软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(12):4746–4757 [doi: 10.13328/j.cnki.jos.006350]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

自适应编码的高容量密文可逆信息隐藏算法*

马文静[1], 吴友情[2], 殷赵霞[1]

[1](多模态认知计算安徽省重点实验室(安徽大学), 安徽 合肥 230601)

[2](合肥师范学院 计算机学院, 安徽 合肥 230601)

通信作者: 殷赵霞, E-mail: yinzhaoxia@ahu.edu.cn

摘 要: 随着数字信息技术的普及, 密文可逆信息隐藏(reversible data hiding in encrypted images, RDHEI)逐渐成为云存储中隐私保护的研究热点. RDHEI 作为一种能在密文中嵌入额外信息, 并正确提取嵌入信息和无损恢复原始图像的技术, 受到研究者的广泛关注. 为了能在加密图像中嵌入充足的额外信息, 提出了一种自适应编码的高容量 RDHEI 算法. 首先, 计算原始图像不同预测误差的出现概率并自适应的生成哈夫曼编码; 然后, 利用流密码加密原始图像, 根据像素预测误差对应的哈夫曼码字对加密后像素进行标记; 最后, 以位替换方式将信息嵌入到已标记像素的预留空间中. 经实验验证: 该算法在正确提取嵌入信息的同时, 无损地恢复了原始图像. 与同类算法相比, 该算法充分利用了图像本身的纹理特性, 有效地提高了图像嵌入率. 在 UCID, BOSSBase 和 BOWS-2 这 3 个图像集上, 该算法的平均嵌入率达到 3.162 bpp, 3.917 bpp 以及 3.775 bpp, 与当前性能最佳算法相比, 提升了 0.263 bpp, 0.292 bpp 以及 0.280 bpp.

关键词: 隐私保护; 可逆信息隐藏; 加密图像; 自适应编码; 预测误差

中图法分类号: TP309

中文引用格式: 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. 软件学报, 2022, 33(12): 4746–4757. http://www.jos.org.cn/1000-9825/6350.htm

英文引用格式: Ma WJ, Wu YQ, Yin ZX. High-capacity Reversible Data Hiding in Encrypted Images Using Adaptive Encoding. Ruan Jian Xue Bao/Journal of Software, 2022, 33(12): 4746–4757 (in Chinese). http://www.jos.org.cn/1000-9825/6350.htm

High-capacity Reversible Data Hiding in Encrypted Images Using Adaptive Encoding

MA Wen-Jing[1], WU You-Qing[2], YIN Zhao-Xia[1]

[1](Anhui Provincial Key Laboratory of Multimodal Cognitive Computation (Anhui University), Hefei 230601, China)

[2](School of Computer Science and Technology, Hefei Normal University, Hefei 230601, China)

Abstract: With the popularization of digital information technology, the reversible data hiding in encrypted images (RDHEI) has gradually become the research hotspot of privacy protection in cloud storage. As a technology which can embed additional information in encrypted domain, extract the embedded information correctly, and recover the original image without loss, RDHEI has been widely paid attention by researchers. To embed sufficient additional information in the encrypted image, a high-capacity RDHEI method using adaptive encoding is proposed in this study. Firstly, the occurrence frequency of different prediction errors of the original image is calculated and the corresponding adaptive Huffman coding is generated. Then, the original image is encrypted with stream cipher and the encrypted pixels are marked with different Huffman codewords according to the prediction errors. Finally, additional information is embedded in the reserved room of marked pixels by bit substitution. The experimental results show that the proposed algorithm can extract the embedded information correctly and recover the original image losslessly. Compared with similar algorithms, the proposed algorithm makes full use of the characteristics of the image itself and greatly improves the embedding rate of the image. On UCID, BOSSBase, and BOWS-2 datasets, the average embedding rate of the proposed algorithm reaches 3.162 bpp, 3.917 bpp, and 3.775 bpp, which is higher than the state-of-the-art algorithm of 0.263 bpp, 0.292 bpp, and 0.280 bpp, respectively.

* 基金项目: 国家自然科学基金(61872003, 61502009); 计算机体系结构国家重点实验室开放课题(CARCHB202018)
收稿时间: 2021-02-08; 修改时间: 2021-03-09; 采用时间: 2021-04-15; jos 在线出版时间: 2021-12-24

Key words: privacy protection; reversible data hiding; encrypted images; adaptive encoding; prediction error

过去的几十年间, 随着数字媒体技术不断发展并日益完善, 用于数字媒体保护的技术[1,2]层出不穷. 国家商务部、科技部在近期调整发布的《中国禁止出口限制出口技术目录》(商务部科技部公告 2020 年第 38 号)中新增“信息防御技术”作为限制出口技术, 信息隐藏与发现技术为其控制要点, 表明信息隐藏在信息安全中起至关重要的作用. 传统的信息隐藏技术可以被划分为 3 类, 分别为数字水印、隐写与隐写分析以及可逆信息隐藏. 数字水印[3,4]在不影响原数字作品使用价值的情况下嵌入信息, 被广泛用于版权保护、完整性认证等安全领域. 鲁棒性是数字水印的重要属性, 表示经过各种攻击, 如去除攻击、几何攻击后仍能提取且验证水印信息的能力. 隐写[5−7]以数字媒体内容为载体实施隐蔽通信, 侧重不可感知性, 即隐写行为既不会被人眼感知, 也难以被各种隐写分析[1,8]算法检测. 不同于数字水印和隐写, 早期的可逆信息隐藏[9,10]主要用于明文域, 载体信号嵌入信息后仍能可逆恢复为原始内容, 不影响图像质量. 率失真性能[11]为三者共同的评价指标, 其要求在获得同等嵌入率情况下, 尽可能减少图像失真.

明文域可逆信息隐藏不断发展及完善, 现有的方法主要包括无损压缩[12,13]、差值扩展[14,15]及直方图平移[9,16], 这些方法极大地提高了可逆信息隐藏的性能. 但明文域可逆信息隐藏方法嵌入信息后, 得到的是与原载体极为相似的图像, 图像内容存在被泄露的风险, 这在一些敏感领域中是不被允许的. 例如: 医疗诊断中, 患者隐私的泄露会给患者带来不便; 军事图像中, 国家机密的暴露会造成难以挽回的局面. 图像加密是一种对载体信号进行加密的技术, 能够保护个人隐私, 非法操作者难以在加密图像中获取有价值的信息. 基于此, 人们提出将图像加密与信息隐藏方法共同作用, 即图像所有者使用密钥加密原始载体信号, 信息隐藏者在加密图像中嵌入信息, 最后合法接收者根据密钥提取信息或恢复图像. 这种密文可逆信息隐藏(reversible data hiding in encrypted images, RDHEI)方法[17−19]近年来受到人们的广泛关注, 该方法对于云存储中隐私保护有良好的应用前景, 也可以被应用于医疗、军事图像传输和存储以及法庭取证等场景中.

