基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法

李锦伟，张晓雅，姚远志，俞能海
（中国科学技术大学信息科学技术学院，安徽 合肥 230027）

摘　要：针对云数据管理中的用户隐私保护需求，密文域图像可逆信息隐藏受到了学术界的广泛关注。基于加密前预留空间的数据嵌入框架将载体图像分割成由图像块组成的两个独立区域，使用传统的可逆信息隐藏技术腾出数据嵌入空间，可以取得较好的性能。为了更好地利用图像的空间相关性，提出了一种细粒度的可伸缩嵌入空间预留策略。该策略将图像块重新排列，构成纹理区域和平坦区域。图像块的大小可以根据图像的纹理和需要预留空间的大小自适应调整。这些图像块的原始位置将作为待嵌入边信息，用于无损恢复载体图像。由于平坦区域的像素更容易被预测，所以平坦区域可以容纳更多纹理区域的像素比特，以预留更多的数据嵌入空间。同时，在平坦区域使用传统的可逆信息隐藏技术腾出数据嵌入空间时造成的嵌入失真更小。充分的实验证明了基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法在嵌入容量和载密图像质量方面的优越性。

关键词：可逆信息隐藏；空间相关性；细粒度嵌入空间预留；预测误差扩展；直方图平移
中图分类号：TP309.2
文献标志码：A
DOI: 10.11959/j.issn.2096−109x.2022008

Reversible data hiding in encrypted images based on fine-grained embedding room reservation

LI Jinwei, ZHANG Xiaoya, YAO Yuanzhi, YU Nenghai
School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China

Abstract: Reversible data hiding in encrypted images has attracted considerable attention due to the privacy-preserving requirement for cloud data management. The good performance in this area can be achieved by using the existing framework of reserving room before encryption, where the image is partitioned to two independent slices consisting of blocks and then traditional reversible data hiding techniques are utilized to vacate room. In order to better exploit the spatial correlation of images, a fine-grained scalable embedding room reservation strategy in which blocks were rearranged to constitute the textured slice and the smooth slice was proposed. The

收稿日期：2021−08−31；**修回日期：**2021−10−07
通信作者：姚远志，yaoyz@ustc.edu.cn
基金项目：国家重点研发计划（2018YFB0804102）；国家自然科学基金（61802357）；中央高校基本科研业务费专项资金（WK3480000009）
Foundation Items: The National Key R&D Program of China (2018YFB0804102), The National Natural Science Foundation of China (61802357), The Fundamental Research Funds for the Central Universities (WK3480000009)

引用格式：李锦伟, 张晓雅, 姚远志, 等. 基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法[J]. 网络与信息安全学报, 2022, 8(1): 106-117.
Citation Format: LI J W, ZHANG X Y, YAO Z Y, et al. Reversible data hiding in encrypted images based on fine-grained embedding room reservation[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 106-117.

block-size can be adjusted adaptively according to the texture of the images and the size of room to be vacated. The original locations of these blocks were efficiently represented as the to-be-embedded auxiliary information for image restoration. Because pixels in the smooth slice are easier to be predicted, the smooth slice can contain more pixel bits from the textured slice to reserve more room and fewer embedding distortions are induced with traditional reversible data hiding techniques. Extensive experiments demonstrate the merits of the proposed method in terms of embedding capacity and image quality.

Keywords: reversible data hiding, spatial correlation, fine-grained embedding room reservation, prediction error expansion, histogram shifting

0　引言

云外包（cloud outsourcing）是指基于云计算（cloud computing）商业模式应用的服务外包资源与平台的总称。在云平台下，众多的服务外包资源云整合成资源池，通过云管理系统提供外包服务，达到灵活和便利的目的，也可以降低成本和提高效率。云计算的高虚拟化与高可扩展性等优势，使个人和企业愿意外包数据到云端服务器。然而，上传数据中往往含有大量包括病史、收入、身份、兴趣及位置等在内的隐私信息，对这些信息的共享、收集、发布、分析与利用等操作会直接或间接地泄露用户隐私，给用户带来极大的威胁和困扰[1-4]。因此，用户隐私保护已成为人们广泛关注的焦点，而安全外包是云计算隐私保护中不可或缺的关键技术之一[1]。

可逆信息隐藏（RDH，reversible data hiding）是一种特殊的信息隐藏技术，它除了要保证嵌入信息的隐秘性和可提取性，同时需要完全无损地恢复原始载体图像[5-18]。这一重要技术广泛应用于医学影像标注、法律取证等领域，在这些领域，原始图像不能有任何修改，图像像素的微小变化就可能导致诊断结果出错或者法律诉讼失败[7,11-12]。一般来说，RDH 技术在图像空间域有 4 种基本策略，即无损压缩（LC，lossless compression）[19]、差值扩展（DE，difference expansion）[20]、直方图平移（HS，histogram shifting）[21]和最优编码（OC，optimal coding）[22]。

随着云计算的不断发展，将 RDH 外包给云服务器完成可以节约本地的计算资源，数据传输过程中的安全和隐私保护就变得十分重要，图像加密技术因其在隐私保护方面的有效性而被广泛应用。在某些情况下，云服务器需要在加密图像中嵌入一些附加数据，如用户信息、版权数据、时间戳等。如图 1 所示，用户在将图片上传至云服务器前，先对图像预处理并加密。云在密文域图像嵌入附加数据后，由其他用户下载，其中授权用户可以成功解密恢复原始图像，非授权用户则不能获取图像信息，从而保护了用户的隐私。尽管传统的明文域图像 RDH 方法已经十分成熟，但对加密图像无法直接使用。因此，在云外包计算中，密文域可逆信息隐藏（RDH-EI，reversible data hiding in encrypted images）发挥了很大的作用，而如何获得更好的嵌入容量和载密图像视觉质量是 RDH-EI 领域重点关注的问题[5-18]。

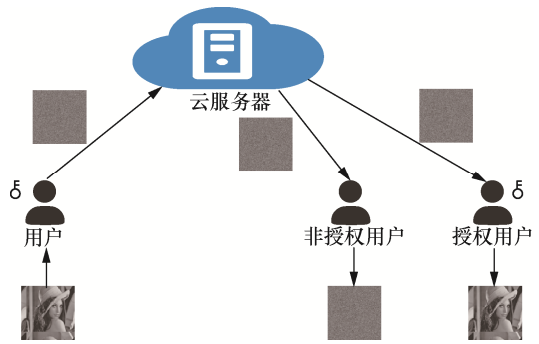


图 1　云外包计算中的密文域可逆信息隐藏
Figure 1　RDH-EI in cloud outsourcing computing

针对上述问题，本文提出了一种细粒度的可伸缩嵌入空间预留策略，可以更好地利用图像的空间相关性，进而在加密图像前预留出更多的空间，同时提高载密图像的视觉质量。由于载体图像之间的差异，本文所提方法会根据实际情况自动调整预留空间尺寸大小，以适配当前载体图像纹理分布情况。通过大量实验，验证了该方法在嵌入容量、载密图像质量、可提取性和可逆性等方面的优势。

