基于预测误差位平面压缩的密文图像可逆信息隐藏

吴友情[1]，马文静[2]，殷赵霞[3]，彭银银[4]，张新鹏[5]

（1. 合肥师范学院计算机学院，安徽 合肥 230601；2. 安徽大学多模态认知计算安徽省重点实验室，安徽 合肥 230601；
3. 华东师范大学通信与电子工程学院，上海 200241；4. 合肥工业大学计算机与信息学院，安徽 合肥 230031；
5. 复旦大学计算机科学与技术学院，上海 200433）

摘 要：为进一步提升密文图像可逆信息隐藏算法性能，提出预测误差位平面联合编码无损压缩算法，可更充分地利用图像冗余，以预留更多可嵌入空间。图像所有者首先计算图像的预测误差，将预测误差位平面划分为相同大小的非重叠块，接着将其按块进行重新排列，利用游程编码和哈夫曼编码压缩重排后的比特流以预留空间。信息隐藏者在加密图像的预留空间中嵌入信息。在接收端，合法接收者能无损并可分离地提取信息和恢复图像。实验结果表明，所提算法充分利用位平面分布特性，获得了高嵌入性能，在 BOSSbase 和 BOWS-2 图像集中平均嵌入率达到 3.763 bpp 和 3.642 bpp，比同类算法至少提升 0.081 bpp 和 0.058 bpp。

关键词：密文图像可逆信息隐藏；预测误差；游程编码；哈夫曼编码；位平面

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022149

Reversible data hiding in encrypted image based on bit-plane compression of prediction error

WU Youqing[1], MA Wenjing[2], YIN Zhaoxia[3], PENG Yinyin[4], ZHANG Xinpeng[5]

1. School of Computer Science and Technology, Hefei Normal University, Hefei 230601, China
2. Anhui Provincial Key Laboratory of Multimodal Cognitive Computation, Anhui University, Hefei 230601, China
3. School of Communication & Electronic Engineering, East China Normal University, Shanghai 200241, China
4. School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230031, China
5. School of Computer Science, Fudan University, Shanghai 200433, China

Abstract: To further improve the performance of reversible data hiding in encrypted image, an algorithm for lossless compression of the prediction error bit-plane using joint encoding was proposed, which could make full use of image redundancy and reserve more embedding room. Firstly, the image owner calculated the prediction error of the image and divided the prediction error bit-plane into non-overlapping blocks of the same size. Then, the prediction error bit-plane was rearranged according to blocks and the rearranged bitstream was compressed by run-length encoding and Huffman encoding to reserve room. The data hider embedded information in the reserved room of the encrypted image. At the receiving end, the legitimate receiver extracted information and recovered images losslessly and separately. Experimental results show that the proposed algorithm makes full use of the bit-plane distribution characteristics and achieves higher embedding performance. The average embedding rates in BOSSbase and BOWS-2 datasets reach 3.763 bpp and 3.642 bpp, which are at least 0.081 bpp and 0.058 bpp higher than the state-of-the-art algorithms.

Keywords: reversible data hiding in encrypted image, prediction error, run-length encoding, Huffman encoding, bit-plane

收稿日期：2022−05−07；**修回日期：**2022−07−20

通信作者：殷赵霞，zxyin@cee.ecnu.edu.cn

基金项目：国家自然科学基金资助项目（No.62172001, No.61872003, No.U1936214）；安徽省高等学校自然科学重点资助项目（No.KJ2021A0901）；多模态认知计算安徽省重点实验室（安徽大学）开放基金资助项目（No.MMC202106）

Foundation Items: The National Natural Science Foundation of China (No.62172001, No.61872003, No.U1936214), The Natural Science Foundation of Anhui Higher Education Institutions of China (No.KJ2021A0901), The Open Project of Anhui Provincial Key Laboratory of Multimodal Cognitive Computation, Anhui University (No.MMC202106)

0 引言

不断发展的网络技术使远程沟通和信息共享更加便利。用户可以在社交软件分享所见所闻，极大丰富了娱乐及生活方式。但科技的飞速发展也带来了部分隐患，隐私泄露、信息滥用、版权侵犯等事件的频繁发生，不仅损害公民个人合法权益，甚至危及社会进步以及国家安全。近年来，随着公民隐私保护[1]意识的逐渐提升，在信息安全领域担任重要角色的信息隐藏技术[2]日益完善。

根据应用场景不同，信息隐藏主要包括数字水印[3]、隐写术[4-5]以及可逆信息隐藏技术[6]。前两者或多或少都会对载体造成不可逆的失真，可逆信息隐藏则可确保原始载体信号能够完全恢复。除了面向视频[7]、音频[8]、3D 点云[9]等数字信号外，数字图像是研究最广泛的载体格式[10]。

根据数字图像的编码情况，图像可逆信息隐藏又可分为压缩域和空间域两大类，其中压缩域以 JPEG（joint photographic experts group）压缩标准为代表，主要通过修改图像不同压缩阶段的编码来嵌入信息[11-15]。由于压缩编码导致数据冗余空间下降，因此面向图像压缩编码算法的嵌入容量也相对较低。

与压缩图像中的可逆信息隐藏相比，面向空间域图像的算法在嵌入容量上有很大优势，成果也相对丰富。早期工作主要面向明文信号，核心技术包括无损压缩[16]、插值扩展[17]和直方图修改[18]三类。明文算法中载密图像与原始图像极其相似，无法保护图像内容隐私；而加密算法能将载体信号转换为无意义的密文信号，实现将包含隐私信息的载体进行脱敏保护的作用。随着隐私保护需求日益被重视，密文图像可逆信息隐藏（RDHEI, reversible data hiding in encrypted image）[19]被提出并被首先应用到图像数据中。密文图像可逆信息隐藏[20]能够有效地结合图像加密算法与可逆信息隐藏技术，即图像所有者利用加密算法保护原始载体信号，信息隐藏者在密文信号中嵌入信息，实现信息隐藏，最后，接收者根据需求提取信息或恢复图像。密文图像可逆信息隐藏技术有效解决了载体中的隐私泄露问题，是密文信号处理与信息隐藏技术交叉领域的研究热点之一，在隐私保护方面发挥着重要作用。

近年来，随着云存储技术的普及，RDHEI 技术不断发展和完善，在近年 CCF A/B/C 类国际期刊发表的 267 篇可逆信息隐藏论文中占比 32%[21]。按照图像加密与腾出空间的先后顺序，密文图像可逆信息隐藏技术主要包括加密后腾出空间（VRAE, vacating room after encryption）[22-34]以及加密前预留空间（RRBE, reserving room before encryption）[35-53]算法。

早期的 RDHEI 算法利用加密图像的冗余嵌入信息，多属于 VRAE 类算法。且算法中信息提取和图像恢复操作耦合[22-24]，难以分离，而在实际应用中，部分用户可能只被授予一种操作权限。文献[25]介绍一种可分离方案，分别使用图像加密密钥和信息隐藏密钥加密原始图像和待嵌入信息，信息隐藏者压缩加密图像，创建可嵌入信息的稀疏空间。接收者获取载密图像后，可直接从其对应稀疏空间中提取信息。由于该算法未压缩图像的多位最高有效位（MSB, most significant bit），接收者直接解密载密图像后即可恢复图像的多位 MSB，然后解压缩最低有效位（LSB, least significant bit）信息，从而恢复原始图像，即该算法能够分别完成信息提取和图像恢复操作。