根据加密与腾出空间步骤的发生次序, RDHEI 方法可以被划分为两大类: 加密后腾出空间(vacating room after encryption, VRAE)以及加密前预留空间(reserving room before encryption, RRBE). VRAE[20−23]的方法利用加密后图像冗余嵌入信息. 文献[20]提出一种分块的图像加密算法, 通过翻转图像块中像素的 3 个最低有效位(least significant bit, LSB), 进行额外信息的嵌入和提取. 通过利用自然图像的像素相关性, 该算法能够成功地提取嵌入信息, 并很好地恢复原始图像. 但是当图像分块过小时, 可能会在图像的非平滑区域中错误提取信息. 文献[22]提出一种可分离的 VRAE 算法, 通过压缩加密图像的低位有效位, 来创建可嵌入信息的稀疏空间. 在该算法中, 嵌入信息的提取和图像恢复能够可分离地进行, 进一步拓宽了 RDHEI 的应用场景. 文献[23]介绍了一种新的 RDHEI 框架, 在该算法中, 图像被分块加密, 加密后分块中仍保留像素相关性, 因此, 大多数明文域可逆信息隐藏方法可用于加密后图像中腾出空间. 该方法也进一步证明了: 保留图像像素间相关性, 对创建用于信息嵌入的空间至关重要.

上述 VRAE 方法先加密图像后腾出空间, 由于加密后图像冗余较低, 导致该方法的嵌入容量受限且在图像恢复过程中存在一定误码率. 不同于 VRAE 方法, RRBE[24−27]方法首先对图像预处理预留出空间, 随后加密图像, 能够达到与 VRAE 方法相同的保护载体信息的效果. 文献[24]首次提出了 RRBE 算法, 实现了信息的正确提取和图像的无损恢复. 随后, 文献[25]提出利用预测误差直方图移位在加密前图像中预留空间, 同时根据不同场景的需求分别从加密图像和解密图像中提取嵌入的信息. 文献[26]首次采用对像素的最高有效位(most significant bit, MSB)进行预测的算法. 由于 RDHEI 算法在加密域中不考虑图像视觉质量的损失, 选取比 LSB 更易预测的 MSB 嵌入信息不会产生影响; 此外, 该算法显著提升了 RDHEI 的嵌入容量. 受 MSB 预测方法的启发, 对多 MSB 进行操作的方法随之而来. 文献[27]介绍了一种基于多 MSB 预测和哈夫曼编码的算法, 该算法将原始像素与预测值的二进制序列进行比较, 记录从 MSB 到 LSB 的相同比特数, 并采用哈夫曼编码标记像素, 进一步提升了 RDHEI 算法的嵌入性能. 该算法对多 MSB 预测的同时还考虑到对像素进行标记, 这种标记像素的算法近年来也受到研究者的关注.

文献[28]提出一种采用参数二叉树编码标记像素的 RDHEI 算法，通过利用二叉树编码标记像素来实现在像素的非标记位嵌入信息. 文献[29]扩展了参数二叉树标记的算法，对其改进后，利用图像整体像素相关性预留空间，进一步提升了嵌入容量. 文献[30]提出了一种基于像素预测和位平面压缩的 RDHEI 算法，该算法首先计算原始图像的预测误差，然后利用预测误差间的冗余对其进行位平面压缩. 该算法不仅能够无损地恢复原始图像，还大大提高了嵌入容量. 与利用加密前原始图像预留空间的 RDHEI 算法相比，对加密前的预测误差进行处理能够获得更高的嵌入容量，为在图像中嵌入信息提供更充足的空间. 这是由于原始图像的空间冗余存在一定限制，而图像对应的预测误差波动范围相对较小，因此利用预测误差预留空间能达到很好的效果.

文献[29]采用定长编码标记预测误差不同的像素，该算法能够获得较高嵌入容量，但其未考虑原始图像预测误差的分布特性. 基于此，本文对文献[29]进行改进，提出一种自适应编码的高容量 RDHEI 算法. 本文使用自适应生成的变长哈夫曼编码标记预测误差不同的像素，还采用冗余性更高的预测误差图像作为媒介，结合哈夫曼编码标记加密后图像像素，以此来预留空间. 在本文所提算法中，首先计算整张图像的预测误差，根据其不同出现概率进行哈夫曼编码. 生成的哈夫曼编码码字被用来标记加密后像素，标记剩余位则用于嵌入额外信息. 与文献[29]相比，本文采用自适应哈夫曼编码来标记像素，结合了每张图像自身的纹理特性，充分利用了图像冗余，获得了更高的嵌入容量.

本文第 1 节描述自适应编码的高容量 RDHEI 算法的研究框架，介绍不同角色的作用. 然后，在第 2 节详细展示本文所提出的 RDHEI 算法，主要从预测误差计算、哈夫曼编码和标记、额外信息嵌入以及信息提取和图像恢复进行介绍. 第 3 节展示本文所提算法的实验部分，并对实验数据进行分析与解释. 最后总结全文，对本文存在的不足之处和未来值得进一步探索的方向作简要说明.

1 研究框架

RDHEI 中主要包含 3 类角色，分别为图像所有者、信息隐藏者以及图像接收者：图像所有者掌握原始图像信息并对其加密以保护图像内容；信息隐藏者在未经图像所有者许可时，无法获取原始图像信息，但却能在加密图像中嵌入必要的额外信息；图像接收者接收到信息隐藏者处理后的图像，执行信息提取或图像恢复的操作.

不同图像的纹理特性存在差别，相应地，其预测误差分布也不尽相同. 为了充分利用图像自身特性，本文提出一种自适应编码的高容量 RDHEI 算法，如图 1 所示.

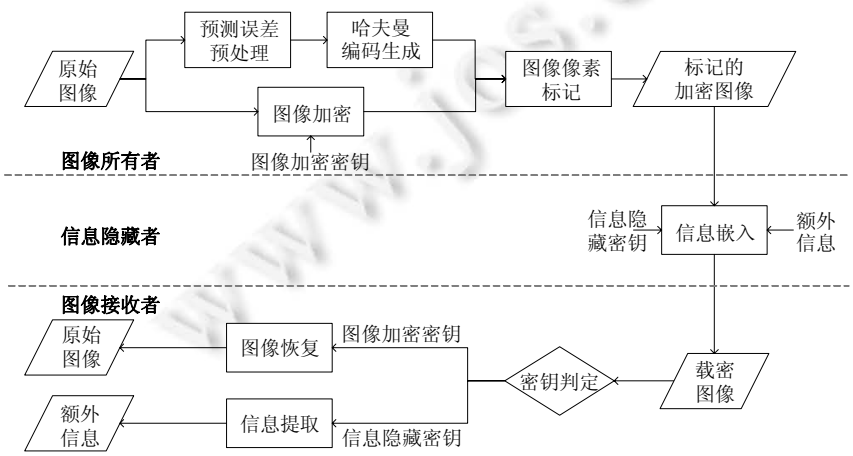


图 1 所提 RDHEI 算法的框架

本文算法主要分为以下 3 个步骤.

