilde{\boldsymbol{Y}}$。与公式(26)类似，重建敏感区域为加密图像$\hat{\boldsymbol{X}}_{Enc}$，根据辅助信息定位$\hat{\boldsymbol{X}}_{Enc}$的加密敏感区域$\hat{\boldsymbol{X}}_{Enc\Delta}$，利用秘钥$K_2$对$\hat{\boldsymbol{X}}_{Enc\Delta}$进行解密：

$$\hat{\boldsymbol{X}}_{\Delta}=Dec\left(\hat{\boldsymbol{X}}_{Enc\Delta},K_2\right) \tag{27}$$

其中，$\hat{\boldsymbol{X}}_{\Delta}$表示解密后的敏感区域，$Dec(\cdot)$表示为HF-TPE解密操作。为提高敏感区域的视觉质量，再将提取出的保真信息R用于还原$\hat{\boldsymbol{X}}_{\Delta}$。假设对第$i$位比特进行还原，首先将$\hat{\boldsymbol{X}}_{\Delta}$像素第$i$位进行清除：

$$\hat{\boldsymbol{X}}_{\Delta}'=\hat{\boldsymbol{X}}_{\Delta}\&\left(\sim(1<<i)\right) \tag{28}$$

其中，$\hat{\boldsymbol{X}}_{\Delta}'$表示清除第$i$位比特后的结果，$\sim$表示按位取反运算符。接下来，将要嵌入的值$R_i$左移$i$位，并将其与$\hat{\boldsymbol{X}}_{\Delta}'$按位异或操作进行嵌入：

$$\hat{\boldsymbol{X}}_{final\Delta}=\hat{\boldsymbol{X}}_{\Delta}'|(R_i<<i) \tag{29}$$

其中，$\hat{\boldsymbol{X}}_{final\Delta}$为最终还原敏感区域图像，$|$为按位取反运算符。将$\hat{\boldsymbol{X}}_{final\Delta}$与$\hat{\boldsymbol{X}}_{\Delta}^c$结合得到最终还原图像$\hat{\boldsymbol{X}}_{final}$。

4 实 验

本文从4个方面全面评估对所提出方案性能，概述如下：

(1)参数选取：选择适合的参数能提高图像的视觉质量与嵌入效率。

(2)视觉效果：分析本文提出的自嵌入与外嵌入方案的视觉质量和块排序对视觉质量的提升。

(3)对比分析：通过与最新方案进行定量和定性分析，证明本文方案的优越性。

(4)时间复杂度：分析本文方案在不同层数下的时间复杂度，验证本文方案是否能满足实际应用。

4.1 实验设置

通过实验分析来展示本文提出的多层循环预测RDH方案的优越性。实验在i7-8700 CPU@3.2 GHz、16 GB RAM和Window 10平台的MATLAB 2021b上进行。对于自嵌入，本文从公开数据集DIV2K[42]选择8张具有敏感区域的图像作为测试图像，这些图像涉及人物、建筑、车牌等，将其尺寸设定为

512×512，类型转换为YCbCr格式。对于外嵌入，本文对数据集BSD68[43]进行实验，验证载密测量值的可用性与秘密信息的隐蔽性。

4.2　参数选取

4.2.1　层数选择

利用CS渐进恢复特性对部分测量值进行预测，理论上层数越大，其预测精度越高，恢复性能越好。但层数增加会多次调用CS算法，影响其时间效率；此外，其预测精度也受采样率和采样矩阵影响。因此，需要权衡时间效率和图像质量来选择合适的层数。本节对数据集BSD68的68张图像进行实验，固定嵌入数据量，以PSNR为指标，观察PSNR随层数变化。如图6所示，随着层数增加，各采样率下的PSNR呈现先递增，后趋于平稳或下降趋势，其PSNR峰值集中在3-5层。因此，层数选择为3-5为优，本文选取层数为4。