本文的主要贡献如下：

1) 提出基于细粒度嵌入空间预留策略的密文域图像可逆信息隐藏方法；

2) 提炼并解决适配图像内容的预留空间尺寸优化问题；

3) 通过充分的实验结果证明所提方法的有效性。

1　相关工作

根据嵌入场合和方式的不同，主流 RDH-EI 可分为基于加密后空间预留（VRAE，vacating room after encryption）框架[10,23-25]和基于加密前空间预留（RRBE，reserved room before encryption）框架[5-8,17-18,26-28]。

1.1　加密后空间预留框架

VRAE 框架对加密图像进行压缩，为数据嵌入腾出空间，如图 2(a)所示。在此框架中，图像所有者使用加密密钥对图像进行加密，然后将加密图像交给数据隐藏者（如云服务器等），数据隐藏者使用数据隐藏密钥腾出一些空间，将一些边信息和秘密消息嵌入加密图像中。然后，接收者使用数据隐藏密钥提取嵌入的数据，并根据加密密钥将密文域图像解密。Zhang[23]提出加密图像可逆信息隐藏方法。该方法将加密图像分块，然后通过翻转每个块中加密像素的 3 个最低有效位（LSB，lowest significant bit）来嵌入信息。然而当分割的图像块相对较小时，该方法在提取消息时会有较大的提取误差，恢复的图像也可能会有失真。Hong 等[24]提出了新的平滑测度函数和边缘匹配机制。相比文献[23]，文献[24]提出的方法消息提取的误差更小，但恢复的图像仍然存在较大的失真。文献[23-24]在提取数据之前都必须要对图像进行解密，即在密文域图像中无法完成对信息的提取，这在实际应用中存在局限性。为此，Zhang[25]提出了压缩加密像素的 LSB 的方法，以腾出空间来容纳额外的数据，这样可实现数据提取与图像解密的分离。

然而，通过 VRAE 框架提取的信息仍然可能会出现错误，恢复的图像可能会有失真，这不能满足某些特定场景的需要。

1.2　加密前空间预留框架

为了实现完全的可逆性，RRBE 框架应运而生。如图 2(b)所示，RRBE 框架在对图像加密前

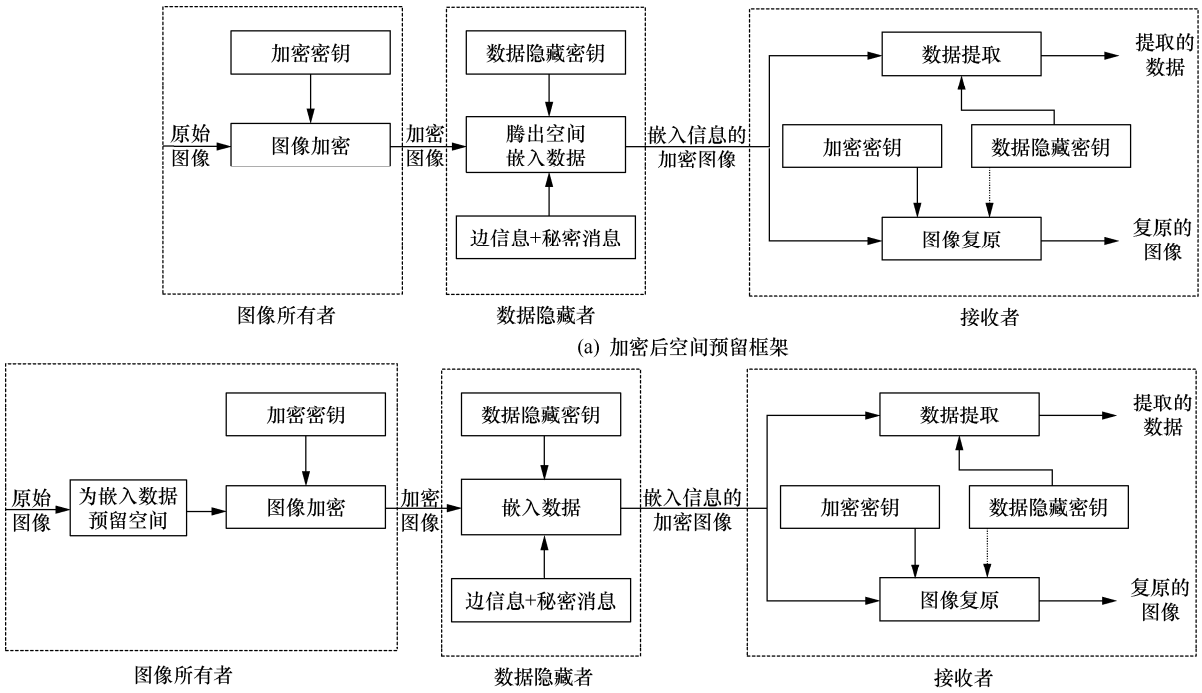


图 2　空间预留框架

Figure 2　Framework of vacating room

对图像进行预处理，为嵌入数据预留空间，然后由数据隐藏者根据数据隐藏密钥在加密图像中嵌入边信息和秘密消息。相比 VRAE 框架，RRBE 框架可以获得更好的嵌入容量和载密图像质量[29]。Ma 等[6]在传统 RDH 方法的基础上，提出了将某些像素的 LSB 嵌入其他像素中来预留嵌入空间的方法。该方法能正确提取数据和重构图像，但嵌入容量较小，解密后的载密图像的视觉质量有待提升。Zhang 等[8]提出了使用预测误差直方图保留预测空间的方法，在一定限度上提高了嵌入容量。Cao 等[26]利用稀疏表达的优势，提出了一种高容量可分离 RDH-EI 方法，大大提高了嵌入容量，但增加了图像所有者的计算负担。Yin 等[17]提出了一种基于最高比特位预测和哈夫曼编码的密文域图像可逆信息隐藏方法。Yin 等[18]提出了一种基于像素预测和比特平面压缩的密文域图像可逆信息隐藏方法。这两种方法[17-18]巧妙地使用像素预测和压缩增加了用于数据嵌入的预留空间。RRBE 框架可以通过改进嵌入空间预留策略进一步提升密文域图像可逆信息隐藏方法的性能[26-29]。

2　细粒度嵌入空间预留策略

现有基于 RRBE 框架的 RDH-EI 方案无法实现细粒度嵌入空间预留，不能充分利用自然图像的空间相关性。如 Yao 等[5]、Ma 等[6]、Zhang 等[8]提出的方案，首先将自然图像分割为纹理与平坦区域，然后用标准的 RDH 算法将纹理区域的 LSB 平面嵌入平坦区域，以达到预留嵌入空间的目的，但该方案在图像分割时只能条带化预留嵌入空间，其将条带纹理复杂度定义为

$$g(n_0)=\sum_{i=n_0+1}^{n_0+n_s-2}\sum_{j=2}^{W-1}\left|p_{i,j}-\frac{p_{i,j-1}+p_{i+1,j}+p_{i,j+1}+p_{i-1,j}}{4}\right| \tag{1}$$