(1) 图像所有者对原始图像进行预处理以及加密操作. 图像所有者首先预处理原始图像，一方面计算图

像的预测误差并按照其出现概率进行哈夫曼编码, 另一方面直接对原始图像进行加密获得加密图像. 加密图像像素按照其预测误差对应的哈夫曼码字, 以位替换的方式标记, 得到标记的加密图像;

(2) 信息隐藏者嵌入额外信息得到载密图像. 标记的加密图像像素的非标记位为预留空间, 信息隐藏者无法获得原始图像的信息, 直接以位替换的方式将额外信息嵌入到预留空间中, 获得载密图像. 为了确保额外信息的安全性, 对其使用信息隐藏密钥加密;

(3) 图像接收者提取嵌入的信息或恢复原始图像. 图像接收者接收载密图像后, 根据其拥有的密钥种类和需求执行信息提取或图像恢复操作.

2 自适应编码的高容量 RDHEI 算法

本节对提出算法的细节进行描述. 在第 1 阶段中, 图像所有者计算图像预测误差, 具体过程在第 2.1 节中描述. 第 2.2 节根据预测误差的出现概率自适应生成哈夫曼编码, 并对采用图像加密密钥加密后的像素按照其预测误差对应的哈夫曼码字进行标记, 得到标记的加密图像. 在第2阶段中, 信息隐藏者接收到标记的加密图像后, 在像素的非标记位嵌入加密后的额外信息, 生成载密图像, 详细操作见第 2.3 节. 最后, 第 2.4 节表明图像接收者获得载密图像后, 可以提取嵌入的信息或恢复图像.

2.1 预测误差计算

对于尺寸为 $m\times n$ 的灰度图像, 可采用中值边缘预测[31]方法计算其原始图像的预测值. $x(i,j)(2\leqslant i\leqslant m, 2\leqslant j\leqslant n)$为原始图像的一个像素值, 如图 2 所示, 选取像素 $x(i,j)$左方、上方以及左上方这 3 个像素为参考值, 计算其预测值 $p(i,j)$:

$$p(i,j)=\begin{cases}\max(x_2,x_3), & x_1\leqslant \min(x_2,x_3)\\ \min(x_2,x_3), & x_1\geqslant \max(x_2,x_3)\\ x_2+x_3-x_1, & \text{others}\end{cases} \tag{1}$$

计算原始图像的预测值时, 第 1 行及第 1 列像素作为参考像素不做任何操作. 从第 2 行第 2 列像素开始, 按照上述操作计算像素预测值. 然后, 结合像素值 $x(i,j)$和其预测值 $p(i,j)$, 计算其预测误差 $e(i,j)=x(i,j)-p(i,j)$. 顺序扫描剩余像素, 计算整张图像的预测误差. 一方面, 中值边缘预测方法利用像素的邻近信息预测像素, 能够在低复杂度的情况下获得较为准确的像素预测值; 另一方面, 采用中值边缘预测方法便于图像恢复. 由于被预测像素邻近的 3 个像素为参考值, 且第 1 行与第 1 列像素得以保留, 在图像恢复时可以顺序扫描图像像素, 计算其预测值进而恢复图像.

X_1	X_3
X_2	X

图 2 采用中值边缘预测方法进行像素预测

2.2 哈夫曼编码和标记

为了能够结合图像自身纹理特性, 在图像中预留空间嵌入额外信息, 需要对图像的预测误差进行自适应哈夫曼编码. 哈夫曼编码的作用是标记像素, 并在标记时预留空间, 因此, 哈夫曼码字的长度不能超过 8 位. 为了满足这一限制条件, 需要对预测误差的出现概率进行预处理. 假设哈夫曼编码表中码字长度均为 8, 此时对应的编码表为满足限制条件时能得到码字最多的情况. 记录此时哈夫曼编码码字的平均出现概率为分区阈值, 用于初始分类可进行哈夫曼编码的预测误差. 图 3 为所有哈夫曼码字长度均为 8 时对应的哈夫曼树, 此时每个码字的平均概率为 1/256, 记为初始分区阈值, 用于预测误差预处理. 出现概率低于分区阈值的预测误差记为一种情况, 计算这些预测误差出现概率之和. 出现概率高于分区阈值的预测误差划分为 s(s 取值由分区阈值内预测误差数量决定)种情况. 最后, 根据此时的 s+1 种预测误差对应的出现概率进行哈夫曼编码.

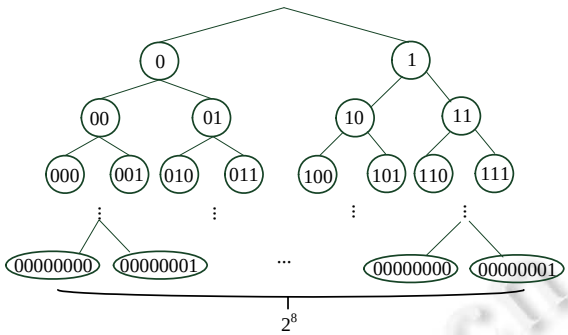


图 3 哈夫曼编码长度均为 8 位时对应的哈夫曼树

判断当前生成的哈夫曼编码是否满足限制条件. 若不满足, 则调整 s 为 s–2, 缩小预测误差范围继续编码, 直到满足限制条件, 得到最终的分区阈值, 获取符合图像纹理特性的哈夫曼编码.

编码过程中, 像素被划分为 3 种类型: 参考像素、不可嵌入像素以及可嵌入像素. 参考像素为第一行与第一列像素, 不进行任何操作; 剩余像素按照分区阈值被划分为不可嵌入像素和可嵌入像素. 不可嵌入像素为预测误差出现概率低于分区阈值的像素, 进行哈夫曼编码时视为同一种情况, 对应一种哈夫曼编码码字. 可嵌入像素为预测误差出现概率高于分区阈值的像素, 可在其中嵌入额外信息, 预测误差不同的可嵌入像素对应不同哈夫曼编码码字.