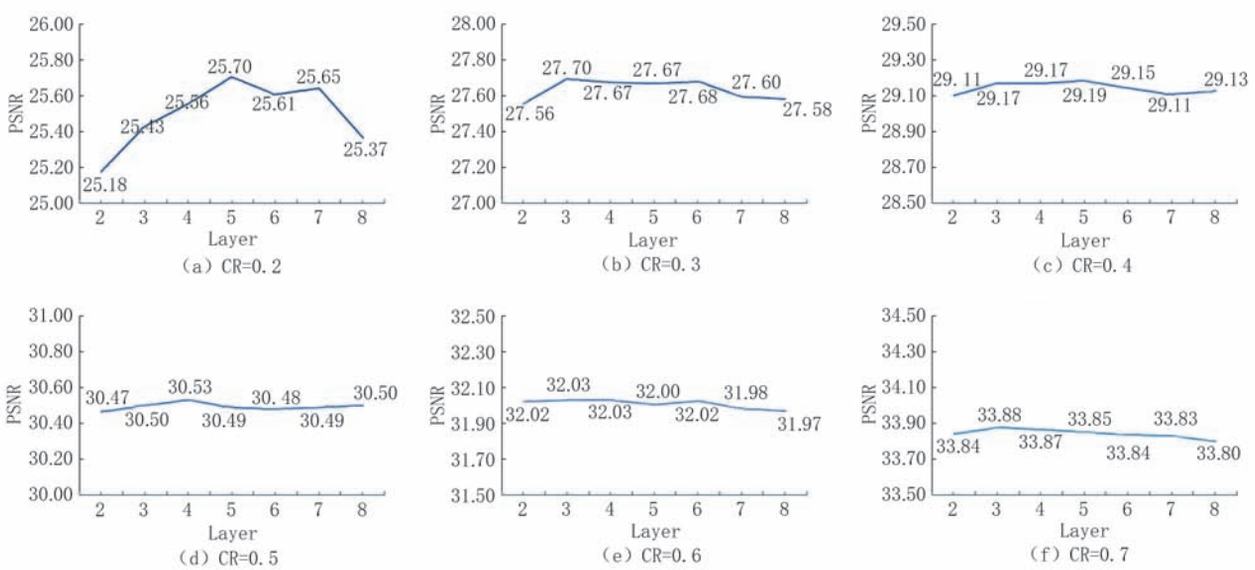

图6　在层数为2-8、嵌入容量为20 000 bit时，不同采样率下的平均PSNR

4.2.2　辅助信息

信息盲提取是在无额外信息或秘钥的条件下只利用图像自身信息进行信息提取。对本文而言，接收端在得到测量值后，需从测量值中提取辅助信息进行秘密信息提取以及图像的重建。为实现盲提取，本文在测量值的LSB中嵌入辅助信息。这些辅助信息由图像信息、量化信息、秘钥信息和CS循环预测嵌入信息组成：

(1)图像信息：图像尺寸N，占位9 bit。

(2)量化信息：原始测量值的最大值、最小值(−1000到1000之间)和映射区间，共占位28 bit。

(3)秘钥信息：高斯随机测量矩阵生成秘钥K_1，若为自嵌入，还需HF-TPE秘钥K_2和敏感区域坐标，共占位88 bit。

(4)CS循环预测嵌入信息：嵌入模式、与容量相关的参数T、层数、每层嵌入信息长度、和块排序序列号，共计2163 bit。

综上所述，辅助信息共计2288 bit，需从指定行或列的最低比特位提取2288 bit以嵌入辅助信息，嵌入秘密信息时需要将真实测量值最低比特一并嵌入。

4.3　视觉效果

4.3.1　自嵌入

自嵌入是为用户提供多级权限保护，即保证半授权用户能获取图像敏感区域外的信息，全授权用户获取图像全部信息。本节从数据集DIV2K中挑选8张具有敏感区域的图像，图7展示了初始采样率设为0.5、层数为4、总嵌入容量为30 000 bit时时自嵌入结果。其中敏感区域用红色方框标出并放大，如第一列所示；首先，原始图像经CS采样后，在嵌入端对图像进行重建，如第二列所示；然后，使用HF-TPE对图像敏感区域进行加密，如第三列所示；最后对加密后的图像重新采样，得到测量值，并对其进行CS循环预测嵌入秘密信息。对于半授权用户，可从载密测量值指定LSB区域中提取秘钥K_1生成采样矩阵，再通过CS重建算法重建图像。如第四列所示，半授权用户只能浏览重建图像的非敏感区域，而敏感区域以模糊的形式存在。对于全授