为进一步降低信息提取或图像恢复时的误码率，提升嵌入容量，文献[26]利用分块置乱操作加密图像，保留各分块内原始像素分布，结合像素块平滑度，在像素块中利用直方图移位的方法隐藏信息。在接收端，能够可分离地执行图像解密和信息提取操作。由于直方图移位过程中可能存在多个峰值点，因此同一像素块内可嵌入多比特信息，提升了嵌入容量。文献[31-34]利用分块加密保留块内像素冗余进一步提升了嵌入性能。

上述基于 VRAE 的 RDHEI 算法中，图像所有者仅需加密图像内容。然而，由于加密图像像素间相关性较低，难以探索其中规律进行信息嵌入，导致该类算法的嵌入容量存在限制，甚至部分算法在追求提升嵌入容量的同时会导致无法可逆地提取信息或恢复图像，造成图像永久失真。

为解决上述问题，RRBE 类密文图像可逆信息隐藏算法被提出。在该类算法中，图像所有者预处理原始载体以预留可嵌入空间。文献[35]首次提出基于 RRBE 类的算法思想，将原始图像按照平滑度划分为 A、B 两部分，图像所有者利用 B 中像素进行预测误差直方图移位，将 A 中像素部分信息位保存在 B 中，以此实现在 A 中预留空间。与以往的 VRAE 类算法相比，该算法不仅能可逆地提取信息

和恢复图像，还极大地提升了嵌入容量。

考虑到相邻像素间的强相关性，与低位平面相比，高位平面中相邻比特位相同的概率更大，因此，利用像素 MSB 预留空间的操作在理论上可以获得更理想的嵌入性能。文献[37]是首次提出利用像素 MSB 预测来预留空间的 RRBE 类 RDHEI 算法。由于 RDHEI 算法在图像加密域中不考虑图像质量损失，因此选择比 LSB 更易预测的 MSB 来嵌入信息，显著提升了 RDHEI 算法的嵌入容量。文献[38-39]提出 2 种无损压缩图像高位平面的 RDHEI 算法，利用相邻像素间的强相关性，压缩图像的 MSB 能够获得更佳的压缩效果，预留出更多的可嵌入空间。

除上述算法外，近年来致力于探索高容量的 RDHEI 算法层出不穷。文献[48-49]利用像素标记的思想，在标记后像素或位平面中嵌入信息。文献[50]介绍一种基于多位平面重排的 RDHEI 算法，通过位平面的分割和重新排列实现信息嵌入。文献[51]则引入一种分层嵌入思想，按照预测误差范围进行分层嵌入，即使预测误差较大的像素也能用于嵌入信息，进一步提升了图像嵌入性能。

上述算法表明，与 VRAE 类 RDHEI 算法相比，基于 RRBE 框架的算法能获得更高的嵌入性能，从而满足多位信息隐藏的需求。此外，由于可嵌入空间在图像加密前已经获得，信息隐藏者嵌入信息和图像接收者提取信息的操作更加便捷，且提取信息与嵌入信息完全一致，恢复图像也与原始图像相同，实现了真正的可逆性。

与直接基于载体图像 MSB 位平面压缩的 RDHEI 算法不同，文献[53]提出一种基于载体图像的预测误差位平面无损压缩的 RDHEI 算法，采用扩展的游程编码压缩预测误差图像以预留空间。因预测误差图像的像素分布更加集中，相邻像素间的相关性更强，与已有成果相比，该算法的嵌入性能大大提升。然而，文献[53]中采用的压缩算法未充分考虑预测误差位平面的分布特性。基于此，本文在预测误差位平面上采用一种更适应位平面分布特性的联合编码算法，提出一种基于预测误差位平面压缩的 RDHEI 算法，在实现可逆的同时进一步提升了嵌入容量。

本文主要研究贡献如下。

1) 与直接基于载体图像 MSB 位平面压缩的 RDHEI 算法不同，本文提出在载体图像的预测误差位平面上采用一种充分利用位平面分布特性的联合编码算法来无损压缩比特流以预留空间。

2) 与文献[53]相比，本文压缩算法利用预测误差位平面自身分布特性，将哈夫曼编码和游程编码有效结合，能更充分地压缩位平面，从而预留更多的可嵌入空间。

3) 利用像素分布更加集中，相邻像素间相关性更强的预测误差，本文提出一种基于预测误差位平面压缩的高容量 RDHEI 算法，在满足分离并无损提取信息和恢复图像的同时能进一步提升嵌入容量。

1　联合编码算法

文献[53]算法采用扩展的游程编码压缩图像，获得了较好的压缩效果，但该算法未充分利用位平面自身的分布特性。为此，本文在预测误差位平面上采用一种联合编码算法，适应性地生成适合不同图像位平面的压缩编码。此外，为获取包含更多重复位的位平面比特流，进一步提高压缩效果，需对位平面进行重排[38]。

1.1　位平面重排

灰度图像像素可用 8 位二进制数表示，对应图像由 8 个位平面构成。为充分利用图像相邻像素间相关性，文献[38]提出一种位平面重排算法。在该算法中，位平面被划分为尺寸为$t\times t$的无重叠块，根据块内和块间不同的排列方式，生成 4 种位平面排列顺序，并用两位二进制数记录。第一位数表示块内排列方式，“0”和“1”分别表示块内逐行和逐列排列；第二位数表示块间排列方式，“0”和“1”分别表示块间逐行和逐列排列。以图 1 为例，当分块大小 t=2 时，位平面有相应 4 种重排序后的比特流。由于相邻像素之间具有相关性，因此重排后比特流中相邻位往往相同，这为位平面的压缩创造了条件。

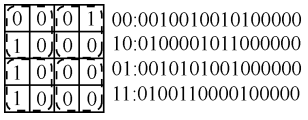


图 1　t=2 时对应的位平面重排示例

1.2　编码规则

位平面重排后，可得到包含多个相同相邻位的比特流。将每个相同相邻位的比特流定义为一个比特串，其对应长度为L。比较比特串长度L与参数L_{fix}（L_{fix}的选择在 3.2 节中说明），若$L\geqslant L_{\text{fix}}$，则视其为长比特串；否则为短比特串。2 种比特串对

应编码规则描述如下。

1) 当 $L \geqslant L_{\text{fix}}$ 时，由于长比特串中重复位较多，因此可借助游程编码完成压缩，其对应编码包含前缀 L_{pre}、中间部分 L_{mid} 以及后缀 L_{tai}。L_{pre} 代表比特串编码类型，为“0”代表当前为长比特串编码；L_{mid} 用当前比特串长度 L 的二进制表示，其长度由预定义参数 L_{run}（L_{run} 的选择在 3.2 节中说明）决定。例如，当 L_{run}=5、L=17 时，中间部分为 $L_{\text{mid}}=(10001)_2$，即比特串长度 L=17 时对应的 5 位二进制数；后缀 L_{tai} 由“0”或“1”组成，表示当前比特串的重复位数值。最后，连接三部分即获得编码后比特串。