为了保护图像原始信息, 标记像素前需要采用图像加密密钥加密图像. 图像加密时, 根据图像加密密钥生成一个与原始图像大小相同的 $m\times n$ 伪随机矩阵 H, $h(i,j)$为 H 中像素值. 然后将原始图像像素值 $x(i,j)$与对应位置的像素值 $h(i,j)$转换为八位二进制数表示, 具体转换操作如公式(2)所示, *floor* 为向下取整函数, mod 代表求余函数, k 为二进制数对应的位数. 转换后的 $x(i,j)$与 $h(i,j)$, 按照公式(3)进行异或操作实现加密, ⊕代表异或操作. 然后, 将加密后二进制数按照公式(4)操作转换为十进制, 即得到加密后像素值. 依次加密所有像素, 得到加密图像:

$$y^k(i,j)=\left[\ floor\left(\frac{y(i,j)}{2^{k-1}}\right)\right]\ \bmod\ 2,\ k=1,2,...,8 \tag{2}$$

$$x_e^k(i,j)=x^k(i,j)\oplus h^k(i,j),\ k=1,2,...,8 \tag{3}$$

$$x_e(i,j)=\sum_{k=1}^{8}x_e^k(i,j)\times 2^{k-1},\ k=1,2,...,8 \tag{4}$$

图像加密完成后, 对加密后像素进行哈夫曼编码标记. 根据像素种类的不同, 对其标记时的操作也有所区别. 参考像素不进行标记, 其信息记录为辅助信息; 不可嵌入像素根据其对应的哈夫曼码字进行位替换标记, 被替换下的信息同样记录为辅助信息; 可嵌入像素根据其预测误差对应的不同哈夫曼码字进行标记, 每个可嵌入像素的非标记位为预留空间, 可用于嵌入额外信息. 完成标记后, 将哈夫曼编码规则转换为二进制比特流, 以位替换的方式存储在原参考像素位置, 辅助信息同样以位替换的方式嵌入可嵌入像素的预留空间中, 便于后续信息嵌入或提取.

图 4 截取了部分 Lena 图像, 简要说明像素标记全过程. 图 4(a)为截取的原始图像, 第 1 行与第 1 列像素为参考像素; 根据第 2.1 节中预测误差计算方法, 计算得到如图 4(b)所示的预测误差, 将此时的预测误差预处理后进行哈夫曼编码得到如表 1 所示的哈夫曼编码表, 表头和表尾省略部分编码表信息; 图 4(c)为加密图 4(a)后的加密图像; 按照表 1 所示哈夫曼编码表以位替换的方式标记加密图像, 得到图 4(d), 加粗信息为当前像素对应的哈夫曼标记位, 剩余位代表预留空间, 可在其中嵌入信息; 由于相邻像素的预测误差往往差别较小, 为了防止泄露图像信息, 对标记后的图像进行翻转, 得到如图 4(e)所示的标记的加密图像.

162	162	162	161
162	162	162	161
162	162	162	161
162	162	162	161

(a) 原始图像

162	162	162	161
162	0	0	0
162	0	0	0
162	0	0	0

(b) 预测误差

00100001(33)	11100010(226)	10010010(146)	10101101(173)
11010111(215)	01111010(122)	10001110(142)	10011101(157)
11111011(251)	00101000(40)	01001001(73)	00101100(44)
10111010(186)	10100001(161)	00100100(36)	00010001(17)

(c) 加密图像

00100001(33)	11100010(226)	10010010(146)	10101101(173)
11010111(215)	**100**11010(154)	**100**01110(142)	**100**11101(157)
11111011(251)	**100**01000(136)	**100**01001(137)	**100**01100(140)
10111010(186)	**100**00001(129)	**100**00100(132)	**100**10001(145)

(d) 对加密图像进行哈夫曼标记

10000100(132)	01000111(71)	01001001(73)	10110101(181)
11101011(235)	01011**001**(89)	01110**001**(113)	10111**001**(185)
11011111(223)	00010**001**(17)	10010**001**(145)	00110**001**(49)
01011101(93)	10000**001**(129)	00100**001**(33)	10001**001**(137)

(e) 标记的加密图像

图 4 像素标记过程示意图

表 1 哈夫曼编码表

预测误差	哈夫曼编码
…	…
−5	[0,1,0,0,1]
−4	[1,1,0,1]
−3	[0,1,1,0]
−2	[0,0,1,0]
−1	[0,0,0,0]
0	[1,0,0]
1	[1,1,1]
2	[0,0,0,1]
3	[0,1,0,1]
4	[1,1,0,0]
5	[0,1,0,0,0]
…	…

2.3 额外信息嵌入

在标记的加密图像中, 假设辅助信息共 l 比特, 存在 t 个可嵌入像素$\{x_1,x_2,x_3,\ldots,x_t\}$, 每个可嵌入像素 x_p ($1\leqslant p\leqslant t$)分别采用 n_p($n_p\leqslant 8$)比特哈夫曼码字标记, 预留出 $8-n_p$ 比特空间. 净嵌入容量 c(比特)可以根据所有可嵌入像素预留空间总数减去辅助信息所占空间计算:

$$c=\sum_{p=1}^{t}(8-n_p)-l \tag{5}$$

信息隐藏者获得标记的加密图像后, 获取参考像素位置存储的哈夫曼编码规则, 根据其异字头码字的特性定位到图中的可嵌入像素, 获得净预留空间的位置, 最后以位替换的方式将额外信息嵌入到净预留空间中, 生成载密图像. 为了确保额外信息的内容不被泄露, 在将额外信息嵌入到标记的加密图像前, 需要加密额外信息, 加密方法与第 2.2 节中图像加密方法相同, 但采用的加密密钥为信息隐藏密钥.

2.4 信息提取或图像恢复

在信息提取或图像恢复时, 图像接收者在参考像素位置提取并获得哈夫曼编码, 定位所有可嵌入像素, 提取其中嵌入的信息. 提取出的信息由两部分组成: l 比特辅助信息和加密后的额外信息. 图像接收者根据拥有密钥的不同, 对提取的信息和载密图像做不同处理, 主要可分为以下 3 种类型.

(1) 只拥有图像加密密钥: 当图像接收者只拥有图像加密密钥时, 能够无损地恢复图像. 图像接收者将提取的辅助信息还原到相应位置, 得到加密后的参考像素值以及不可嵌入像素值, 然后使用图像加密密钥解密图像, 此时图像的参考像素值和不可嵌入像素值均已恢复为原始状态. 利用哈夫曼码字对应的预测误差, 获得可嵌入像素的预测误差值, 由公式(1)计算得到可嵌入像素的预测值. 最后, 结合预测值和预测误差恢复可嵌入像素. 经过上述操作, 载密图像即恢复为原始图像;

(2) 只拥有信息隐藏密钥: 当图像接收者只拥有信息隐藏密钥时, 能够正确提取嵌入的额外信息. 图像接收者将提取出的额外信息采用信息隐藏密钥解密, 得到原始的额外信息;

(3) 同时拥有图像加密密钥和信息隐藏密钥: 当图像接收者同时拥有图像加密密钥和信息隐藏密钥时, 既可以正确提取并恢复额外信息, 也可以无损恢复原始图像. 在信息提取和图像恢复的过程中, 二者互不影响, 因此该算法的信息提取和图像恢复是可分离的.