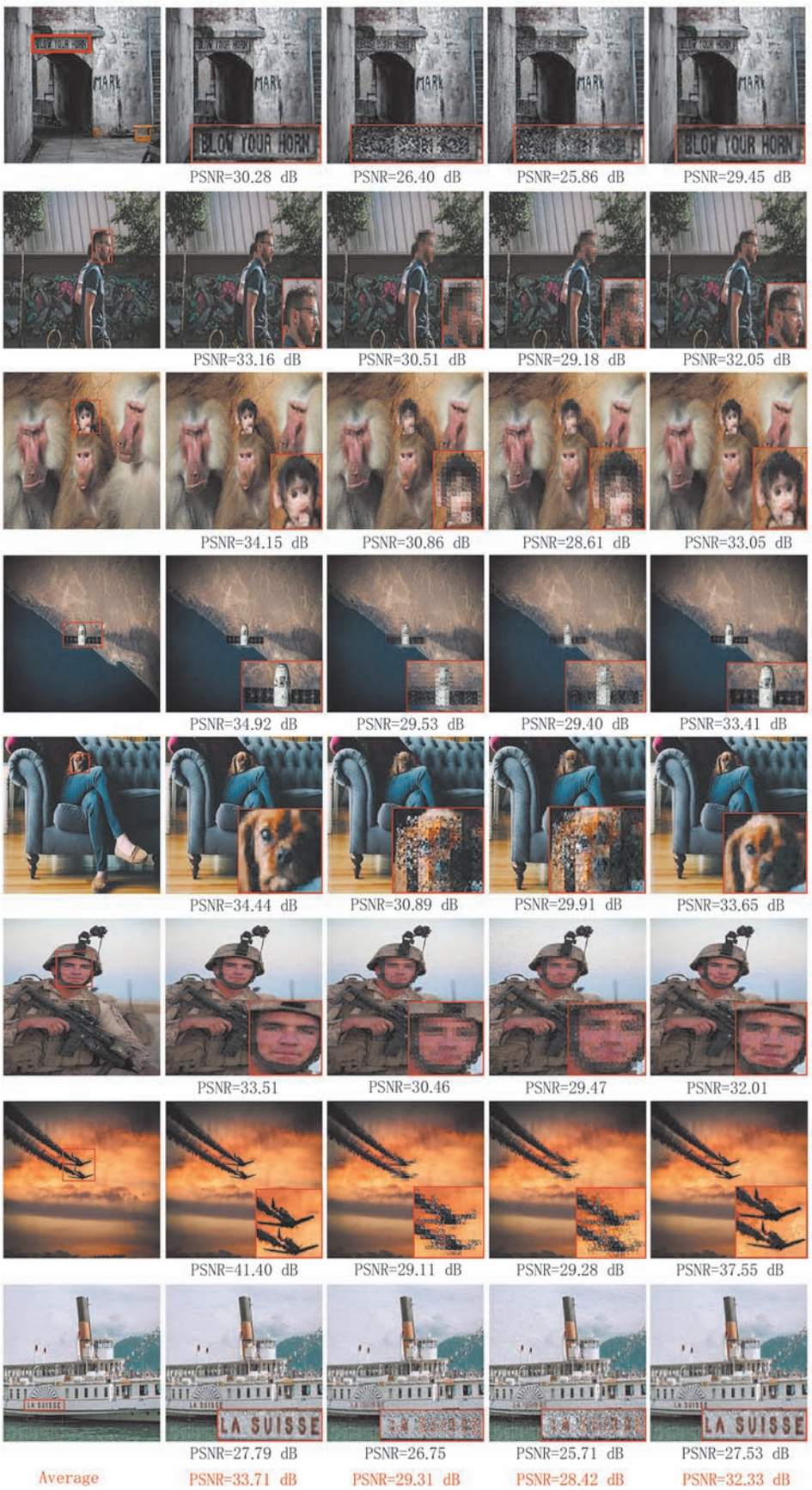

图7 采样率为0.5、层数为4、嵌入量为30 000 bit的时自嵌入结果(从左往右依次为:原始图像、CS重建图、HF-TPE加密图、直接CS重建图、CS完全重建图)

权用户，通过CS循环预测提取保真值，再重建完整图像，如第五列所示，全授权用户获取图像完整信息；此外图像视觉质量也未出现太大改变。本文以PSNR作为视觉质量评价指标，第二列中CS重建图与原图之间的平均PSNR为33.71 dB，第五列中保真值提取后CS完全重建图与原图之间的平均PSNR为32.33 dB，证明本文提出方案并未对图像视觉质量造成较大失真，不影响用户体验，能够满足不同权限用户需求。

4.3.2　外嵌入

外嵌入是为嵌入秘密信息，保证半授权用户在不提取秘密信息时直接使用载密测量值进行图像重建，实现测量值的直接可用性；而全授权用户能实现秘密信息提取和图像重建。本文选取层数为4，采样率为0.2～0.7，有效嵌入量为5000～50 000 bit（即5 k—50 k）时，在数据集BSD68上进行分析，如图10所示，随着嵌入容量提升，用载密测量值重建的图像与原图之间的PSNR逐渐下降，且采样率越低，其PSNR下降速度越快，因此其图像质量越差。

此外，验证本文外嵌方案在测量值中嵌入秘密信息不影响测量值的可用性。在BSD68中设定采样率为0.5、嵌入量为20 000 bit、层数为4时，对比每张测量值重建图像、载密测量值重建图像与原始图像PSNR，如图8所示。由于图像内容差异，各图像测量值重建质量有所不同，最好重建图像PSNR最好能达到40 dB以上，而最差重建图像质量低于25 dB。但是，测量值重建图和载密测量值重建图在图像质量方面趋势大致相同，并未出现较大差异。因此，载密测量值不影响实现图像重建，即本文提出的外嵌入方法能够保证载密测量值在不提取嵌入数据的前提下可直接重建图像，保证载密测量值的直接可用性。