2) 当 $L < L_{\text{fix}}$ 时，由于短比特串中重复位较少，使用上述编码方式可能会获得更长的压缩后比特串，难以实现理想的压缩效果。因此，选取能获得平均最短编码长度的哈夫曼编码对短比特串进行压缩，此时编码包含前缀 L_{pre} 和哈夫曼码字 L_{huff} 两部分，L_{pre}=1 代表当前为短比特串编码；L_{huff} 代表当前短比特串对应的哈夫曼码字。为获得高效的哈夫曼编码，编码前需要预处理短比特串。首先，以短比特串首位为开端，截取长度为 L_{fix} 的比特串。然后，遍历所有位平面，记录每个短比特串对应截取比特串的出现概率，根据其出现概率自适应生成哈夫曼编码。最后，用哈夫曼码字压缩相应的短比特串。完成上述步骤后，连接 L_{pre} 和 L_{huff} 即可获得编码后比特串。

由于联合编码算法充分利用了位平面分布特性，将哈夫曼编码和游程编码有效结合，能够取得更好的压缩效果，预留出更多可嵌入空间。以部分截取的比特流为例，当 L_{fix}=4、L_{run}=3 时，联合编码算法的执行过程如图 2 所示。首先，计算下划线处比特串的长度 L，然后比较 L 和 L_{fix} 的长度，按照比较结果选择相应的编码规则。若 $L \geqslant L_{\text{fix}}$，代表当前为长比特串，按照编码规则获取编码前缀 L_{pre}、中间部分 L_{mid} 以及后缀 L_{tai}，以此完成编码；反之，当前为短比特串，按照对应编码规则从短比特串首位截取长度为 L_{fix} 的比特串，然后遍历比特流，记录每个短比特串对应截取比特串的出现概率，根据其出现概率自适应生成哈夫曼码字，用对应的哈夫曼码字完成编码。最后，连接所有编码后比特串，生成压缩后比特流。通过上述操作，图 2 中对应的原始比特流“10001111111100010000000”被压缩编码为“100011111111001110”，压缩后比特流长度小于原始比特流长度。编码过程中产生的辅助信息有预定义参数 L_{fix}、L_{run} 和哈夫曼编码规则，其占用的存储空间较小，根据压缩后比特流，结合辅助信息，可逆向解压缩恢复原始比特流。

图 2 联合编码算法的执行过程

2　算法设计

为充分利用图像冗余性，进一步提高图像嵌入性能，本文设计一种基于预测误差位平面压缩的 RDHEI 算法。

2.1　研究框架

本文提出一种基于预测误差位平面压缩的 RDHEI 算法，实现了可逆性、可分离性以及高嵌入率。图 3 给出了基于预测误差位平面压缩的 RDHEI 算法框架。首先，图像所有者计算整幅图像的预测误差，并将其划分为相同大小的非重叠块；然后，利用第 1 节介绍的联合编码算法对预测误差的每个位平面进行重新排列和压缩，以预留空间；最后，加密压缩后的图像以保护图像内容。信息隐藏者接收加密图像后，能够定位预留空间并将加密后的信息对象嵌入其中。在接收端，结合不同的密钥，合法的图像接收者能够从载密图像中可分离地提取信息或恢复图像。

2.2　预留空间

为获得更高的嵌入容量，图像所有者加密图像前会预留可嵌入空间。预留空间主要包含两步操作，首先，图像所有者结合中值边缘预测器[54]计算整幅图像的预测误差并对其进行预处理。然后，利用联合编码算法压缩预测误差的位平面，压缩剩余位为可嵌入空间。经过上述操作，可获得预留空间的压缩图像 I_c。将压缩图像 I_c 采用流密码进行加密，即获得预留空间的加密图像。

对于尺寸为 $M\times N$ 的灰度图像，本文采用中值边缘预测方法[54]计算其像素的预测值。一方面，中值边缘预测器利用像素的邻近像素计算其预测值，计算复杂度较低且预测较为准确；另一方面，采用中值边缘预测方法便于逆向恢复图像像素值。假设 $x(i,j)$ 为原始图像的任一像素值，(i,j) 表示像素坐标且 $1\leqslant i\leqslant M$，$1\leqslant j\leqslant N$。在预测过程中，图像的首行和首列像素，即 i=1 或 j=1 对应像素充当参考像素，不进行任何操作。从图像的第二行和第二列开始，选取像素 $x(i,j)$ 左上方、左方以及上方 3 个像素 x_1、x_2 以及 x_3 为参考值，计算 $x(i,j)$ 的预测值 $px(i,j)$ 为

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

依次扫描图像剩余像素，计算其预测值。结合像素值 $x(i,j)$ 和其预测值 $px(i,j)$，计算像素预测误差 $e(i,j)$ 为

$$e(i,j)=x(i,j)-px(i,j)\tag{2}$$

随后，图像所有者将预测误差按照式(3)转换成 8 位二进制数。

$$e'_k(i,j)=\begin{cases}\text{floor}\left(\dfrac{|e(i,j)|}{2^{k-1}}\right)\bmod 2, k=1,2,\cdots,7\\ 1, k=8 \text{ 且 } e(i,j)<0\\ 0, k=8 \text{ 且 } e(i,j)\geqslant 0\end{cases}\tag{3}$$

其中，$e'_k(i,j)$ 表示预测误差的第 k 位，floor(*) 表示向下取整函数，$|*|$ 表示取绝对值操作，mod 表示取

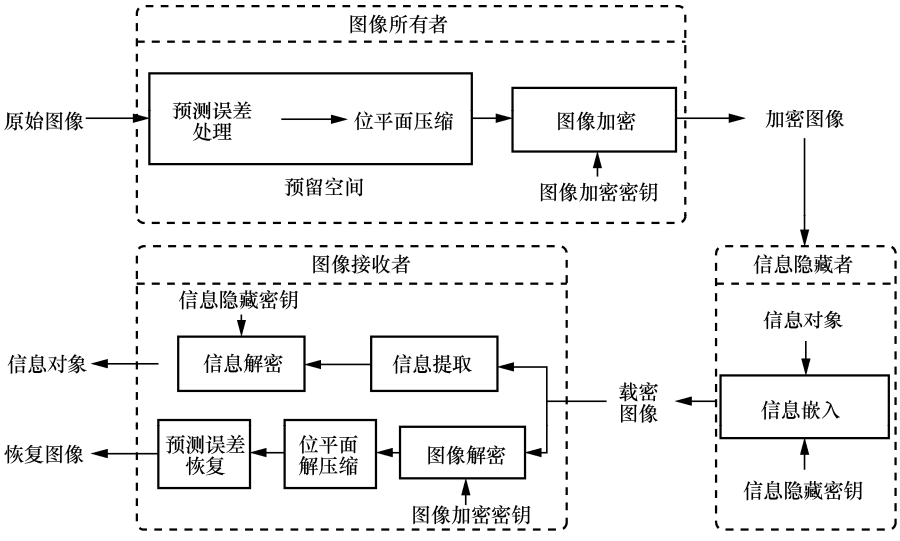


图 3　基于预测误差位平面压缩的 RDHEI 算法框架

余数操作。由于预测误差存在正负之分，为了能唯一表示不同预测误差，选取其 MSB，即 $k=8$ 时的二进制位表示符号标记位。当预测误差为负时，MSB 标记为“1”；否则为“0”。剩余 7 位则由当前预测误差绝对值的二进制位表示。最终，经过处理后的预测误差 $e'(i,j)$ 为

$$e'(i,j)=\begin{cases}x(i,j), e(i,j)\notin[-127,127]\\ 2^{k-1}\sum_{k=1}^{8}e'_k(i,j), \text{其他}\end{cases} \tag{4}$$