3 实验结果和分析

为了验证所提算法的可行性, 本节设计了大量的实验并分析实验结果. 如图 5 所示, 本文使用 5 张常规灰度图像进行实验对比, 验证该算法的性能. 为了减少随机选取图像的纹理复杂度对实验产生影响, 本文还在 UCID[32], BOSSBase[33]和 BOWS-2[34]这 3 个图像集中测试了不同算法的性能. 由于 RDHEI 算法对载密图像的图像质量不做要求, 因此嵌入性能成为衡量该算法的重要指标. 实验采用嵌入率(embedding rate, ER)为关键指标衡量嵌入性能, 其含义为每像素嵌入的比特数(bit per pixel, bpp), 可嵌入额外信息的最大值被用于计算图像嵌入率. 此外, 本文还采用了常用指标均方差(mean square error, MSE)和结构相似性(structural similarity, SSIM)来检验该算法的可逆性.

(a) Peppers (b) Lena (c) Lake (d) Baboon (e) Tiffany

图 5 5 张常规测试图像

3.1 可逆性分析

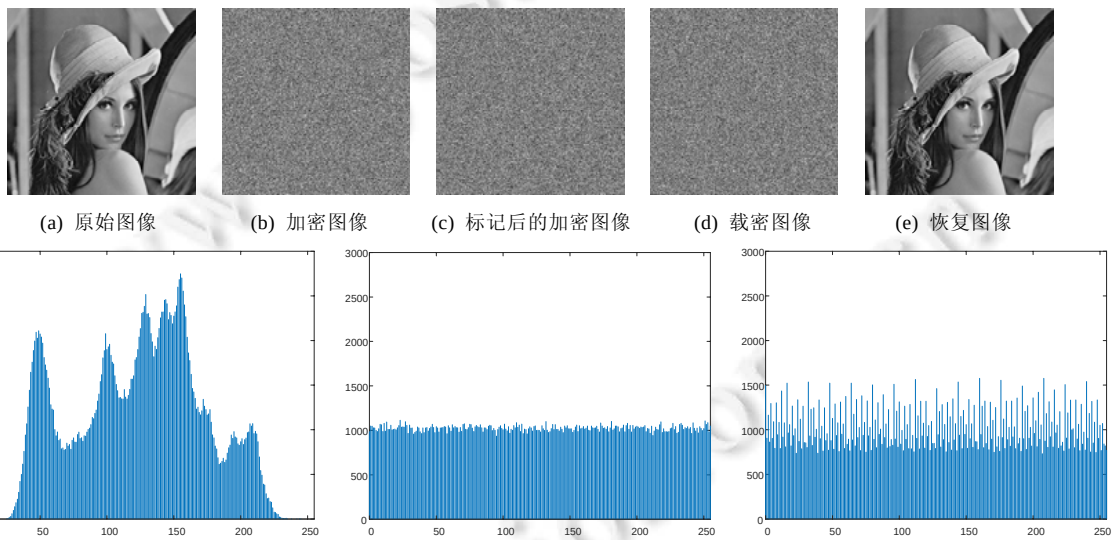
为了验证所提算法能够可逆地提取信息或恢复图像, 本节进行了关于可逆性的分析. 在信息提取或图像恢复时, 根据哈夫曼编码异字头码字的特性并结合哈夫曼编码规则, 可以获取像素的预测误差, 结合参考像素值和不可嵌入像素值, 可以无损地恢复图像信息. 本文在 UCID[32], BOSSBase[33]和 BOWS-2[34]这 3 个图像集进行测试, 以验证该算法图像恢复的可逆性. 实验结果如表 2 所示: 图像集的 MSE 均为‘0’, 说明恢复图像与原始图像像素没有任何区别; 同时, 恢复图像与原始图像的 SSIM 为‘1’, 代表两种图像的结构相同. 即, 该算法能够可逆地恢复原始图像. 第 2.4 节介绍了所提算法的信息提取过程, 图像接收者定位所有可嵌入像素, 并提取其中嵌入的信息. 在这个过程中, 嵌入的信息都能被完好无损地提取并恢复, 说明本文算法能够实现信息提取的可逆性. 在本文算法中, 信息提取和图像恢复的过程互不影响, 均可独立完成, 进一步证实了该算法信息提取或图像恢复不仅是可逆的, 也是可分离的.

表 2 原始图像集和恢复图像集的 MSE 及 SSIM

	UCID	BOSSBase	BOWS-2
MSE	0	0	0
SSIM	1	1	1

3.2 安全性分析

作为一种自适应编码的高容量 RDHEI 算法, 本文既要保护原始图像内容不被泄露, 也要保护嵌入在图像中的额外信息. 为了证明该算法的安全性, 本节分析了加密算法并对比了不同状态下图像像素特征图. 第 2.2 节介绍了本文采用图像加密密钥进行加密, 对任意尺寸为 $m\times n$ 的灰度图像, 其图像加密密钥对应的伪随机矩阵 H 中所有像素转换为 8 位二进制数表示后共有 $8\times m\times n$ 比特‘0’或‘1’, 则图像加密密钥存在的可能性为 $2^{8\times m\times n}$ 种, 因此在图像加密密钥未知的情况下, 试图预测正确的伪随机矩阵难度较大. 同样的, 假设在标记的加密图像中嵌入 g 比特额外信息, 则信息隐藏密钥生成的伪随机序列有 2^g 种存在的可能性, 完整地获取经过信息隐藏密钥加密后的额外信息也难以实现. 两种密钥的存在, 使非法用户难以获取图像明文信息和嵌入的额外信息. 图 6 对不同状态图像像素特征的分析进一步证实了本文算法的安全性. 图 6(a)为原始 Lena 图像, 加密后得到加密图像图 6(b), 使用哈夫曼编码标记加密图像得到图 6(c)所示标记后的加密图像, 在图 6(c)中嵌入额外信息得到载密图像图 6(d), 最后进行信息提取和图像恢复, 获得恢复图像图 6(e). 图 6(f)是原始图像的像素分布直方图, 图 6(g)为加密图像的像素分布直方图, 其像素分布平缓, 难以获得有意义的图像特征信息. 图 6(h)为标记的加密图像像素分布直方图, 与图 6(g)相比, 该直方图部分像素的数量增长, 但像素整体分布依旧杂乱无章, 无法据此获取原始图像信息. 这意味着本文所提的 RDHEI 算法在安全性方面得到了保障.