其中，W 是图像宽度，$p_{i,j}$ 是图像第 i 行第 j 列像素的灰度值，条带的宽度 n_s 为

$$n_s=\left\lceil\frac{m}{W}\right\rceil \tag{2}$$

其中，m 是待嵌入数据长度，条带的最优起始位置 n_0 为

$$n_0^*=\arg\max_{n_0} g(n_0), 1\leqslant n_0\leqslant H-n_s+1 \tag{3}$$

H 是图像高度。为了无损地恢复图像，需要将 n_s 与 n_0 的值作为边信息一同嵌入预留空间中。因此，此策略的纯嵌入容量为

$$C_s=n_s\cdot W-2\cdot\lceil \mathrm{lb}H\rceil \tag{4}$$

虽然基于条带化的空间预留策略取得了良好的性能，但依然有较大的提升空间。Qiu 等[7]提出的方案在图像分割时不再拘泥于条带化预留嵌入空间，而是图像块化预留嵌入空间。其对图像分割的依据有两个：一是图像块本身的空间相关性；二是在图像块上使用可逆广义整数变换算法[30]后是否会有像素溢出。该方案虽然在一定限度上利用了图像块的空间相关性，却忽视了块与块之间的空间相关性，而且不能针对不同纹理情况的图像自适应调整图像块大小。

针对以上问题，本文提出了一种细粒度嵌入空间预留（FERR，fine-grained embedding room reservation）策略，FERR 策略依然遵循惯例的思想，处理过程分为 3 个阶段：图像划分、RDH、图像加密。不同于传统的空间预留策略，FERR 策略根据实际载体图像的纹理情况，以及需要嵌入的秘密消息长度，模拟分析出最适合的分块尺寸 $h\times w$，即

$$\begin{aligned}&h^*,w^*=\arg\min_{h,w}\mathrm{MSE}(I,I^{\mathrm{DM}})\ \text{subject to}\\&\mathrm{mod}(H,h)=\mathrm{mod}(W,w)=0\end{aligned} \tag{5}$$

其中，I 为原始图像，I^{DM} 为带有嵌入消息的解密图像。

$$\mathrm{MSE}(x,y)=\frac{1}{n}\sum_{i=1}^{n}(x_i-y_i)^2 \tag{6}$$

为了充分利用图像块内与图像块间的空间相关性，将每个像素点 (i,j) 的纹理复杂度用数值 $g_{i,j}$ 度量出来，像素点 (i,j) 的灰度值为 $p_{i,j}$，则定义像素点 (i,j) 周围所有像素灰度值的均值与 $p_{i,j}$ 的绝对差值，即 $g_{i,j}$ 的取值。例如，当像素点处于非边缘位置时，有

$$g_{i,j}=\left|p_{i,j}-\frac{p_{i,j-1}+p_{i+1,j}+p_{i,j+1}+p_{i-1,j}}{4}\right| \tag{7}$$

将图像按式(5)分析得到最优分块尺寸 $h\times w$，假设第 k 个图像块的纹理复杂度为 G_k，其左上角

像素位置为 (i_k, j_k)，则由式(7)可得

$$G_k = \sum_{i=i_k}^{i_k+h-1} \sum_{j=j_k}^{j_k+w-1} \left| p_{i,j} - \frac{p_{i,j-1} + p_{i+1,j} + p_{i,j+1} + p_{i-1,j}}{4} \right| \tag{8}$$

对 $N = \frac{H \cdot W}{h \cdot w}$ 个图像块的纹理复杂度 $\{G_1, G_2, \cdots, G_N\}$ 按照降序排列，得到

$$\{G_{\sigma(1)}, G_{\sigma(2)}, \cdots, G_{\sigma(N)}\}, G_{\sigma(1)} \geqslant G_{\sigma(2)} \geqslant \cdots \geqslant G_{\sigma(N)} \tag{9}$$

根据待嵌入消息的长度 m，可得出最优的纹理区域图像块数目为

$$\begin{aligned} n_b^* &= \arg\min_{n_b} C_f \text{ subject to} \\ C_f &\geqslant m, \mathrm{mod}(n_b, W) = 0 \end{aligned} \tag{10}$$

其中，C_f 为纯嵌入容量。由式(10)可以看出，纹理区域 A 和平坦区域 B 均为与原图像等宽的图像，这不仅为后续的 RDH 过程[31]提供了极大的便利，纹理区域 A 的 LSB 平面略大于消息的长度 m，还增大了对嵌入数据的不可预测性，提高了待嵌入消息的安全性。

由式(10)得到纹理区域 A 图像块数目 n_b 的值后，用“1”标注第 $\sigma(1), \sigma(2), \cdots, \sigma(n_b)$ 个图像块的位置，用“0”标注其余位置，便可得到图像分割的位置图（LM，location map）。为了能在图像解密过程中恢复图像块的原始位置，需要将 LM 作为边信息嵌入纹理区域 A 中。LM 的数据长度即图像块的总数量 N，考虑到自然图像的空间相关性，LM 可以使用 JBIG 算法来进行压缩，因此，LM 的实际长度为

$$l_1 = \min\left\{ \frac{H \cdot W}{h \cdot w}, \mathrm{Length}\left(\mathrm{JBIG(LM)}\right) \right\} \tag{11}$$

其中，Length(JBIG(LM)) 表示对 LM 使用 JBIG 压缩后生成的比特流长度。

由于 FERR 策略在分割图像时，分块尺寸 $h \times w$ 会根据实际图像纹理情况和待嵌入消息长度自适应地调整，同样地，为了实现可逆性，分块尺寸需要作为边信息嵌入纹理区域 A 中。考虑到实际情况，可以分别用 6 bit 来表示 h 和 w。分块尺寸长度 l_2=12。FERR 策略的纯嵌入容量为

$$C_f = n_b hw - l_1 - l_2 \geqslant n_b hw - \frac{H}{h}\frac{W}{w} - 12 \tag{12}$$

将第 $\sigma(1), \sigma(2), \cdots, \sigma(n_b)$ 个图像块按列顺序依次移至图像的上方，即可组成纹理区域 A，剩余图像块采用同样方式可组成平坦区域 B，图像分割前后图像块对应关系如图 3 所示。

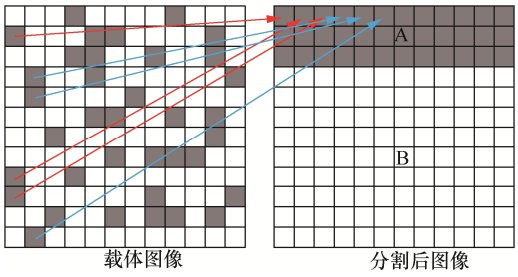


图 3　图像分割前后图像块对应关系

Figure 3　Image block correspondence before and after segmentation

3　可逆信息隐藏方法实现

本文提出的 FERR 策略仍然基于 RRBE 框架，整个密文域可逆信息隐藏流程如图 4 所示。图像所有者以 FERR 策略为依据对图像做预处理，即图像分割、嵌入空间预留、图像加密、边信息嵌入，然后将加密图像上传至云服务器，云服务器将秘密数据嵌入加密图像中。在接收端，有数据提取权限的用户可以根据数据隐藏密钥准确无误地提取出秘密消息，有图像查看权限的用户可以根据加密密钥对图像进行解密，而具有双权限的用户可以在完整地提取出秘密数据的同时，无损地恢复载体图像。