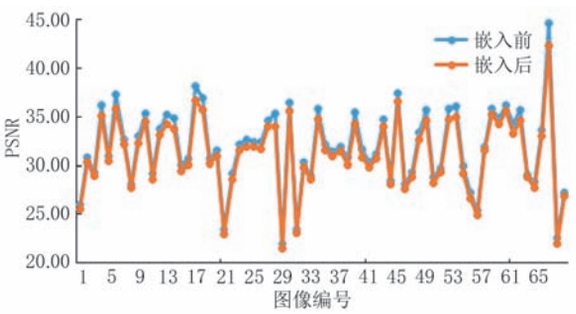

图8　采样率为0.5、层数为4、嵌入量为20 000 bit时，嵌入前、后测量值图像PNSR

此外，本文可实现边循环提取数据边重建图像功能。在循环提取时，由于真实测量值逐层恢复，其重建图像的视觉质量也随之提高，而未提取层的数据提取依赖于已经提取数据的测量值的重建图像，因此可为用户提供渐进浏览功能。在数据集BSD68上，有效嵌入容量为20 000 bit、采样率为0.5时，图像的视觉质量随数据的逐层提取而逐渐提升，PSNR如表2所示。

表2　数据集BSD68数据逐层提取重建图平均PSNR

层数	提取0层数据	提取1层数据	提取2层数据	提取3层数据	提取4层数据	提取5层数据	提取6层数据	提取7层数据	提取8层数据
2	30.475	30.904	30.095						
3	30.501	30.967	30.979	30.982					
4	30.532	31.003	31.005	31.013	31.042				
5	30.498	30.974	30.975	30.980	31.002	31.035			
6	30.492	30.971	30.974	30.979	30.991	31.012	31.043		
7	30.488	30.982	30.984	30.986	30.999	31.016	31.037	31.068	
8	30.504	30.995	30.993	30.997	31.004	31.018	31.036	31.062	31.090

4.3.3　块排序

块排序是为提高本文提出方案的视觉质量，提升载密测量值的可用性。本文在采样率为0.5、层数为4时，对数据集BSD68进行实验。如图9所示，随着有效嵌入比特数的提升，块排序前后载密测量值重建图与原图之间的平均PSNR不断下降；但经过块排序后（蓝线），其PSNR下降幅度明显低于块排序前（橙线），证明本文提出的块排序方法能较好抵御嵌入秘密信息导致的视觉质量下降。

4.4　对比分析

为体现本文提出方案具有盲提取和测量值直接可用的优越性，本文与基于CS隐藏方法[21-23]进行定性对比，如表3所示。Wang等人[21]通过水印嵌入的方法在CS测量值中嵌入二值水印，但需要会生成水印编码矩阵作为提取水印信息时的秘钥，不

图9 块排序前后平均图像PSNR变化

能实现盲提取；Xiao等人[22]利用CS预测的方法，在测量值的最高有效位中腾出空间用于信息嵌入，这种嵌入方法使得修改值与原值表现出较大差异，无法直接用于图像重建，因此其测量值缺少直接可用性，易暴露隐藏信息；Wang等人[23]通过在测量值中直接利用直方图平移方法进行信息嵌入，可用于用户身份验证，但由于测量值是轻量级加密，且满足正态分布，其峰值较小，而直方图平移数据隐藏容量取决于峰值，因此该方案数据隐藏的嵌入容量低，不足以满足大容量需求。而本文提出方案具有盲提取、不易察觉、多级权限以及具有直接可用性的优点。

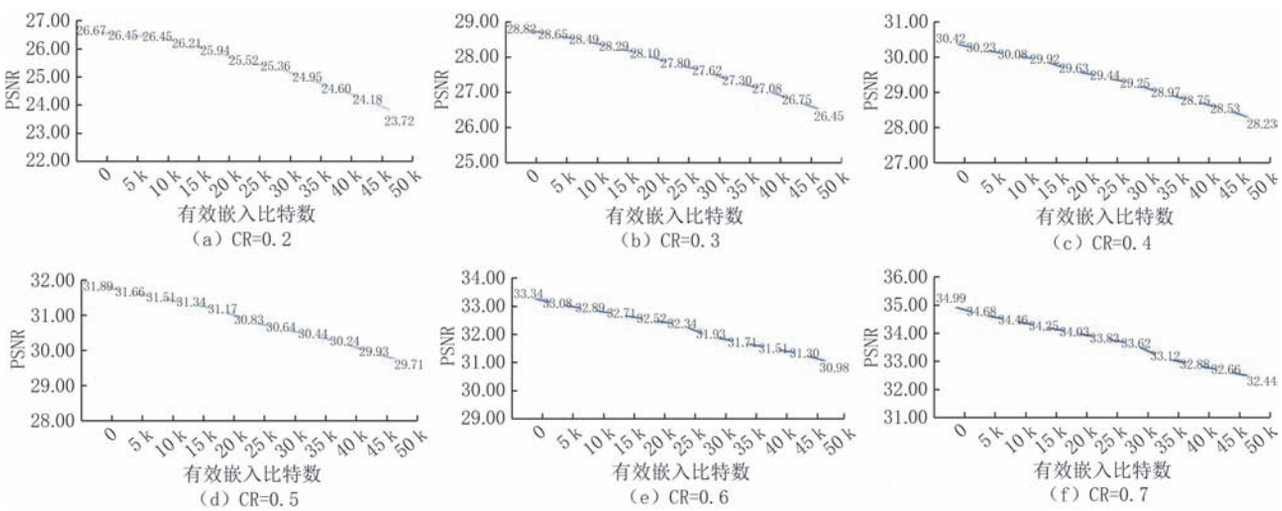

图10 在层数为4、嵌入容量为5 kbit-50 kbit时，不同采样率下的载密测量值重建图像平均PSNR

表3 与最新CS数据隐藏方案定性对比

方案	嵌入方法	测量值具有直接可用性	盲提取	秘密信息不易察觉	多级权限
Wang等[23]	直方图平移	√	×	√	√
Wang等[21]	水印	√	×	√	√
Xiao等[22]	MSB嵌入	×	×	×	√
本文	直方图平移	√	√	√	√