(a) 原始图像 (b) 加密图像 (c) 标记后的加密图像 (d) 载密图像 (e) 恢复图像

(f) 原始图像直方图 (g) 加密图像直方图 (h) 标记的加密图像直方图

图 6 不同状态的图像像素特征表示

3.3 性能对比

本文采用自适应哈夫曼编码标记像素的方法改进文献[29]中的算法, 充分利用了图像的纹理特性, 获得更高的嵌入率. 在本文算法中, 可嵌入像素的非标记位用于嵌入信息. 第 2.3 节中公式(5)介绍了净嵌入容量 c 的计算方法, 结合公式(5)可计算图像的嵌入率 $ER=c/(m\times n)$ (bpp). 表 3 从多方面对比文献[29]与本文算法的性能, 与文献[29]相比, 本文算法的可嵌入像素增多, 不能用于预留空间的辅助像素(参考像素以及不可嵌入像素)数量减少, 像素利用率有一定程度的增大, 图像嵌入率得到了明显的提升. 这里的像素利用率用可嵌入像素所占比例表示. 由于载体图像的像素数固定, 本文算法使用更多可嵌入像素用于预留空间, 且本文还采用了自适应哈夫曼编码对图像像素进行标记, 对于出现概率较高的预测误差对应的像素采用较短的哈夫曼码字标记, 充分利用了图像自身的特性, 预留出更多可嵌入空间.

表 3 本文与文献[29]中算法的性能对比

测试图像	算法	可嵌入像素	辅助像素	像素利用率=可嵌入像素数量/图像总像素量(%)	$ER=c/(m\times n)$ (bpp)
Lena	文献[29]	243 107	19 037	92.7	2.645
	本文算法	246 614	15 530	94.1	3.262
Baboon	文献[29]	155 266	106 878	59.2	0.969
	本文算法	225 530	36 614	86.0	1.481
Tiffany	文献[29]	243 463	18 681	92.9	2.652
	本文算法	245 814	16 330	93.8	3.376
Peppers	文献[29]	235 184	26 960	89.7	2.494
	本文算法	249 882	12 262	95.3	2.910
Lake	文献[29]	209 185	52 959	79.8	1.998
	本文算法	243 183	18 961	92.8	2.409

另外，为了更充分说明本文算法的性能提升，本文与目前性能较高的几种同类算法[26,28−30]进行了嵌入性能对比. 文献[26]在单 MSB 中嵌入信息，图像嵌入率接近 1bpp. 文献[28]采用参数二叉树编码的方法标记图像像素，提高了图像的嵌入性能. 文献[29]采用改进的参数二叉树编码标记更多可嵌入像素，使图像嵌入率得到了很大的提升. 文献[30]利用预测误差位平面存在众多相似位的特性，结合预测误差压缩图像位平面，进一步提升了图像嵌入率. 如图 7 所示，本文首先比较图 5 中测试图像的嵌入率大小. Baboon 图像的嵌入率在所有算法中都明显低于其他几张图像，这是由于 Baboon 图像纹理更加复杂，空间冗余度较低. 表 3 中可以观察到: 在本文算法中, Baboon 图像中存在 36 614 个辅助像素，多于其他测试图像，但本文算法中 Baboon 图像的嵌入率仍高于其他算法. 另外 4 张测试图像的实验结果同样表明: 本文所提算法与同类算法相比，均能获得更高的图像嵌入率.

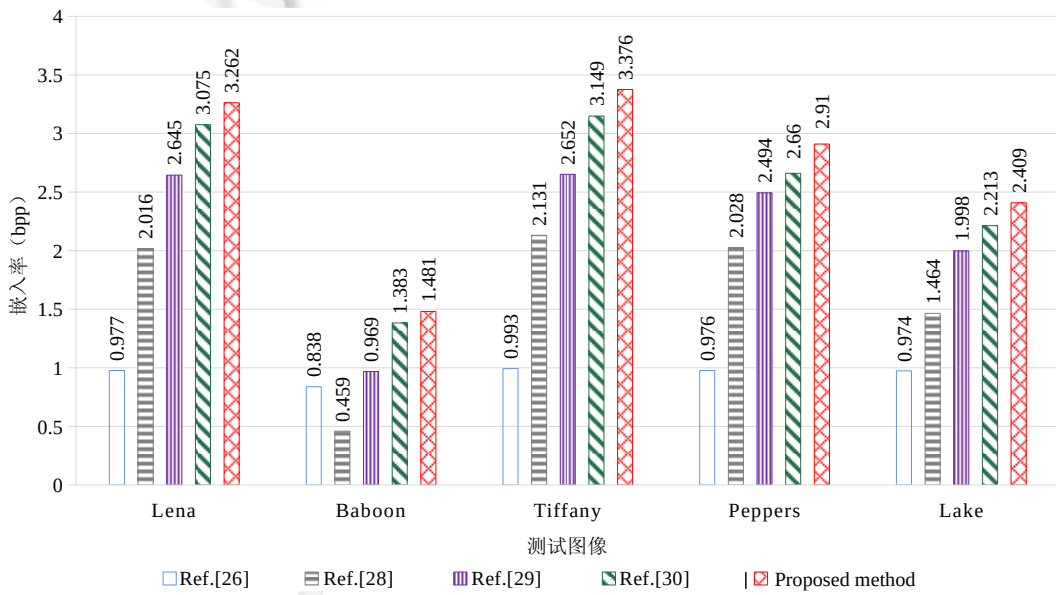


图 7 不同算法在 5 幅测试图像上的嵌入率(bpp)

为了验证这种性能提升并不是偶然事件，本文还在 UCID[32]，BOSSBase[33]以及 BOWS-2[34]图像集上进行了对比实验. 通过比较本文算法与同类算法在 3 个图像集上的平均嵌入率，验证该算法的有效性. 如图 8 所示，本文算法均获得了最高的平均嵌入率. 在 UCID[32]，BOSSBase[33]以及 BOWS-2[34]图像集上分别达到了 3.162 bpp, 3.917 bpp 以及 3.775 bpp. 相比于同类算法，本文算法的平均嵌入率有了明显提升，即使与性能最佳的文献[30]相比，本文算法的平均嵌入率仍提升了 0.263 bpp, 0.292 bpp 以及 0.280 bpp. 与其他算法相比，本文算法采用自适应哈夫曼编码对预测误差不同的像素进行标记，结合哈夫曼编码构造平均长度最短的码字特

性, 充分利用了图像自身的纹理特性, 得到了最佳的图像嵌入性能.