由于预测误差超出[−127,127]的像素不能用 8 位二进制数表示，因此将这些溢出像素记录为辅助信息，其对应处理后预测误差仍用原始像素值表示。

对于预处理后的所有预测误差，将其划分为 $t\times t$（t 的选择在 3.2 节中说明）大小的非重叠块，采用第 1 节介绍的联合编码算法压缩其位平面。在位平面压缩过程中，哈夫曼编码可以有效地压缩短比特串，而游程编码对长比特串的压缩效果更好。因此，该联合编码算法能够获得更好的压缩效率。此外，与原始图像相比，处理后预测误差的分布更加集中，对预测误差位平面进行压缩可以取得更好的效果。预测误差位平面压缩的具体步骤如下。

1) 首先，将预处理后预测误差的每个位平面按照 1.1 节的 4 种重排类型，生成 4 种位平面重排比特流。然后，图像所有者使用联合编码算法压缩各个位平面的 4 种比特流，选择并记录压缩效果最佳的重排后位平面比特流 $(P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8)$，同样记录下对应的位平面重排类型。

2) 压缩位平面后即可获得对应压缩后比特流，比较压缩后位平面和原始位平面对应比特流的长度，若压缩后的长度更大，则不执行压缩；反之，则图像所有者压缩位平面并记录压缩后位平面信息。如图 4(a)所示，压缩后位平面信息由压缩标记位、位平面重排类型、压缩后位平面比特流及其长度共 4 个部分构成。压缩标记位被用于判断当前位平面是否被压缩，为“0”代表当前位平面能够被压缩；否则，位平面无法压缩。如图 4(b)所示，未压缩位平面信息由压缩标记位和原始位平面比特流组成。依次遍历所有重排后位平面比特流 $(P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8)$，得到相应的压缩后或未压缩的位平面信息。最后，统一记录为处理后的位平面比特流 $(P_{c1},P_{c2},P_{c3},P_{c4},P_{c5},P_{c6},P_{c7},P_{c8})$。

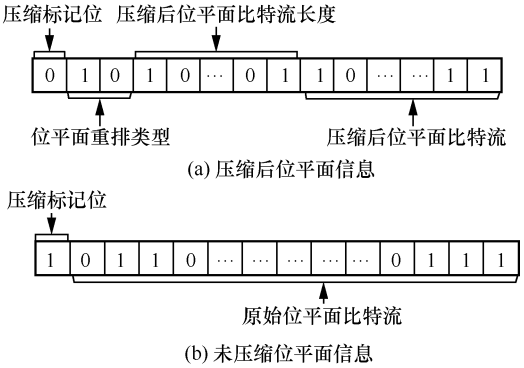


图 4 处理后的位平面比特流

3) 结合用于解压缩编码的辅助信息 A，并连接所有处理后的位平面比特流 $(P_{c1},P_{c2},P_{c3},P_{c4},P_{c5},P_{c6},P_{c7},P_{c8})$，可重建得到压缩图像 I_c。辅助信息 A 由分块大小 t，预定义参数 L_{fix}、L_{run}，哈夫曼编码规则以及溢出像素和参考像素信息构成。此外，为便于图像恢复操作，辅助信息 A 的长度和所有处理后位平面比特流的总长度分别用 lb(MN) 以及 lb(8MN) 位记录。压缩图像的简要构成如图 5 所示，压缩图像从最高位平面开始存储信息，低位平面中的空白位则代表预留空间，可用于嵌入信息。

为防止图像内容泄露，图像所有者预留空间后需要对压缩图像 I_c 执行加密操作。在图像加密阶段，首先，利用图像加密密钥生成一个与压缩图像尺寸相同的 $M\times N$ 的伪随机矩阵 $\boldsymbol{H}$。然后，压缩图

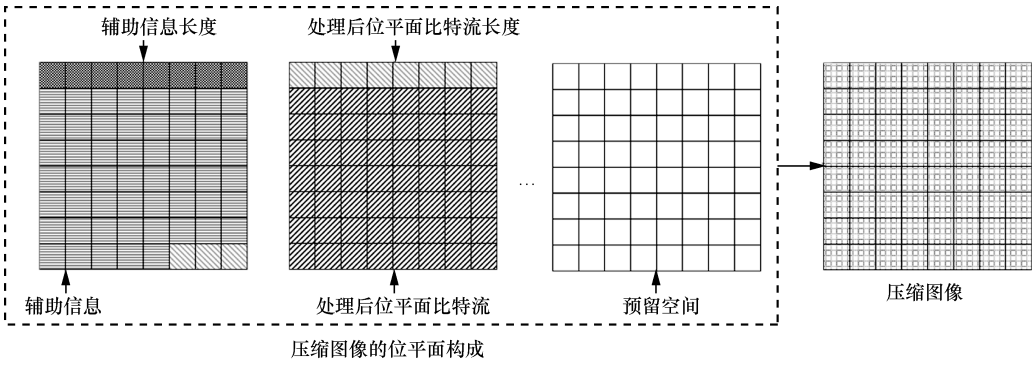


图 5 压缩图像的简要构成

像像素 $x_c(i,j)$ 和 $\boldsymbol{H}$ 中元素 $h(i,j)$ 并转换成 8 位二进制表示，转换式为

$$x_c^k(i,j)=\text{floor}\left(\frac{x_c(i,j)}{2^{k-1}}\right) \bmod 2, k=1,2,\cdots,8 \quad (5)$$

$$h^k(i,j)=\text{floor}\left(\frac{h(i,j)}{2^{k-1}}\right) \bmod 2, k=1,2,\cdots,8 \quad (6)$$

其中，$x_c^k(i,j)$ 和 $h^k(i,j)$ 分别表示 $x_c(i,j)$ 和 $h(i,j)$ 二进制表示的第 k 位。随后，图像所有者执行按位异或操作实现加密，加密步骤如式(7)所示。

$$x_e^k(i,j)=x_c^k(i,j)\oplus h^k(i,j), k=1,2,\cdots,8 \quad (7)$$

其中，$x_e^k(i,j)$ 表示加密像素的第 k 位，‘⊕’表示异或操作。最后，根据式(8)可重构获得加密图像 I_e。

$$x_e(i,j)=2^{k-1}\sum_{k=1}^{8}x_e^k(i,j), k=1,2,\cdots,8 \quad (8)$$

其中，$x_e(i,j)$ 为像素值。此外，为了便于信息隐藏者嵌入信息，在加密图像最低位平面的第 M 行，即预留空间的末 lb(8MN) 位中存储净嵌入容量 c。