此外，CS域作为一种压缩域，也应与现有压缩域直方图数据隐藏进行比较。本文与最新的文献[6]和文献[9]进行比较，其中本文方法的循环层数设定为4层，由于压缩率与JPEG的QF因子未有直接换算关系，且每张图像在JPEG压缩后其文件大小也有差异。因此，本文在对图像数据集进行大量JPEG压缩实验后，得出压缩率和QF因子大致对应关系。例如QF因子95对应压缩率大致为0.7，QF因子90大致对应压缩率为0.5。如表4所示，文献[6]在低嵌入量时，其重建图像视觉质量表现出色，文件大小增量(File Size Increment，FSI)相对较小，但随着嵌入量增加，在数据集BSD68中，部分图像由于其内容不同，因此出现嵌入数据超过可嵌入容量问题；文献[9]在视觉质量和文件大小增量方面略逊于文献[6]，但其在数据集BSD68随着嵌入量的提升其嵌入失败率低于文献[6]，因此其在嵌入容量方面表现良好；本文方案利用CS进行预测，能实现大容量数据嵌入，且提前在量化步骤中为嵌入预留位移空间，文件大小不会发生改变。因此，与现有JPEG压缩域直方图数据隐藏相比，本文提出方案具有嵌入容量大和文件大小不变的优势。

4.5 安全性分析

本文基于CS的直方图循环预测数据隐藏框架的安全性源自两个方面。首先，由秘钥控制的随机

表4　在数据集BSD68上不同压缩率，不同嵌入量下图像平均PSNR和平均FSI

方案	指标	CR=0.7(QF=90) 有效嵌入比特数(bit)									
		10 000	12 500	15 000	17 500	20 000	22 500	25 000	27 500	30 000	32 500
文献[6]	PSNR	**48.97**	**47.26**	**45.04**	**43.09**	～	～	～	～	～	～
	FSI	11 172	15 017	17 687	20 002	～	～	～	～	～	～
文献[9]	PSNR	45.06	43.55	42.22	41.04	38.64	37.71	～	～	～	～
	FSI	13 854	17 998	22 449	26 774	30 178	34 162	～	～	～	～
Ours	PSNR	41.35	40.66	40.07	39.54	**39.06**	**38.05**	**37.36**	**36.97**	**36.61**	**36.26**
	FSI	0	0	0	0	0	0	0	0	0	0
方案	指标	CR=0.5(QF=95) 有效嵌入比特数(单位:bit)									
		10 000	12 500	15 000	17 500	20 000	22 500	25 000	27 500	30 000	32 500
文献[6]	PSNR	**52.74**	**51.07**	**49.65**	**48.39**	**46.6311**	**43.46**	～	～	～	～
	FSI	12 162	15 286	18 259	20 847	22 840	23 916	～	～	～	～
文献[9]	PSNR	48.44	46.95	45.68	44.56	43.58	42.70	**41.89**	**40.44**	37.68	～
	FSI	14 625	18 743	23 004	27 378	31 600	36 042	40 034	43 653	45 329	～
Ours	PSNR	43.32	42.61	42.00	41.47	40.97	40.53	40.13	39.75	**39.41**	**38.14**
	FSI	0	0	0	0	0	0	0	0	0	0

测量机制的CS技术确保了信号采集的计算安全性，秘钥控制HF-TPE技术保证敏感区域的安全性。其次，得益于CS重建算法的鲁棒性，使得嵌入秘密信息的测量值具有较强的隐蔽性。具体解释如下：

(1)CS技术可保证信号安全性。Candes等人[44]证明了具有随机分布的测量矩阵有很高的概率满足k阶RIP. Bianchi等人[45]证明，每次测量时使用高斯随机分布更新的测量矩阵可以实现CS的安全加密。对于本文方案，假设攻击者已知测量矩阵由秘钥K_1生成，则估计K_1则最多需要计算2^{32}次。此外，对于自嵌入，HF-TPE给敏感信息提供保护，敏感区域尺寸为$a\times b$，则估计敏感区域最大需要计算2^{8ab}次；假设攻击者已知HF-TPE由秘钥K_2控制生成，则估计K_2则最多需要计算2^{32}次。综上所述，攻击者只有在已知CS重建方法、秘钥K_1、秘钥K_2和HF-TPE解密方法的前提下才能正确重建图像，而这些条件几乎不可能同时满足，因此可以保证图像信息安全性。