3.1　数据嵌入

3.1.1　图像分割与嵌入空间预留

按照本文提出的 FERR 策略，根据实际载体图像和待嵌入消息的长度，将图像 I 分为纹理区域 A 和平坦区域 B，如图 3 所示，并生成位置图 LM。若 LM 在使用 JBIG 算法压缩后长度变短，则将压缩后的比特流视为边信息，否则边信息仍为原始的 LM。

根据边信息与待嵌入消息的长度，用数据加密密钥确定腾出空间的位置，即区域 A 的部分 LSB 平面用标准的 RDH 算法[31-32]（并不依赖特定的 RDH 算法）嵌入平坦区域 B 中。以 SACHNEV 等[31]提出的 RDH 算法为例，该算法

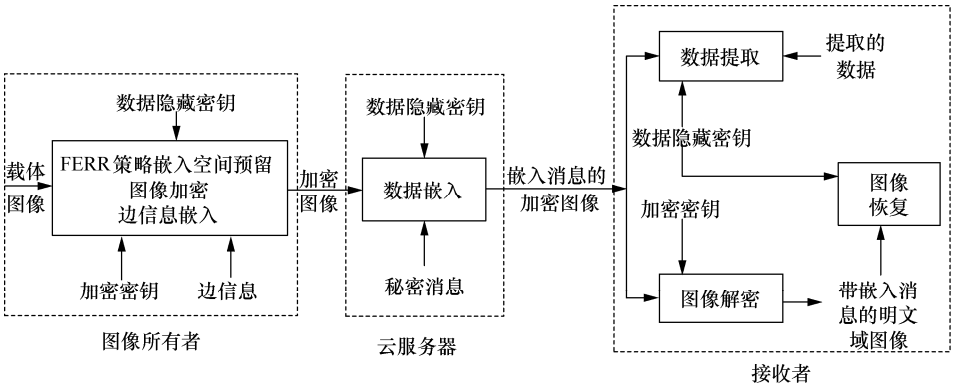


图 4　基于 FERR 策略的 RDH-EI 流程
Figure 4　Flow chart of RDH-EI based on FERR strategy

将载体图像中的所有像素交错地分为黑像素和白像素两种，如图 5 所示。

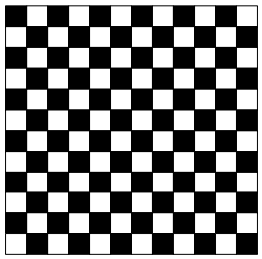


图 5　RDH 算法对像素的分类
Figure 5　Classification of pixels by RDH algorithm

对于每一个黑像素 $u_{i,j}$，由其相邻的所有白像素进行插值估计，如式(13)所示。

$$u'_{i,j}=\left\lfloor \frac{v_{i,j-1}+v_{i+1,j}+v_{i,j+1}+v_{i-1,j}}{4} \right\rfloor \tag{13}$$

黑像素(i,j)的预测误差为

$$d_{i,j}=u_{i,j}-u'_{i,j} \tag{14}$$

通过预测误差扩展与直方图平移技术，可以将消息比特嵌入黑像素(i,j)中，如式(15)～式(16)所示。

$$D_{i,j}=\begin{cases}2d_{i,j}+m_k, d_{i,j}\in[T_n,T_p]\\ d_{i,j}+T_p+1, d_{i,j}>T_p\\ d_{i,j}+T_n, d_{i,j}<T_n\end{cases} \tag{15}$$

$$U_{i,j}=D_{i,j}+u'_{i,j} \tag{16}$$

其中，T_p,T_n 分别是正负阈值。与其他 RDH 算法一样，当自然边界像素由 255 变为 256 或从 0 变为负数时，会出现溢出问题。因此，需要记录在使用预测误差扩展与直方图平移技术后溢出的像素点，作为边信息一同嵌入其他像素 点中。

同样地，在所有黑像素中完成消息嵌入后，白像素可以用相邻的载密黑像素来进行插值估计，完成第二轮消息的嵌入。如此反复，可以实现多轮嵌入，大大提高了嵌入容量。为保证解密后图像的视觉质量，本文在使用 RDH 算法[31]时，至多嵌入 8 轮，然后将嵌入轮数同样纳入边信息中，以便在接收端能无损提取消息、恢复图像。

3.1.2　图像加密与边信息嵌入

将纹理区域A的部分LSB平面嵌入平坦区域B 中以后，将区域 A、B 按上下顺序拼在一起，得到重排图像 I^{R}。利用加密密钥对 I^{R} 进行加密，构造密文域图像 I^{E}。图像 I^{R} 像素的灰度值（0～255）可以用 8 bit 表示，如像素(i, j)可以表示为 $\left\{v_{i,j}^{(0)},v_{i,j}^{(1)},v_{i,j}^{(2)},v_{i,j}^{(3)},v_{i,j}^{(4)},v_{i,j}^{(5)},v_{i,j}^{(6)},v_{i,j}^{(7)}\right\}$，其与灰度值 $V_{i,j}$ 的关系为

$$v_{i,j}^{(k)}=\left\lfloor \frac{V_{i,j}}{2^k} \right\rfloor \bmod 2, k=0,1,\cdots,7 \tag{17}$$

$$V_{i,j}=\sum_{k=0}^{7}v_{i,j}^{(k)}2^k \tag{18}$$

利用加密密钥生成大小为 $8\times H\times W$ 的随机序列

$$E=\left\{e_{i,j}^{(k)}\mid e_{i,j}^{(k)}\in\{0,1\},k=0,1,\cdots,7\right\} \tag{19}$$

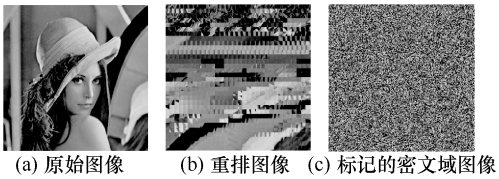
然后计算像素位与伪随机位的逐位异或结果

$$v'^{(k)}_{i,j}=v_{i,j}^{(k)}\oplus e_{i,j}^{(k)} \tag{20}$$

则加密后位置(*i*,*j*)的像素灰度值为

$$V'_{i,j}=\sum_{k=0}^{7}v'^{(k)}_{i,j}2^k \tag{21}$$

这样便获得了密文域图像 I^{E}。再将边信息嵌入 I^{E} 头部的 LSB 中，就得到了标记的密文域图像 I^{EM}，云服务器通过读取 I^{EM} 带有的边信息，可以得知允许其嵌入秘密数据的像素点的位置。图像加密上传后，如果没有加密密钥，云服务器或者第三方非授权用户就无法访问原始图像，从而保护图像所有者的隐私。定义嵌入率（ER，embedding rate）为平均每像素嵌入的比特数，单位为 bpp。当 ER = 0.2 bpp 时，Lena 图像的原始图像 I、重排图像 I^{R} 和标记的密文域图像 I^{EM} 如图 6 所示。