2.3　信息嵌入

完成预留空间操作后，结合重排位平面比特流 $(P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8)$、辅助信息 A，以及处理后位平面比特流 $(P_{c1},P_{c2},P_{c3},P_{c4},P_{c5},P_{c6},P_{c7},P_{c8})$，在加密图像中可计算出图像净嵌入容量 c。由于加密图像中辅助信息长度以及处理后位平面比特流长度分别占 lb(MN) 以及 lb(8MN) 位，且预留空间的末 lb(8MN) 位被用于存储净嵌入容量，因此，净嵌入容量 c 为

$$c=\sum_{k=1}^{8}\left[l(P_k)-l(P_{ck})\right]-l(A)-3\text{lb}(MN)-6 \quad (9)$$

其中，l(*) 代表信息对应长度。由于联合编码算法能够取得较好的位平面压缩效果，且辅助信息 A 的长度相对较小，因此所提算法最终能获得较高的净嵌入容量 c。如 2.2 节所述，净嵌入容量 c 存储在加密图像的最低位平面中，当信息隐藏者接收到加密图像后，可以首先获取最低位平面中存储的净嵌入容量，定位加密图像中的预留空间。然后，使用信息隐藏密钥对嵌入对象完成加密操作，操作过程与图像加密过程类似。最后，以位替换的方式在加密图像的预留空间中嵌入信息，获得载密图像 I_{ee}。

2.4　信息提取和图像恢复

在信息提取和图像恢复阶段，图像接收者可从载密图像 I_{ee} 中提取嵌入的信息对象并借助辅助信息恢复图像。在信息提取阶段，图像接收者首先提取载密图像最低位平面中存储的净嵌入容量以定位嵌入信息的坐标，然后提取出加密的信息对象并结合信息隐藏密钥完成解密操作，即可提取原始的嵌入信息；在图像恢复阶段，图像接收者解密图像，截取其中包含的辅助信息和处理后的位平面比特流，进而解压缩恢复原始图像。根据图像接收者持有的密钥，可分为以下 3 种情况。

1) 当仅持有信息隐藏密钥时，能够提取原始的信息对象。首先，图像接收者从载密图像的最低位平面中提取净嵌入容量 c，根据净嵌入容量定位并提取加密的信息对象。然后，使用信息隐藏密钥解密提取的信息，即可获得原始的信息对象。

2) 当仅持有图像加密密钥时，能够可逆地恢复图像。首先，图像接收者利用图像加密密钥对载密图像进行解密，结合辅助信息长度和处理后位平面比特流长度，提取其中的辅助信息和处理后的位平面比特流信息。然后，利用辅助信息解压缩处理后的位平面比特流，并将其恢复为预测误差的位平面，获取原预测误差。最后，利用辅助信息恢复首行首列的参考像素值，从第二行第二列像素开始，顺次遍历计算剩余像素的预测值，结合原预测误差恢复原像素值，从而恢复原始图像。

3) 当同时持有图像加密密钥和信息隐藏密钥时，按照上述操作，能够可逆、可分离地提取原始的信息对象并恢复原始图像。

3　实验结果与分析

为证明所提算法的有效性和可行性，本节设计了大量仿真实验并进行分析。首先分析了算法的可逆性和可分离性，并将所提算法与目前性能较好的算法进行定性比较。然后对联合编码算法的 3 个相关参数进行优化，以获得更好的性能。最后，将所提算法与已有经典算法的嵌入率进行定量比较。在加密操作方面，由于加密是密文信号处理固有框架的一部分，本文采用多数密文图像可逆信息隐藏文献[22-25]中普遍使用的流密码加密算法，且其安全性已被充分讨论[55]。在实验设置方面，如图 6 所示，使用 3 幅常见灰度图像 Lena、Baboon 以及 Airplane 展示实验结果，其中 Lena 图像既包含纹理平滑区域，又包含纹理复杂区域；Baboon 是典型的纹理复杂图像；Airplane 是典型的纹理平滑图像。为降低图像纹理复杂度对实验结果的影响，在各有 10 000 幅

灰度图像的 BOSSbase[56]和 BOWS-2[57]图像集中进一步完成实验验证，且选取均方误差（MSE, mean square error）作为评价指标来检验算法的可逆性。

$$\mathrm{MSE}=\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}(x'-x)^2}{MN} \tag{10}$$

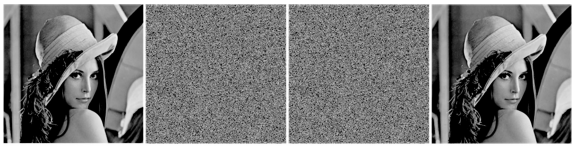
其中，MN 为图像尺寸，x' 和 x 分别为恢复图像和原始图像的像素值。MSE 值越小，表示 2 幅图像之间的差异越小，当其为 0 时，代表 2 幅图像完全相同。此外，选取嵌入率（ER, embedding rate）作为衡量算法嵌入性能的关键指标，图像尺寸 MN 以及净嵌入容量 c 被用于计算图像嵌入率，即 $\mathrm{ER}=\frac{c}{MN}$，表示平均每像素所嵌入的比特数（BPP, bit per pixel）。

(a) Lena (b) Baboon (c) Airplane

图 6 常见灰度测试图像

3.1 性能分析

图 7 为不同状态下的 Lena 图像。图 7(a)为原始图像，图 7(b)和图 7(c)分别为加密状态和载密状态的 Lena 图像，图 7(d)为恢复图像。从图 7 可以看出，恢复图像与原始图像一致。经实验验证，图 7(a)和图 7(d)间的 MSE 值为 0，表明 2 幅图像完全相同，证明了图像恢复的可逆性。为进一步证明这种可逆性与图像纹理复杂度无关，实验还计算了图像集 BOSSbase[56]和 BOWS-2[57]中恢复图像和原始图像间的 MSE。实验结果同样显示，图像集中原始图像与恢复图像间的 MSE 均为 0，说明所提算法能可逆地恢复图像。此外，实验对提取信息与嵌入信息内容进行了对比，结果表明信息对象能够可逆地提取。而且，在实际操作中，所提算法的信息提取和图像恢复步骤互不影响，均能独立完成，进一步证实了所提算法的可分离性。