(2)重建算法的鲁棒性保证本文秘密信息的隐蔽性。以图像Lena为例，比较采样率为0.5、层数为4、嵌入数据为20 000 bit时测量值直方图。如图11所示，测量值直方图(a)与载密测量值直方图(b)之间无明显差异，通过直方图分析无法判断是否嵌入信息。此外，在相同参数下对测量值重建图和载密测量值重建图的像素进行分析。如图12所示，随机选取测量值重建图与载密测量值重建图1000个像素，可以看出其像素值变化差异较小，甚至部分像素可紧密重合。因此，通过直方图和重建图分析无法判断测量值是否嵌入数据，保证了秘密信息的隐蔽性。

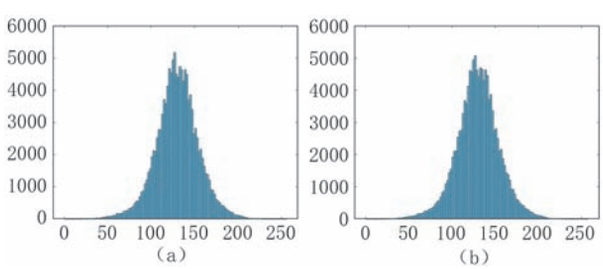

图11　测量值直方图与载密测量值直方图

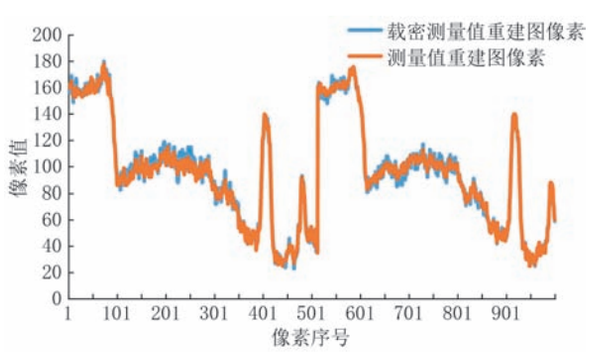

图12　测量值重建图与载密测量值重建图对比

值得说明的是，本文还通过比较原始图像、CS重建图、HF-TPE加密图、直接CS重建图、CS完全重建图的PSNR来展示利用CS重建算法的鲁棒性以保证秘密信息的隐蔽性，如图7所示。

4.6 时间复杂度分析

时间复杂度的长短对算法的实际应用较为关键，本文的时间复杂度主要为多次调用CS重建算法。表5列出了采样率为0.5、嵌入容量为20 000 bit时，测量BDS68数据集的平均时间复杂度。从表5中可以看出，本文的时间复杂度随层数增加而增加，但在4.1节中对层数进行分析后，选择3～5层为最优，也可根据需求调整。本文时间复杂度在3～11秒之间，并且可实现较高的嵌入容量，且无文件大小增量，因此其时间复杂度可以被接受。

表5 时间复杂度 (s)

层数	2	3	4	5	6	7	8
嵌入时间	3.82	5.63	6.85	7.75	8.55	9.78	10.82
提取时间	3.95	5.71	6.74	8.03	8.94	9.73	10.92

5 总 结

针对现有CS域可逆数据隐藏方案不能同时实现秘密信息盲提取和测量值的直接可用问题，本文提出面向压缩域数据盲提取的多层循环预测可逆隐藏方案。该方案利用CS渐进恢复特性，结合预测误差扩展，通过循环预测嵌入的方式对指定测量值进行预测生成预测误差，对误差块进行排序，并通过直方图平移向预测误差中嵌入数据，这种循环预测嵌入方法进一步提高了预测的精确性。此外，结合缩略图保持加密技术为用户提供多权限浏览功能，进一步为用户提供多权限隐私保护。结果表明，所提出的方法在嵌入性能方面优于最先进的压缩域图像可逆数据隐藏，为PEE在CS域中进行数据嵌入提供了新的思路。

参 考 文 献

[1] Tian J. Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896

[2] Ni Z, Shi Y Q, Ansari N, et al. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362

[3] Li Ji-Yu, Fu Zhang-Jie, Wang Fan. Canny-gauss universal domain image steganography algorithm. Chinese Journal of Computers, 2024, 47(1): 213-230 (in Chinese)
(李季瑀, 付章杰, 王帆. Canny-Gauss通用域图像隐写算法. 计算机学报, 2024, 47(1): 213-230)

[4] Sachnev V, Kim H J, Nam J, et al. Reversible watermarking algorithm using sorting and prediction. IEEE Transactions on Circuits and Systems for Video Technology, 2009, 19(7): 989-999

[5] Ou B, Li X, Zhao Y, et al. Pairwise prediction-error expansion for efficient reversible data hiding. IEEE Transactions on Image Processing, 2013, 22(12): 5010-5021