(a) 原始图像 (b) 重排图像 (c) 标记的密文域图像

图 6 Lena 图像

Figure 6 Lena image

3.1.3 秘密消息嵌入

将标记的密文域图像 I^{EM} 上传到云服务器后，即使云服务器没有加密密钥，不能访问原始图像，仍然可以将秘密数据进一步嵌入 I^{EM} 中。云服务器可以直接读取 I^{EM} 头部的 LSB 以获得边信息，边信息中的 LM（或在 JBIG 解码后获得）能够帮助定位 A 区域，从而确定允许嵌入数据的像素点位置。云服务器利用数据隐藏密钥，随机选择像素嵌入顺序，用 LSB 替换的方法将秘密数据嵌入像素点（e 为秘密消息比特，$e\in\{0,1\}$），如式(22)所示。由于这些像素点的 LSB 已经提前嵌入区域 B 中，所以这并不会影响整个过程的可逆性。嵌入过程数据流向示意如图 7 所示。

$$V''_{i,j}=\sum_{k=0}^{7}v'^{(k)}_{i,j}2^k+e \tag{22}$$

3.2 数据提取与图像恢复

接收端在收到图像后，首先同样可以从图像头部的 LSB 获取到边信息，定位出 A、B 区域。如果接收端拥有数据隐藏密钥，就可以在区域 A 中确定数据嵌入像素点的位置以及顺序，从而可以完整地提取出秘密数据。如果接收端拥有加密密钥，利用加密密钥生成随机序列 E，利用式(20)计算图像像素位与 E 的逐位异或结果，便得到了解码的重排图像 I^{DR}，I^{DR} 与 I^{R} 除了在嵌入边信息和秘密数据的像素点 LSB 有所差异之外，其余各位完全相同，所以图像 I^{DR} 与 I^{R} 在视觉上并无差异。从边信息中还可以获得图像拥有者划分图像块的尺寸信息 $h\times w$，按照 $h\times w$ 对图像重新分块后，根据提取出的 LM 信息将图像块放回至原始位置，得到带有嵌入消息的解密图像 I^{DM}。同样地，解密图像 I^{DM} 与原始图像 I 在视觉上并无差异，所以，接收端用户可以获取到图像本身的内容信息。

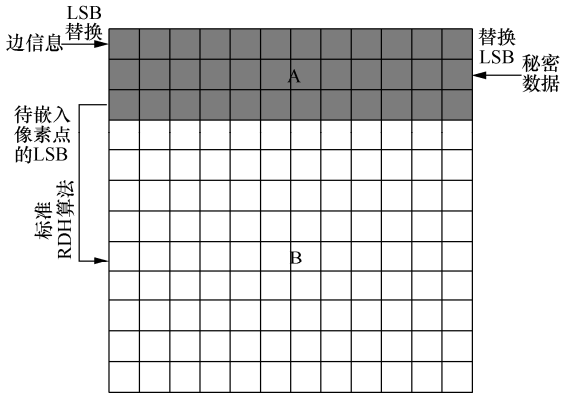


图 7 嵌入过程数据流向示意

Figure 7 Schematic of data transfer during the embedding

而拥有双密钥的授权用户，在完整提取出秘密数据并解密图像后，还可以利用 RDH 算法[31]的提取过程，从区域 B 中提取出 A 的部分 LSB 并还原 B，再利用提取出的 LSB 还原 A，重新放回图像块位置后就得到了完全无损的载体图像，实现了数据隐藏的可逆性。值得一提的是，即使接收端用户是先后获得两种授权的（即先后获得两种密钥），也可以用第一个密钥进行数据提取或者图像解密，当获得第二个密钥时，可以在前面的结果上继续进行，最终获得无损的秘密消息和载体图像。本文所提方案实现了消息提取和图像恢复的分离，在实际应用中满足了隐私保护的需求。当 ER = 0.4 bpp 时，Peppers 图像的原始图像 I、带有嵌入消息的解密图像 I^{DM} 和重构图像 I^{RE} 如图 8 所示。

(a) 原始图像　(b) 解密图像　(c) 重构图像

图 8　Peppers 图像
Figure 8　Peppers image

4　实验结果与分析

4.1　实验设置

为了验证本文提出的基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法的有效性，在实验部分重点针对载密图像质量进行性能测试，并对所提 RDH-EI 方法的安全性进行分析。

将基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法在 Matlab R2016a 中实现，并选取 Ma 等[6]和 Qiu 等[7]提出的密文域图像可逆信息隐藏方法作为对比。实验中使用峰值信噪比（PSNR，peak signal-to-noise ratio）和结构相似性（SSIM，structural similarity）评价载密图像相对于载体图像的视觉质量，PSNR 的单位为 dB。

4.2　载密图像质量

由图 6(b)可以看出，运用 FERR 策略后，图像的纹理情况较为复杂的块被重排至图像上方，而平坦的块被重排至图像下方，平坦区域在做 RDH 时对像素预测十分有利，这会增大 RDH 算法的嵌入容量，提高载密图像质量。由于 RDH 算法服务于实际嵌入空间预留，所以整个 RDH-EI 方法的嵌入容量和解密后的载密图像质量就会随着提高。如图 8(b)所示，当 ER = 0.4 bpp 时，用标准测试图像中 Peppers 图像进行测试得到的解密图像，从视觉上与原图像毫无差异，在隐蔽性方面取得了较好的结果，体现了 FERR 策略的优越性。

与 Ma 等[6]、Qiu 等[7]提出的方法相比，在相同图像的条件下，嵌入率不同时，运用本文所提方法得到的解密图像的 PSNR 与 SSIM 值大多大于文献[6]和文献[7]的方法。以标准测试图像中的 Lena 图像、Mandrill 图像和 Peppers 图像为例，3 种方案的解密图像峰值信噪比与嵌入率关系（PSNR-ER）曲线如图 9～图 11 所示，解密图像结构相似性与嵌入率关系（SSIM-ER）曲线如图 12～图 14 所示。

本文所提方法不仅在大容量嵌入时具有较高的优越性，在小嵌入率的情况下也展现了优于文献[6]方法和文献[7]方法的性能。小嵌入率时的 PSNR-ER 曲线对比如图 15～图 17 所示，SSIM-ER 曲线对比如图 18～图 20 所示。