(a) 原始图像 (b) 加密图像 (c) 载密图像 (d) 恢复图像

图 7 不同状态下的 Lena 图像

表 1 定性分析了所提算法与几种代表算法[28-30,33-34,39,52]的特性，其中将嵌入率在 1 bpp 以下的视为低嵌入率，在 1 bpp 和 3.5 bpp 之间的视为中嵌入率，而大于 3.5 bpp 的则视为高嵌入率。由表 1 可知，文献[28,30,33-34]中算法采取不同的加密方法加密图像，利用加密图像的冗余性嵌入信息，能够可逆、可分离地提取信息和恢复图像，但难以获得理想的嵌入性能。文献[29]则通过创建图像插值空间嵌入信息，能够获得较高的嵌入性能，但同时也使数据产生了扩展，降低了载体传输效率。文献[33,52]中算法采用秘密共享的思想加密图像，均存在数据扩展，其中文献[52]在加密图像前对图像预处理，因此获得了较高的嵌入性能。文献[39]中算法压缩图像的高位平面，而本文提出的基于 RRBE 的算法则利用联合编码算法压缩分布更为集中的预测误差位平面，并采用操作便捷的流密码完成加密操作，在实现可逆性、可分离性的同时获得了比当前算法更高的嵌入率。此外，所提算法在信息隐藏过程中不存在数据扩展，不会造成额外的载体传输压力。

3.2 参数优化

所提算法中主要包含 3 个与联合编码算法相关的参数：分块大小 t，用于判定比特串类型的 L_{fix}，以及表示游程编码长度的 L_{run}。上述 3 个参数的选

表 1 所提算法与文献[28-30,33-34,39,52]中算法的定性比较

算法	类型	加密操作	恢复图像质量	是否具有分离性	嵌入率	是否产生扩展
文献[28]	VRAE	流密码+块置乱	无损	是	低	否
文献[29]	VRAE	矩阵遍历+扩散	无损	是	高	是
文献[30]	VRAE	块置乱+像素置乱	无损	是	中	否
文献[33]	VRAE	秘密共享	无损	是	中	是
文献[34]	VRAE	块置乱+调制	无损	是	中	否
文献[39]	RRBE	流密码	无损	是	中	否
文献[52]	RRBE	秘密共享	无损	是	中	是
所提算法	RRBE	流密码	无损	是	高	否

择会影响预测误差位平面的压缩效果，进而影响图像嵌入率。为提升所提算法的嵌入性能，参数优化步骤必不可少。在参数优化过程中，保持 2 个相关参数不变，观察嵌入性能随第 3 个参数变化的波动情况，选择能够获取最佳嵌入性能的参数。理论上，对每幅图像均采用参数优化的方法可自适应地获得适合每幅图像纹理特性的最优参数，但考虑到算法的计算代价，本节随机选取图像集 BOSSbase[56] 和 BOWS-2[57]中 200 幅图像进行测试，获取对应的能取得最高平均嵌入率的参数。

表 2 描述了当 t=4 、L_{fix} 为 3～6、L_{run} 为 3～6 时测试图像的平均嵌入率。结果表明，当 L_{fix}=6 、L_{run}=5 时测试图像的平均嵌入率最高，超出这个范围平均嵌入率则呈下降趋势。为探究分块大小 t 对嵌入性能的影响，表 3 描述了当 L_{fix}=6， L_{run}=5，分块大小 t 分别取 2、3、4 和 8 时测试图像对应的平均嵌入率。实验结果表明，当 t=4 时，平均嵌入率能够达到最佳水平。

表 2　当 t=4、L_{fix} 为 3～6、L_{run} 为 3～6 时 200 幅测试图像的平均嵌入率

L_{fix}	L_{run}	BOSSbase	BOWS-2
3	3	2.231	3.674
	4	2.365	3.651
	5	3.385	3.593
	6	3.317	3.524
4	3	3.516	3.718
	4	3.528	3.730
	5	3.499	3.705
	6	3.454	3.662
5	3	3.533	3.735
	4	3.562	3.764
	5	3.553	3.759
	6	3.528	3.734
6	3	3.550	3.751
	4	3.589	3.789
	5	**3.591**	**3.794**
	6	3.576	3.780

表 3　当 L_{fix}=6，L_{run}=5，t 分别取 2、3、4、8 时 200 幅测试图像的平均嵌入率

t	BOSSbase	BOWS-2
2	3.569	3.770
3	3.589	3.792
4	**3.591**	**3.794**
8	3.566	3.772

结合表 2 和表 3 可知，当选取参数 t=4 、L_{fix}=6 、L_{run}=5 时，所提算法能获得较高的平均嵌入率。当然，选取更多图像进行参数优化能获得更优的参数，或对每幅图像分别优化以自适应获取适合每幅图像纹理特性的最优参数，可以根据实际需求灵活选择，以平衡参数选择代价和性能。考虑到计算代价，本文后续实验均采用该参数。

3.3　嵌入率对比

为进一步说明所提算法的性能，下面定量比较所提算法与多种基于 RRBE 类经典算法[37-38,41,48-51,53]的嵌入率。图 8 比较了不同算法在 Lena、Baboon 和 Airplane 图像上的嵌入率。

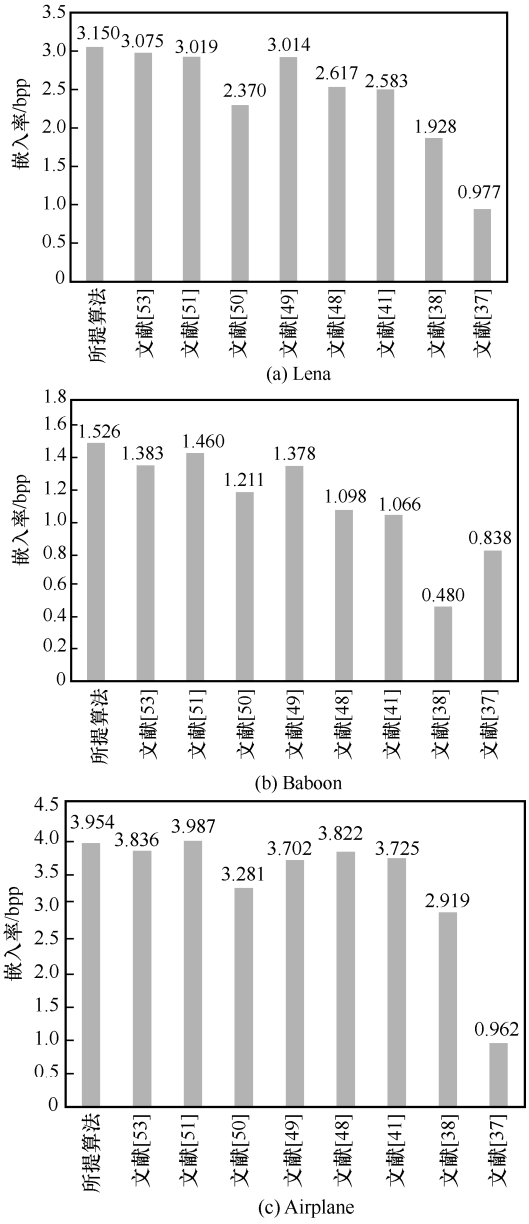


图 8　测试图像的嵌入率

由图 8(a)可知，在 Lena 图像上，大多数算法都能取得较高的嵌入率，但所提算法利用适应位平面分布特性的联合编码无损压缩波动范围较小的预测误差位平面，获得了较其他算法更高的嵌入率；在图 8(b)中，由于 Baboon 图像纹理比较复杂，现存的 RDHEI 算法都难以获得理想的嵌入率，但所提算法仍然取得了较其他算法更高的嵌入率；在图 8(c)中，Airplane 是典型的纹理平滑图像，所有算法的嵌入率均有进一步提升，所提算法的嵌入率仅略逊于文献[51]，仍能取得较好的性能。