[6] Li F, Qi Z, Zhang X, et al. Progressive histogram modification for JPEG reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 34(2): 1241-1254

[7] Hu Y, Wang K, Lu Z M. An improved VLC-based lossless data hiding scheme for JPEG images. Journal of Systems and Software, 2013, 86(8): 2166-2173

[8] Xiao M, Li X, Ma B, et al. Efficient reversible data hiding for JPEG images with multiple histograms modification. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 31(7): 2535-2546

[9] Mao N, He H, Chen F, et al. Reversible data hiding of JPEG image based on adaptive frequency band length. IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(12): 7212-7223

[10] Wen W, Jiang Q, Huang H, Zhang Y, et al. TPE-DF: Thumbnail preserving encryption via dual-2DCS fusion. IEEE Signal Processing Letters, 2024, 31: 1039-1043

[11] Zhou J, Sun W, Dong L, et al. Secure reversible image data hiding over encrypted domain via key modulation. IEEE Transactions on Circuits and Systems for Video Technology, 2015, 26(3): 441-452

[12] Wang C, Wang X, Xia Z, et al. Image description with polar harmonic fourier moments. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 30(12): 4440-4452

[13] Weng S, Zhang C, Zhang T, et al. High capacity reversible data hiding in encrypted images using SIBRW and GCC. Journal of Visual Communication and Image Representation, 2021, 75: 102932

[14] Dai Qiong-Hai, Fu Chang-Jun, Ji Xiang-Yang. Research on compressed sensing. Chinese Journal of Computers, 2011, 34(3): 425-434 (in Chinese)
(戴琼海, 付长军, 季向阳. 压缩感知研究. 计算机学报, 2011, 34(3): 425-434)

[15] Sheikh M A, Baraniuk R G. Blind error-free detection of transform-domainwatermarks//Proceedings of the 2007 IEEE International Conference on Image Processing. San Antonio, USA, 2007, 5: V-453-V-456

[16] Zhang X, Qian Z, Ren Y, et al. Watermarking with flexible self-recovery quality based on compressive sensing and compositive reconstruction. IEEE Transactions on Information Forensics and Security, 2011, 6(4): 1223-1232

[17] Hua G, Xiang Y, Bi G. When compressive sensing meets data hiding. IEEE Signal Processing Letters, 2016, 23(4): 473-477

[18] Hua G, Zhao L, Zhang H, et al. Random matching pursuit for image watermarking. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 29(3): 625-639

[19] Hua G. Over-complete-dictionary-based improved spread spectrum watermarking security. IEEE Signal Processing

Letters, 2020, 27: 770-774

[20] Yamac M, Dikici Ç, Sankur B. Hiding data in compressive sensed measurements: A conditionally reversible data hiding scheme for compressively sensed measurements. Digital Signal Processing, 2016, 48: 188-200

[21] Wang M, Xiao D, Liang J, et al. Distributed privacy-preserving nested compressed sensing for multiclass data collection with identity authentication. Signal Processing, 2023, 204: 108823

[22] Xiao D, Li F, Wang M, et al. A novel high-capacity data hiding in encrypted images based on compressive sensing progressive recovery. IEEE Signal Processing Letters, 2020, 27: 296-300

[23] Wang J, Zhang L Y, Chen J, et al. Compressed sensing based selective encryption with data hiding capability. IEEE Transactions on Industrial Informatics, 2019, 15(12): 6560-6571

[24] Thodi D M, Rodriguez J J. Expansion embedding techniques for reversible watermarking. IEEE Transactions on Image Processing, 2007, 16(3): 721-730

[25] Chang Q, Li X, Zhao Y, et al. Adaptive pairwise prediction-error expansion and multiple histograms modification for reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 31(12): 4850-4863.

[26] Hua Z, Wang Y, Yi S, et al. Reversible data hiding in encrypted images using cipher-feedback secret sharing. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(8): 4968-4982

[27] Candès E J. Compressive sampling//Proceedings of the International Congress of Mathematicians. Madrid, Spain, 2006, 3: 1433-1452

[28] Donoho D L, Elad M. Optimally sparse representation in general (nonorthogonal) dictionaries via ℓ1 minimization. Proceedings of the National Academy of Sciences, 2003, 100(5): 2197-2202

[29] Baraniuk R, Davenport M, DeVore R, et al. A simple proof of the restricted isometry property for random matrices. Constructive Approximation, 2008, 28: 253-263

[30] Figueiredo M A T, Nowak R D, Wright S J. Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems. IEEE Journal of Selected Topics in Signal Processing, 2007, 1(4): 586-597

[31] Zhang J, Zhao C, Zhao D, et al. Image compressive sensing recovery using adaptively learned sparsifying basis via L0 minimization. Signal Processing, 2014, 103: 114-126

[32] Zhao C, Ma S, Zhang J, et al. Video compressive sensing reconstruction via reweighted residual sparsity. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 27(6): 1182-1195

[33] Zhao C, Zhang J, Ma S, et al. Reducing image compression artifacts by structural sparse representation and quantization constraint prior. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 27(10): 2057-2071