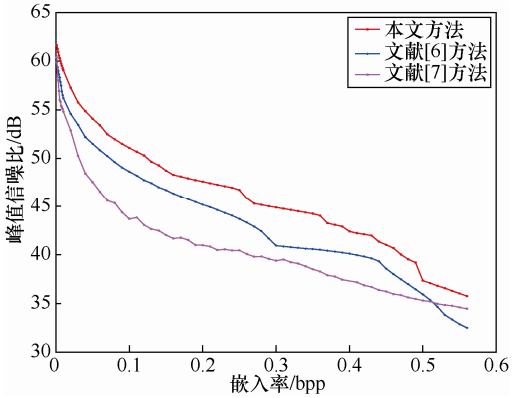


图 9　解密后的 Lena 图像的 PSNR-ER 曲线
Figure 9　PSNR-ER curves of decrypted Lena image

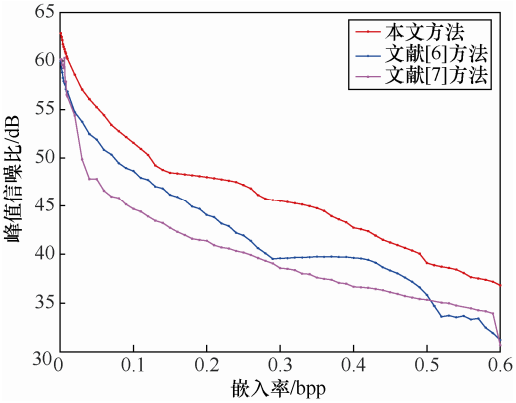


图 10　解密后的 Mandrill 图像的 PSNR-ER 曲线
Figure 10　PSNR-ER curves of decrypted Mandrill image

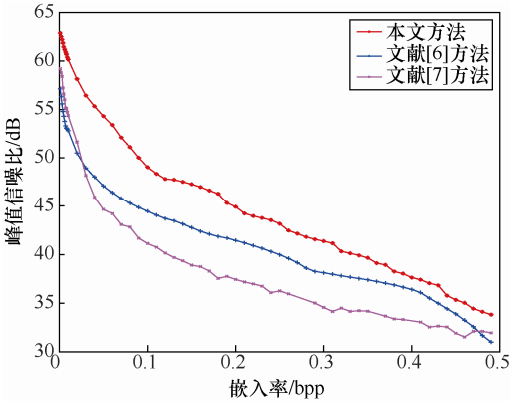


图 11　解密后的 Peppers 图像的 PSNR-ER 曲线
Figure 11　PSNR-ER curves of decrypted Peppers image

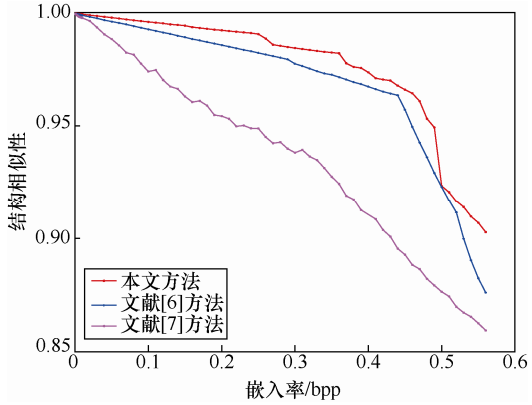


图 12　解密后的 Lena 图像的 SSIM-ER 曲线
Figure 12　SSIM-ER curves of decrypted Lena image

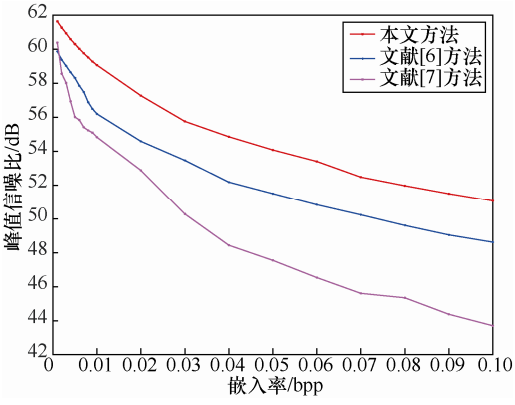


图 15　小嵌入容量时解密后的 Lena 图像的 PSNR-ER 曲线
Figure 15　PSNR-ER curves of decrypted Lena image with small ER

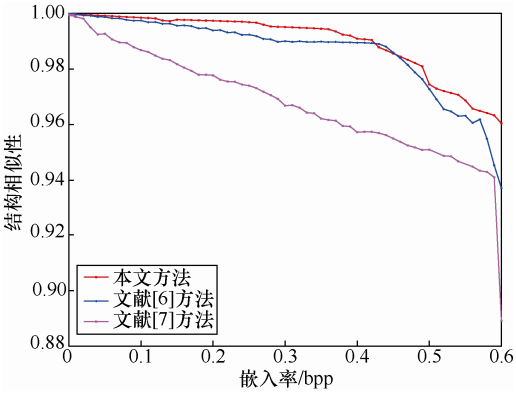


图 13　解密后的 Mandrill 图像的 SSIM-ER 曲线
Figure 13　SSIM-ER curves of decrypted Mandrill image

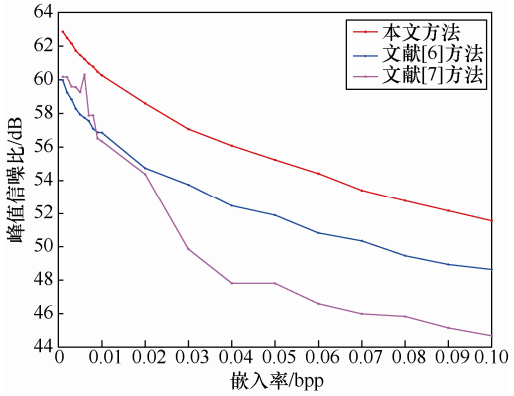


图 16　小嵌入容量时解密后的 Mandrill 图像的 PSNR-ER 曲线
Figure 16　PSNR-ER curves of decrypted Mandrill image with small ER

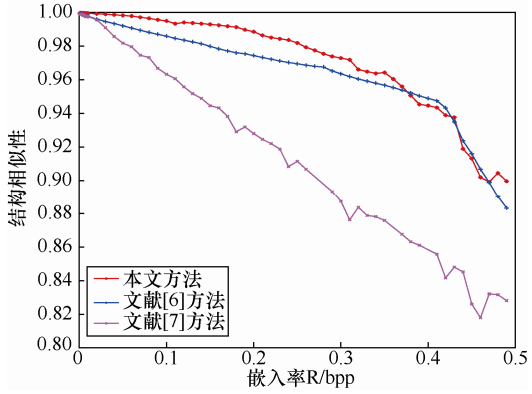


图 14　解密后的 Peppers 图像的 SSIM-ER 曲线
Figure 14　SSIM-ER curves of decrypted Peppers image