此外，为说明所提算法的普适性，图 9 比较了所提算法与相关算法在 BOSSbase[56]和 BOWS-2[57]图像集中的平均嵌入率。由图 9 可知，所提算法均获得了最佳性能，在 BOSSbase[56]和 BOWS-2[57]图像集中平均嵌入率分别达到 3.763 bpp 和 3.642 bpp，与文献[53]相比分别提高了 0.138 bpp 和 0.147 bpp，即使与当前性能最佳算法[49,51]相比，所提算法在 2 个图像集中的平均嵌入率仍然提高了 0.081 bpp 和 0.058 bpp。

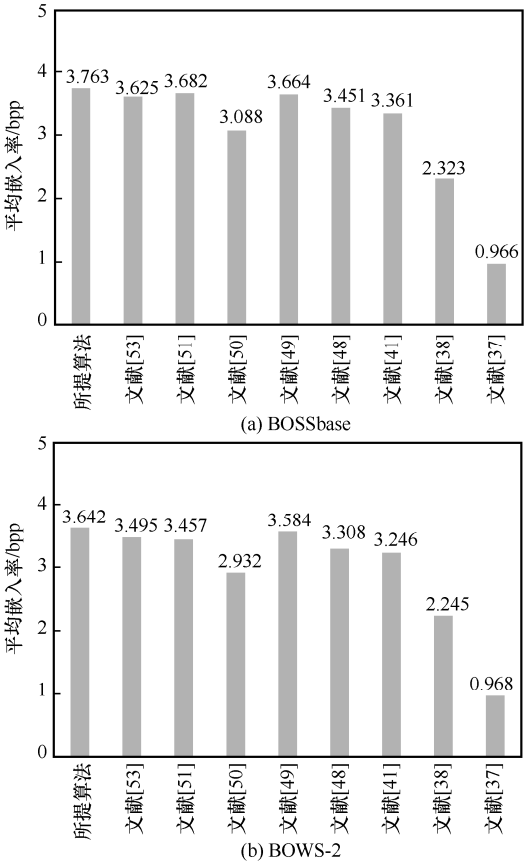


图 9 测试图像集的平均嵌入率

本文在预测误差位平面上采用一种充分利用位平面分布特性的联合编码算法来压缩比特流，与文献[53]算法相比，能更充分地压缩各个预测误差位平面以预留空间，图 8 与图 9 均说明了所提算法在实现可逆、可分离的同时获得了比当前算法更好的性能。

4 结束语

为充分利用图像冗余，提升 RDHEI 算法的嵌入率，本文提出一种基于预测误差位平面压缩的高容量 RDHEI 算法。该算法在波动范围较小的预测误差位平面上采用一种联合编码的压缩算法，联合编码算法将游程编码和哈夫曼编码有效结合，能更充分地利用预测误差位平面的分布特性，从而预留更多可嵌入空间。经实验验证，所提算法能够可逆、可分离地实现信息提取和图像恢复。与当前性能较好的算法相比，所提算法能够获得更高的图像嵌入率。

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] 张新鹏, 殷赵霞. 多媒体信息隐藏技术[J]. 自然杂志, 2017, 39(2): 87-95.
ZHANG X P, YIN Z X. Data hiding in multimedia[J]. Chinese Journal of Nature, 2017, 39(2): 87-95.

[3] 姚远志, 王锋, 严文博, 等. 基于二维码和可逆可视水印的图像隐私保护方案[J]. 通信学报, 2019, 40(11): 65-75.
YAO Y Z, WANG F, YAN W B, et al. Image privacy preservation scheme based on QR code and reversible visible watermarking[J]. Journal on Communications, 2019, 40(11): 65-75.

[4] 周志立, 王美民, 杨高波, 等. 基于轮廓自动生成的构造式图像隐写方法[J]. 通信学报, 2021, 42(9): 144-154.
ZHOU Z L, WANG M M, YANG G B, et al. Generative steganography method based on auto-generation of contours[J]. Journal on Communications, 2021, 42(9): 144-154.

[5] 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[J]. 软件学报, 2021, 32(2): 551-578.
CHEN J F, FU Z J, ZHANG W M, et al. Review of image steganalysis based on deep learning[J]. Journal of Software, 2021, 32(2): 551-578.

[6] SHI Y Q, LI X L, ZHANG X P, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210-3237.

[7] XU D W, WANG R D, SHI Y Q. Data hiding in encrypted H.264/AVC video streams by codeword substitution[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(4): 596-606.

[8] XIANG S J, LI Z H. Reversible audio data hiding algorithm using noncausal prediction of alterable orders[J]. EURASIP Journal on Audio, Speech, and Music Processing, 2017, 2017(1): 1-16.

[9] XU N, TANG J, LUO B, et al. Separable reversible data hiding based on integer mapping and MSB prediction for encrypted 3D mesh models[J]. Cognitive Computation, 2022, 14(3): 1172-1181.

[10] 欧博, 殷赵霞, 项世军. 明文图像可逆信息隐藏综述[J]. 中国图象图形学报, 2022, 27(1): 111-124.
OU B, YIN Z X, XIANG S J. Overview of reversible data hiding in plaintext image[J]. Journal of Image and Graphics, 2022, 27(1): 111-124.

[11] YIN Z X, JI Y, LUO B. Reversible data hiding in JPEG images with multi-objective optimization[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2343-2352.

[12] DU Y, YIN Z X, ZHANG X P. High capacity lossless data hiding in JPEG bitstream based on general VLC mapping[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 1420-1433.

[13] YIN Z X, XIANG Y Z, QIAN Z X, et al. Unified data hiding and scrambling method for JPEG images[C]//Pacific Rim Conference on Multimedia. Berlin: Springer, 2018: 373-383.

[14] HE J H, CHEN J X, LUO W Q, et al. A novel high-capacity reversible data hiding scheme for encrypted JPEG bitstreams[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(12): 3501-3515.

[15] QIAN Z X, XU H S, LUO X Y, et al. New framework of reversible data hiding in encrypted JPEG bitstreams[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2019, 29(2): 351-362.

[16] ZHANG W M, HU X C, LI X L, et al. Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression[J]. IEEE Transactions on Image Processing, 2013, 22(7): 2775-2785.

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

[18] NI Z C, SHI Y Q, ANSARI N, et al. Reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362.

[19] PUECH W, CHAUMONT M, STRAUSS O. A reversible data hiding method for encrypted images[J]. Proceedings of SPIE - The International Society for Optical Engineering, 2008, 6819: 534-542.

[20] PUTEAUX P, ONG S Y, WONG K S, et al. A survey of reversible data hiding in encrypted images-the first 12 years[J]. Journal of Visual Communication and Image Representation, 2021, 77: 103085.