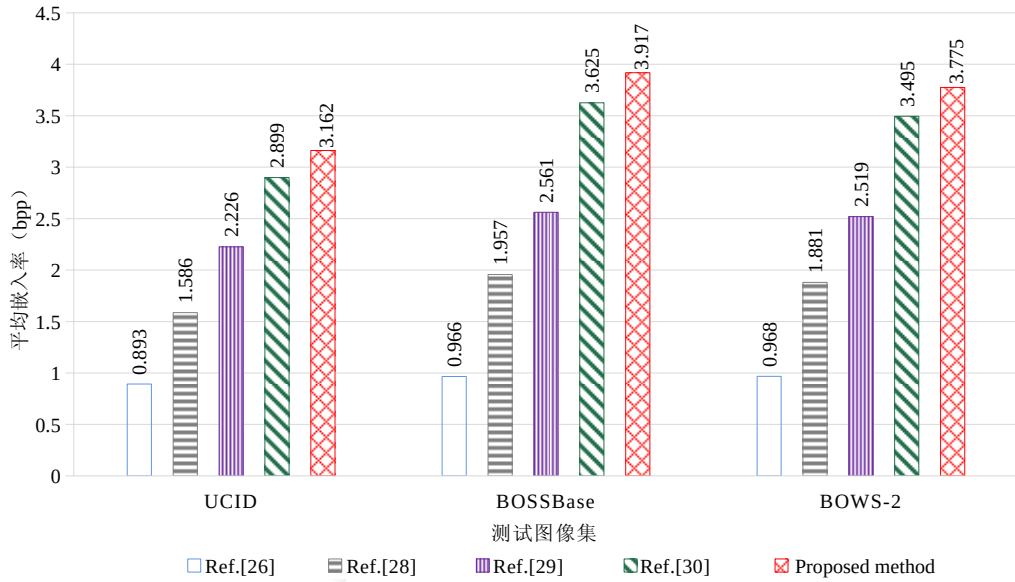


图 8 不同算法在 3 个图像集中的平均嵌入率(bpp)

4 总 结

密文图像可逆信息隐藏在隐私保护中起重要作用, 嵌入性能是衡量该方法的重要指标. 本文对文献[29]进行改进, 提出一种自适应编码的高容量 RDHEI 算法. 该算法使用变长哈夫曼编码标记预测误差不同的像素, 充分利用了图像自身的纹理特性. 相较于文献[29]中的等长编码, 本文的自适应哈夫曼编码更加灵活, 能获得平均码字最短的编码; 同时, 按照预测误差出现概率标记像素, 可标记更多像素, 预留更多可嵌入空间. 经实验验证, 本文算法能够正确地提取信息并无损恢复图像. 与同类算法相比, 本文提出的算法能够得到较高的嵌入率, 为存储更多额外信息提供了充足的空间. 但是, 本文算法在像素标记过程中仍然存在一些不可嵌入像素, 无法在这些像素中完成预留空间操作. 在未来, 可以尝试不断提升可嵌入像素数量的方法, 也可以探寻新的预测器, 产生波动范围更小的预测误差, 获得更多可嵌入像素, 从而进一步提升嵌入性能.

References:

[1] Shen J, Liao X, Qin Z, *et al*. Spatial steganalysis of low embedding rate based on convolutional network. Ruan Jian Xue Bao/Journal of Software, 2021, 32(9): 2901−2915 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5980.htm [doi: 10.13328/j.cnki.jos. 005980]

[2] Li XR, Ji SL, Wu CM, *et al*. Survey on deepfakes and detection techniques. Ruan Jian Xue Bao/Journal of Software, 2021, 32(2): 496−518 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6140.htm [doi: 10.13328/j.cnki.jos.006140]

[3] Xiang SJ, Yang L. Robust and reversible image watermarking algorithm in homomorphic encrypted domain. Ruan Jian Xue Bao/Journal of Software, 2018, 29(4): 957−972 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5406.htm [doi: 10.13328/j.cnki.jos.005406]

[4] Chen HP, Qin J, Shen XJ, *et al*. Robust watermarking algorithm based on the feature of digital image. Computer Science, 2011, 38(5): 258−260, 264 (in Chinese with English abstract). [doi: 10.3969/j.issn.1002-137X.2011.05.063]

[5] Tang WX, Li B, Barni M, *et al*. An automatic cost learning framework for image steganography using deep reinforcement learning. IEEE Trans. on Information Forensics and Security, 2020, 16: 952−957. [doi: 10.1109/TIFS.2020.3025438]

[6] Wu JQ, Zhai LM, Wang LN, *et al*. Enhancing spatial steganographic algorithm based on multi-scale filters. Journal of Computer Research and Development, 2020, 57(11): 2251−2259 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2020.20200441]

[7] Ma S, Zhao XF. Steganalytic feature based adversarial embedding for adaptive JPEG steganography. Journal of Visual Communication and Image Representation, 2021, 103066. [doi: 10.1016/j.jvcir.2021.103066]

[8] Chen JF, Fu ZJ, Zhang WM, *et al*. Review of image steganalysis based on deep learning. Ruan Jian Xue Bao/Journal of Software, 2021, 32(2): 551−578 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6135.htm [doi: 10.13328/j.cnki.jos.006135]

[9] Ni ZC, Shi YQ, Ansari N, *et al*. Reversible data hiding. IEEE Trans. on Circuits and Systems for Video Technology, 2006, 16(3): 354−362. [doi: 10.1109/TCSVT.2006.869964]

[10] Shi YQ, Li XL, Zhang XP, *et al*. Reversible data hiding: Advances in the past two decades. IEEE Access, 2016, 4: 3210−3237. [doi: 10.1109/ACCESS.2016.2573308]

[11] Kalker TON, Willems FMJ. Capacity bounds and constructions for reversible data-hiding. In: Proc. of the 2002 14th Int'l Conf. on Digital Signal Processing Proceedings. IEEE, 2002. 71−76. [doi: 10.1109/ICDSP.2002.1027818]

[12] Zhang WM, Hu XC, Li XL, *et al*. Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression. IEEE Trans. on Image Processing, 2013, 22(7): 2775−2785. [doi: 10.1109/TIP.2013.2257814]

[13] Qin C, Hu YC. Reversible data hiding in VQ index table with lossless coding and adaptive switching mechanism. Signal Processing, 2016, 129: 48−55. [doi: 10.1016/j.sigpro.2016.05.032]

[14] Tian J. Reversible data embedding using a difference expansion. IEEE Trans. on Circuits and Systems for Video Technology, 2003, 13(8): 890−896. [doi: 10.1109/TCSVT.2003.815962]