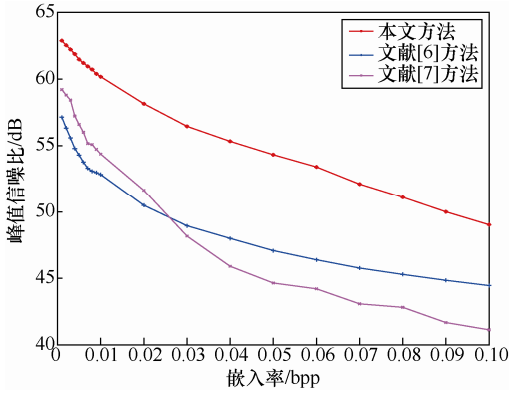


图 17　小嵌入容量时解密后的 Peppers 图像的 PSNR-ER 曲线
Figure 17　PSNR-ER curves of decrypted Peppers image with small ER

为了验证本文所提方法的普适性，在图像数据集 UCID 和 BOSSbase (v1.01)上对本文方法进行测试。在不同嵌入率下，对数据集中所有图像分别使用本文方法、文献[6]方法以及文献[7]方法，计算解密图像与原始图像的 PSNR，并求出数据集的平均 PSNR，所得结果如表 1 所示。

表 1 中的黑体数字表示在相应嵌入率下 3 种不同方法可以取得的最大 PSNR 值。由图 9～图 20 和表 1 可以看出，在不同嵌入率下，本文所提方法在标准测试图像和图像数据集 UCID、BOSSbase 上的解密图像视觉质量均优于文献[6]方法和文献[7]方法，且在嵌入率较小时本文方案

表 1　不同嵌入率下在图像数据集上使用不同方案得到的解密图像平均 PSNR
Table 1　Average PSNR of decrypted images using different schemes on image datasets with different ER

单位：dB

嵌入率	UCID			BOSSbase		
	本文方法	文献[6]方法	文献[7]方法	本文方法	文献[6]方法	文献[7]方法
0.1	**52.396**	48.724	43.798	**53.456**	50.318	44.699
0.2	**48.595**	45.682	41.985	**49.698**	47.272	42.662
0.3	**46.385**	40.929	39.93	**47.669**	43.335	40.838
0.4	**44.201**	40.973	38.07	**45.867**	43.3	39.151
0.5	**39.979**	37.695	36.46	**41.665**	40.356	37.578

优势更为明显。

实验表明，相比较于传统的嵌入空间预留策略，本文所提出的运用 FERR 策略的 RDH-EI 方法在嵌入容量、解密图像视觉质量（用 PSNR 和 SSIM 度量）和实用性（数据提取过程与图像解密过程实现完全分离）等方面均具有明显的优势。

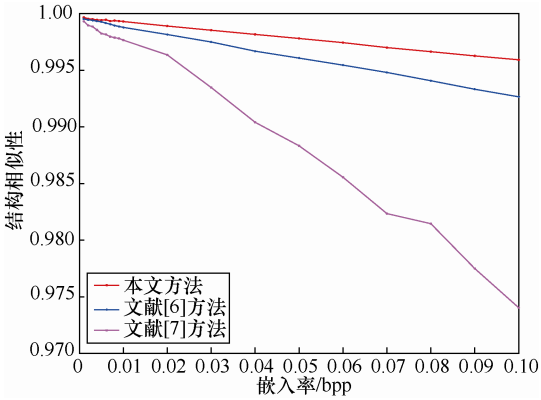


图 18　小嵌入容量时解密后的 Lena 图像的 SSIM-ER 曲线
Figure 18　SSIM-ER curves of decrypted Lena image with small ER

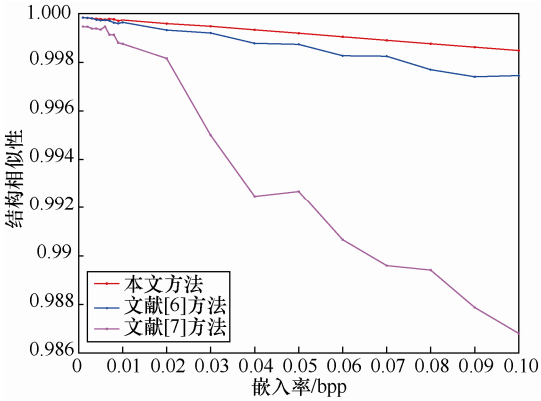


图 19　小嵌入容量时解密后的 Mandrill 图像的 SSIM-ER 曲线
Figure 19　SSIM-ER curves of decrypted Mandrill image with small ER

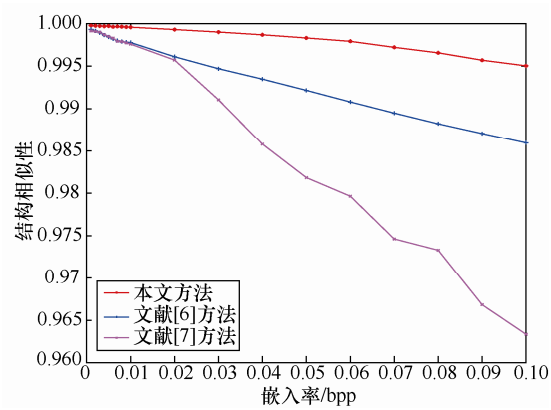


图 20　小嵌入容量时解密后的 Peppers 图像的 SSIM-ER 曲线
Figure 20　SSIM-ER curves of decrypted Peppers image with small ER

4.3　安全性分析

基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法的安全性包括图像内容安全性和嵌入消息安全性。

4.3.1　图像内容安全性

对于云服务器，用户上传的图像处于加密状态，云服务器在没有加密密钥的情况下无法得到解密的图像。在基于细粒度嵌入空间预留的密文域图像可逆信息隐藏方法中，使用图像加密密钥对重排图像 I^{R} 进行加密。若 8 bit 重排图像 I^{R} 的尺寸为 $H\times W$，则密钥的长度为 $8HW$。使用流密码加密重排图像时产生 2^{8HW} 种可能的伪随机序列。在没有图像加密密钥的情况下得到解密重排图像的概率为 $1/2^{8HW}$，以分辨率为 512×512 的图像为例，此概率约为 2×10^{-631306}。因此，在没有图像加密密钥的情况下，非授权用户几乎无法获得解密重排图像。

4.3.2　嵌入消息安全性

将标记的密文域图像 I^{EM} 上传到云服务器

后，即使云服务器没有加密密钥，不能访问原始图像，仍然可以将秘密数据进一步嵌入 I^{EM} 中。为了防止未授权用户非法提取嵌入的秘密数据，云服务器在嵌入数据时利用数据隐藏密钥，对加密图像的 A 区域中的像素嵌入顺序进行随机选择。因此，在没有数据隐藏密钥的情况下，即使拥有载密图像也无法提取嵌入的数据。

5 结束语

本文提出了一种细粒度嵌入空间预留策略，根据实际载体图像纹理情况和嵌入信息大小自适应调整预留空间尺寸大小，将非相邻图像块重新排列，构成纹理区域和平坦区域进行信息嵌入。实验表明，本文所提出的基于细粒度嵌入空间预留策略的密文域图像可逆信息隐藏方法能够提炼并解决适配图像内容的预留空间尺寸优化问题，嵌入性能提升显著，同时可以获得高质量解密图像，具有较高的安全性。