[21] 中国图象图形学报. “数字图像/视频内容安全”前沿论坛暨专刊优秀成果分享会[R]. 2022.
Journal of Image and Graphics. Frontier forum and excellent results sharing session of special issue on “digital image/video content security”[R]. 2022.

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

[23] 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.

[24] ABHINAV A, MANIKANDAN V M, BINI A A. An improved reversible data hiding on encrypted images by selective pixel flipping technique[C]//Proceedings of 2020 5th International Conference on Devices, Circuits and Systems (ICDCS). Piscataway: IEEE Press, 2020: 294-298.

[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] 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.

[27] QIAN Z X, ZHANG X P. Reversible data hiding in encrypted images with distributed source encoding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2016, 26(4): 636-646.

[28] 黄梦雪, 和红杰, 陈帆. 抵抗唯密文攻击的可分离加密域可逆信息隐藏[J]. 计算机辅助设计与图形学学报, 2020, 32(6): 874-882.
HUANG M X, HE H J, CHEN F. Separable reversible data hiding in encrypted image against ciphertext-only attack[J]. Journal of Computer-Aided Design & Computer Graphics, 2020, 32(6): 874-882.

[29] 王继军, 李国祥, 夏国恩, 等. 图像插值空间完全可逆可分离密文域信息隐藏算法[J]. 电子学报, 2020, 48(1): 92-100.
WANG J J, LI G X, XIA G E, et al. A separable and reversible data hiding algorithm in encrypted domain based on image interpolation space[J]. Acta Electronica Sinica, 2020, 48(1): 92-100.

[30] WANG X, CHANG C C, LIN C C. Reversible data hiding in encrypted images with block-based adaptive MSB encoding[J]. Information Sciences, 2021, 567: 375-394.

[31] LIU Z L, PUN C M. Reversible data hiding in encrypted images using chunk encryption and redundancy matrix representation[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 1382-1394.

[32] WANG Y M, HE W G. High capacity reversible data hiding in encrypted image based on adaptive MSB prediction[J]. IEEE Transactions on Multimedia, 2022, 24: 1288-1298.

[33] QIN C, JIANG C Y, MO Q, et al. Reversible data hiding in encrypted image via secret sharing based on GF (p) and GF (2^8)[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(4): 1928-1941.

[34] YU C Q, ZHANG X Q, LI G X, et al. Reversible data hiding with adaptive difference recovery for encrypted images[J]. Information Sciences, 2022, 584: 89-110.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 吴友情, 张睿灵, 汤进, 等. 定长编码和哈夫曼编码的密文域可逆信息隐藏[J]. 中国图象图形学报, 2022, 27(1): 277-288.
WU Y Q, ZHANG R L, TANG J, et al. Reversible data hiding in encrypted images based on joint fixed-length coding and Huffman coding[J]. Journal of Image and Graphics, 2022, 27(1): 277-288.

[40] 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.

[41] YIN Z X, XIANG Y Z, ZHANG X P. Reversible data hiding in en-

crypted images based on multi-MSB prediction and Huffman coding[J]. IEEE Transactions on Multimedia, 2020, 22(4): 874-884.

[42] GUAN B, XU D W. An efficient high-capacity reversible data hiding scheme for encrypted images[J]. Journal of Visual Communication and Image Representation, 2020, 66: 102744.

[43] MOHAMMADI A, NAKHKASH M, AKHAEE M A. A high-capacity reversible data hiding in encrypted images employing local difference predictor[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2020, 30(8): 2366-2376.

[44] PUTEAUX P, PUECH W. A recursive reversible data hiding in encrypted images method with a very high payload[J]. IEEE Transactions on Multimedia, 2021, 23: 636-650.

[45] CHEN F, YUAN Y, HE H J, et al. Multi-MSB compression based reversible data hiding scheme in encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 31(3): 905-916.

[46] YIN Z X, SHE X M, TANG J, et al. Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement[J]. Signal Processing, 2021, 187: 108146.

[47] WENG S W, ZHANG C Y, ZHANG T C, et al. High capacity reversible data hiding in encrypted images using SIBRW and GCC[J]. Journal of Visual Communication and Image Representation, 2021, 75: 102932.

[48] 吴友情, 郭玉堂, 汤进, 等. 基于自适应哈夫曼编码的密文图像可逆信息隐藏算法[J]. 计算机学报, 2021, 44(4): 846-858.
WU Y Q, GUO Y T, TANG J, et al. Reversible data hiding in encrypted images using adaptive Huffman encoding strategy[J]. Chinese Journal of Computers, 2021, 44(4): 846-858.

[49] 余晓萌, 杜洋, 马文静, 等. 基于像素预测和块标记的图像密文图像可逆信息隐藏[J]. 计算机研究与发展, 2021: doi.org/10.7544/issn1000-1239.20210495.
SHE X M, DU Y, MA W J, et al. Reversible data hiding in encrypted images based on pixel prediction and block labeling[J]. Journal of Computer Research and Development, 2021: doi.org/10.7544/issn1000-1239.20210495.

[50] 周旭, 吴福虎, 陈志立, 等. 密文域高嵌入率图像全位面可逆数据隐藏[J]. 中国图象图形学报, 2021, 26(5): 1147-1156.
ZHOU X, WU F H, CHEN Z L, et al. All bit planes reversible data hiding for images with high-embedding-rate in ciphertext field[J]. Journal of Image and Graphics, 2021, 26(5): 1147-1156.

[51] YU C Q, ZHANG X Q, ZHANG X P, et al. Reversible data hiding with hierarchical embedding for encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(2): 451-466.

[52] HUA Z Y, WANG Y X, YI S, et al. Reversible data hiding in encrypted images using cipher-feedback secret sharing[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 32(8): 4968-4982.

[53] 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, 2022, 19(2): 992-1002.

[54] WEINBERGER M J, SEROUSSI G, SAPIRO G. LOCO-I: a low complexity, context-based, lossless image compression algorithm[C]//Proceedings of Data Compression Conference-DCC'96. Piscataway: IEEE Press, 1996: 140-149.

[55] QU L F, HE H J, CHEN F. On the security of block permutation and co-XOR in reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(3): 920-932.

[56] BAS P, FILLER T, PEVNÝ T. Break our steganographic system: the ins and outs of organizing BOSS[C]//International Workshop on Information Hiding. Berlin: Springer, 2011: 59-70.

[57] BAS P, FURON T. Image database of BOWS-2[R]. 2017.

[作者简介]

吴友情（1984– ），女，安徽枞阳人，合肥师范学院讲师，主要研究方向为信息隐藏、多媒体安全等。

马文静（1997– ），女，安徽阜阳人，安徽大学硕士生，主要研究方向为信息隐藏。

殷赵霞（1983– ），女，安徽安庆人，博士，华东师范大学教授，主要研究方向为隐蔽通信、多媒体通信与隐私保护、图像处理与人工智能等。

彭银银（1994– ），女，安徽颍上人，合肥工业大学博士生，主要研究方向为隐私安全。

张新鹏（1975– ），男，黑龙江密山人，博士，复旦大学教授，主要研究方向为多媒体信息安全、AI 安全、图像处理等。