[15] Kim HJ, Sachnev V, Shi YQ, *et al*. A novel difference expansion transform for reversible data embedding. IEEE Trans. on Information Forensics and Security, 2008, 3(3): 456−465. [doi: 10.1109/TIFS.2008.924600]

[16] Wang JX, Chen X, Ni JQ, *et al*. Multiple histograms-based reversible data hiding: Framework and realization. IEEE Trans. on Circuits and Systems for Video Technology, 2019, 30(8): 2313−2328. [doi: 10.1109/TCSVT.2019.2915584]

[17] Chen YC, Hung TH, Hsieh SH, *et al*. A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms. IEEE Trans. on Information Forensics and Security, 2019, 14(12): 3332−3343. [doi: 10.1109/TIFS.2019.2914557]

[18] Zhang XP, Long J, Wang ZC, *et al*. Lossless and reversible data hiding in encrypted images with public-key cryptography. IEEE Trans. on Circuits and Systems for Video Technology, 2015, 26(9): 1622−1631. [doi: 10.1109/TCSVT.2015.2433194]

[19] Xiang SJ, Luo XR. Reversible data hiding in encrypted image based on homomorphic public key cryptosystem. Ruan Jian Xue Bao/Journal of Software, 2016, 27(6): 1592−1601 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5007.htm [doi: 10.13328/j.cnki.jos.005007]

[20] Zhang XP. Reversible data hiding in encrypted image. IEEE Signal Processing Letters, 2011, 18(4): 255−258. [doi: 10.1109/LSP.2011.2114651]

[21] Qin C, Zhang W, Cao F, *et al*. Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection. Signal Processing, 2018, 153: 109−122. [doi: 10.1016/j.sigpro.2018.07.008]

[22] Zhang XP. Separable reversible data hiding in encrypted image. IEEE Trans. on Information Forensics and Security, 2011, 7(2): 826−832. [doi: 10.1109/TIFS.2011.2176120]

[23] Huang FJ, Huang JW, Shi YQ. New framework for reversible data hiding in encrypted domain. IEEE Trans. on Information Forensics and Security, 2016, 11(12): 2777−2789. [doi: 10.1109/TIFS.2016.2598528]

[24] Ma KD, Zhang WM, Zhao XF, *et al*. Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. on Information Forensics and Security, 2013, 8(3): 553−562. [doi: 10.1109/TIFS.2013.2248725]

[25] Zhang WM, Ma KD, Yu NH. Reversibility improved data hiding in encrypted images. Signal Processing, 2014, 94: 118−127. [doi: 10.1016/j.sigpro.2013.06.023]

[26] Puteaux P, Puech W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Trans. on Information Forensics and Security, 2018, 13(7): 1670−1681. [doi: 10.1109/TIFS.2018.2799381]

[27] Yin ZX, Xiang YZ, Zhang XP. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding. IEEE Trans. on Multimedia, 2020, 22(4): 874−884. [doi: 10.1109/TMM.2019.2936314]

[28] Yi S, Zhou YC. Separable and reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Trans. on Multimedia, 2019, 21(1): 51−64. [doi: 10.1109/TMM.2018.2844679]

[29] Wu YQ, Xiang YZ, Guo YT, *et al*. An improved reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Trans. on Multimedia, 2020, 22(8): 1929−1938. [doi: 10.1109/TMM.2019.2952979]

[30] Yin ZX, Peng YY, Xiang YZ. Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression. IEEE Trans. on Dependable and Secure Computing, 2020. [doi: 10.1109/TDSC.2020.3019490]

[31] Weinberger MJ, Seroussi G, Sapiro G. LOCO-I: A low complexity, context-based, lossless image compression algorithm. In: Proc. of the Data Compression Conf. (DCC'96). IEEE, 1996. 140−149. [doi: 10.1109/DCC.1996.488319]

[32] Schaefer G, Stich M. UCID: An uncompressed color image database. In: Yeung MM, ed. Proc. of the Storage and Retrieval Methods and Applications for Multimedia 2004, Vol.5307. 2003. 472−480. [doi: 10.1117/12.525375]

[33] Bas P, Filler T, Pevný T. "Break our steganographic system": The ins and outs of organizing BOSS. In: Filler T, ed. Proc. of the Int'l Workshop on Information Hiding. Springer, 2011. 59−70. [doi: 10.1007/978-3-642-24178-9_5]

[34] Bas P, Furon T. Image database of BOWS-2. 2017. http://bows2.ec-lille.fr/

附中文参考文献:

[1] 沈军, 廖鑫, 秦拯, 等. 基于卷积神经网络的低嵌入率空域隐写分析. 软件学报, 2021, 32(9): 2901−2915. http://www.jos.org.cn/1000-9825/5980.htm [doi: 10.13328/j.cnki.jos.005980]

[2] 李旭嵘, 纪守领, 吴春明, 等. 深度伪造与检测技术综述. 软件学报, 2021, 32(2): 496−518. http://www.jos.org.cn/1000-9825/6140.htm [doi: 10.13328/j.cnki.jos.006140]

[3] 项世军, 杨乐. 基于同态加密系统的图像鲁棒可逆水印算法. 软件学报, 2018, 29(4): 957−972. http://www.jos.org.cn/1000-9825/5406.htm [doi: 10.13328/j.cnki.jos.005406]

[4] 陈海鹏, 秦俊, 申铉京, 等. 基于图像特征的鲁棒性数字水印算法. 计算机科学, 2011, 38(5): 258−260, 264. [doi: 10.3969/j.issn.1002-137X.2011.05.063]

[6] 吴俊锜, 翟黎明, 王丽娜, 等. 基于多尺度滤波器的空域图像隐写增强算法. 计算机研究与发展, 2020, 57(11): 2251−2259. [doi: 10.7544/issn1000-1239.2020.20200441]

[8] 陈君夫, 付章杰, 张卫明, 等. 基于深度学习的图像隐写分析综述. 软件学报, 2021, 32(2): 551−578. http://www.jos.org.cn/1000-9825/6135.htm [doi: 10.13328/j.cnki.jos.006135]

[19] 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. 软件学报, 2016, 27(6): 1592−1601. http://www.jos.org.cn/1000-9825/5007.htm [doi: 10.13328/j.cnki.jos.005007]

马文静(1997－), 女, 硕士生, 主要研究领域为可逆信息隐藏.

吴友情(1984－), 女, 讲师, 主要研究领域为信息隐藏, 多媒体安全.

殷赵霞(1983－), 女, 博士, 副教授, 博士生导师, CCF 专业会员, 主要研究领域为信息隐藏, AI 安全, 多媒体内容保护.