[34] Gregory R L. Knowledge in perception and illusion. Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences, 1997, 352(1358): 1121-1127

[35] Wright C V, Feng W, Liu F. Thumbnail-preserving encryption for JPEG//Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. New York, USA, 2015: 141-146

[36] Marohn B, Wright C V, Feng W, et al. Approximate thumbnail preserving encryption. Proceedings of the 2017 on Multimedia Privacy and Security. New York, USA, 2017: 33-43

[37] Zhang Y, Zhao R, Xiao X, et al. HF-TPE: High-fidelity thumbnail-preserving encryption. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(3): 947-961

[38] Chen J, Sun S, Zhang L, et. al. Compressed sensing framework for heart sound acquisition in internet of medical things. IEEE Transactions on Industrial Informatics, 2022, 18(3): 2000-2009

[39] Chun I Y, Adcock B. Compressed sensing and parallel acquisition. IEEE Transactions on Information Theory, 2017, 63(8): 4860-4882

[40] Suo Z, Xia C, Jiang D, et al. Multi-tiered reversible data privacy protection scheme for IoT based on compression sensing and digital watermarking. IEEE Internet of Things Journal, 2024, 11(7): 11524-11539

[41] Yamac M, Ahishali M, Passalis N, et al. Multi-level reversible data anonymization via compressive sensing and data hiding. IEEE Transactions on Information Forensics and Security, 2020, 16: 1014-1028

[42] Agustsson E, Timofte R. Ntire 2017 challenge on single image super-resolution: Dataset and study//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. Honolulu, USA, 2017: 126-135

[43] Martin D, Fowlkes C, Tal D, et al. A database of human segmented natural images and its application to evaluating segmentation algorithms and measuring ecological statistics//Proceedings Eighth IEEE International Conference on Computer Vision. Vancouver, Canada, 2001, 2: 416-423

[44] Candès E J, Romberg J, Tao T. Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Transactions on Information Theory, 2006, 52(2): 489-509

[45] Bianchi T, Bioglio V, Magli E. Analysis of one-time random projections for privacy preserving compressed sensing. IEEE Transactions on Information Forensics and Security, 2015, 11(2): 313-327

WEN Wen-Ying, Ph. D., professor. Her main research interests include image processing and multimedia security.

YANG Yu-Heng, M. S. candidate. His main research interests are compressed sensing and image hiding.

LUO Xin-Yu, M. S. candidate. His main research interests are compressed sensing and image hiding.

ZHANG Yu-Shu, Ph. D., professor. His main research interests include multimedia security and artificial intelligence security.

Fang Yuming, Ph. D., professor. His main research interests include visual quality assessment, computer vision, 3D image/video processing.

Background

Reversible Data Hiding (RDH), as an important data hiding technology, can extract embedded secret data from the host image while losslessly restoring the host image. It can be widely used in medical imaging, military image processing, and legal services, etc.

Compressed sensing domain, as a type of compressed domain, has been widely studied. For compressed domain RDH schemes, data are often embedded into compression coefficients. Since the redundancy in the compressed domain is much smaller than that in the spatial domain, the embedding capacity obtained by the compressed domain method is very limited. Existing compressed sensing domain hiding can be divided into information hiding before compression and information hiding after compression. Information hiding before compression mainly transforms the image into a sparse domain and embeds information through watermarking; auxiliary information is required for data extraction. Information hiding after compression mainly uses redundancy for further compression to make room for information hiding, but the measured values are not available. The usability of the measured values can be ensured by hiding information in the measured values through histogram shifting (HS) technology. But the measured values are lightweight encrypted and their histogram peaks are small, and the information embedding capacity is small.

This paper combines the progressive recovery characteristics of compressed sensing and prediction error expansion technology to propose a reversible data hiding scheme based on data blind extraction of multi-layer cyclic prediction. This scheme introduces multi-layer cyclic prediction embedding technology to predict CS and utilize histogram shifting to embed additional information on the measurement values, which can achieve data blind extraction and lossless restoration of measurement values during the data extraction stage. In addition, a redundant block estimation method is proposed to further improve the usability of the measurement values, where the information is first embedded in redundant blocks, effectively reducing the distortion rate of the image. This proposed scheme integrates thumbnail preservation encryption to self-embed the fidelity value of the sensitive area of the image itself in the measurement value, which provides different visible areas for users with different permissions and thus realizes multi-level preview. Meanwhile, the measured values are externally embedded with secret information that needs to be hidden by employing the robustness of CS, so that without extracting the secret information, the reconstructed image after the encrypted measurement values remains highly similar to the reconstructed image after the unencrypted measurement values, ensuring the concealment of the secret information.

This work was supported by the National Natural Science Foundation of China (No. 62201233), the Jiangxi Provincial Double Thousand Plan (No. jxsq2023201118), and the Jiangxi Pro-vincial Outstanding Youth Fund Project (No. 20232ACB212004)