随着云数据管理中对隐私保护的要求越来越高，对加密图像中的可逆信息隐藏技术的性能要求日益提升。由于同一图像不同区域的纹理情况也有可能差异较大，受视频编码技术中帧内宏块划分策略的启发，本文所提方法可以采用更为灵活的图像内可变尺寸块，从而进一步提升嵌入性能与图像视觉质量。可视水印技术在识别所有权和阻止恶意侵犯版权的行为中有着巨大的作用，可以将细粒度嵌入空间预留策略迁移至可视水印技术，从而提高带水印图像的视觉质量，图像细节内容不会因嵌入水印而有所丢失，实用性将大大提高。

参考文献：

[1] 李凤华, 李晖, 贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报, 2016, 37(4): 1-11.
LI F H, LI H, JIA Y, et al. Privacy computing: concept, connotation and its research trend[J]. Journal on Communications, 2016, 37(4): 1-11.

[2] 李凤华, 孙哲, 牛犇, 等. 跨社交网络的隐私图片分享框架[J]. 通信学报, 2019, 40(7): 1-13.
LI F H, SUN Z, NIU B, et al. Privacy-preserving photo sharing framework cross different social network[J]. Journal on Communications, 2019, 40(7): 1-13.

[3] LI F H, LI H, NIU B, CHEN J J. Privacy computing: concept, computing framework, and future development trends[J]. Engineering, 2019, 5(6): 1179-1192.

[4] 张亮轩, 李晖. 云计算中支持有效用户撤销的多授权方基于属性加密方案[J]. 网络与信息安全学报, 2016, 2(2): 62-74.
ZHANG L X, LI H. Multi-authority attribute-based encryption with efficient user revocation in cloud computing [J]. Chinese Journal of Network and Information Security, 2016, 2(2): 62-74.

[5] YAO Y Z, ZHANG W M, WANG H, et al. Content-adaptive reversible visible watermarking in encrypted images June[J]. Signal Processing, 2019, 164(11): 386-401.

[6] MA K D, ZHANG W M, ZHAO X F, et al. Reversible data hiding in encrypted images by reserving room before encryption [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 553-562.

[7] QIU Y Q, YING Q C, LIN X D, et al. Reversible data hiding in encrypted images with dual data embedding[J]. IEEE Access, 2020, 8: 23209-23220.

[8] ZHANG W M, MA K D, YU N H. Reversibility improved data hiding in encrypted images[J]. Signal Processing, 2014, 94(1): 118-127.

[9] HU X C, ZHANG W M, YU N H, et al. Fast estimation of optimal marked-signal distribution for reversible data hiding[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(5): 779-788.

[10] ZHANG X P, QIAN Z X, FENG G R. Efficient reversible data hiding in encrypted images[J]. Journal of Visual Communication and Image Representation, 2014, 25(2): 322-328.

[11] 杨杨, 张卫明, 侯冬冬, 等. 具有对比度增强效果的可逆信息隐藏研究进展与展望[J]. 网络与信息安全学报, 2016, 2(4): 12-20.
YANG Y, ZHANG W M, HOU D D, et al. Research and prospect of reversible data hiding method with contrast enhancement [J]. Chinese Journal of Network and Information Security, 2016, 2(4): 12-20.

[12] BRAR A S, KAUR M. Reversible watermarking techniques for medical images with ROI-temper detection and recovery - a survey [J]. International Journal of Emerging Technology and Advanced Engineering, 2012, 2(1): 32-36.

[13] YIN Z X, LUO B, HONG W. Separable and error-free reversible data hiding in encrypted image with high payload [J]. The Scientific World Journal, 2014, (2014): 604876.

[14] YIN Z X, ABEL A, ZHANG X P, et al. Reversible data hiding in encrypted image based on block histogram shifting [C]//2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2016: 2129-2133.

[15] 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.

[16] YI S, ZHOU Y C. Separable and reversible data hiding in encrypted images using parametric binary tree labeling [J]. IEEE Transactions on Multimedia, 2019, 21(1): 51-64.

[17] YIN Z X, XIANG Y Z, ZHANG X P. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding[J]. IEEE Transactions on Multimedia, 2020, 22(4): 874-884.

[18] YIN Z X, PENG Y Y, XIANG Y Z. Reversible data hiding in

encrypted images based on pixel prediction and bit-plane compression [J]. IEEE Transactions on Dependable and Secure Computing, 2020: 1.

[19] CELIK M U, SHARMA G, TEKALP A M, et al. Lossless generalized-LSB data embedding[J]. IEEE Transactions on Image Process, 2005, 14(2): 253-266.

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

[21] LI X L, ZHANG W M, GUI X L, et al. Efficient reversible data hiding based on multiple histograms modification[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 2016-2027.

[22] ZHANG X P. Reversible data hiding with optimal value transfer[J]. IEEE Transactions on Multimedia, 2013, 15(2): 316-325.

[23] ZHANG X P. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.

[24] HONG W, CHEN T S, WU H Y. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202.

[25] ZHANG X P. Separable reversible data hiding in encrypted image [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 826-832.

[26] CAO X C, DU L, WEI X X, et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation[J]. IEEE Transactions on Cybernetics, 2016, 46(5):1132-1143.

[27] YI S, ZHOU Y C. Binary-block embedding for reversible data hiding in encrypted images[J]. Signal Processing, 2017, 133: 40-51.

[28] CHEN K M, CHANG C-C. High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement[J]. Journal of Visual Communication and Image Representation, 2019, 58: 334-344.

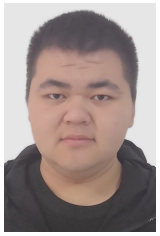
[29] LONG M, ZHAO Y, ZHANG X, et al. A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering[J]. Signal Processing, 2020, 176: 107703.

[30] WANG X, LI X L, YANG B, et al. Efficient generalized integer transform for reversible watermarking[J]. IEEE Signal Processing Letters, 2010, 17(6): 567-570.

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

[32] LUO L X, CHEN Z Y, CHEN M, et al. Reversible image watermarking using interpolation technique[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 187-193.

[作者简介]



李锦伟（1997− ），男，安徽蚌埠人，中国科学技术大学硕士生，主要研究方向为信息隐藏、隐私保护和媒体内容安全。

张晓雅（1998− ），女，河北衡水人，中国科学技术大学硕士生，主要研究方向为信息隐藏、隐私保护和媒体内容安全。

姚远志（1989− ），男，安徽望江人，博士，中国科学技术大学副研究员，主要研究方向为信息隐藏和视频编码。

俞能海（1964− ），男，安徽无为人，博士，中国科学技术大学教授、博士生导师，主要研究方向为图像视频处理与分析、计算机视觉与模式识别、信息隐藏与媒体内容安全、信息检索与数据挖掘。