基于自适应哈夫曼编码的密文可逆信息隐藏算法

吴友情[1),2)] 郭玉堂[2)] 汤 进[1)] 罗 斌[1)] 殷赵霞[1)]

[1)](安徽大学多模态认知计算安徽省重点实验室 合肥 230601)

[2)](合肥师范学院计算机学院 合肥 230601)

摘 要 随着云存储和隐私保护的发展,密文域可逆信息隐藏作为一种可以在密文中嵌入秘密信息,保证嵌入后的信息可以无错误提取,并能无损恢复原始明文图像的技术,越来越受到人们的关注.本文提出了一种基于自适应哈夫曼编码的密文域可逆信息隐藏算法,对不同的图像采用不同的哈夫曼码字编码腾出空间来嵌入秘密信息.首先利用自然图像相邻像素间的相关性对原始明文图像进行像素值预测,从最高有效位到最低有效位,对原始像素值和预测像素值的相同比特位进行自适应的哈夫曼编码标记.然后,利用流密码对原始明文图像进行加密.最后在腾出的空间,通过位替换来自适应的嵌入秘密信息.由于哈夫曼编码和解码的可逆性,合法接收者可以对原始明文图像和秘密信息实现分离的无损恢复和提取.实验结果表明,与现有的几种方法相比,本文提出的方法具有更好的安全性和更高的嵌入率,在BOSSBase、BOWS-2和UCID三个数据集上的平均嵌入率比MPHC算法分别提高了0.09 bpp、0.062 bpp和0.06 bpp,在最佳情况下比MPHC算法能分别高出0.958 bpp、0.797 bpp和0.320 bpp,最差情况下的嵌入率比MPHC算法也分别高出了0.01 bpp、0.039 bpp和0.061 bpp.

关键词 密文域;可逆信息隐藏;哈夫曼编码;自适应;分离

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2021.00846

Reversible Data Hiding in Encrypted Images Using Adaptive Huffman Encoding Strategy

WU You-Qing[1),2)] GUO Yu-Tang[2)] TANG Jin[1)] LUO Bin[1)] YIN Zhao-Xia[1)]

[1)](*Anhui Provincial Key Laboratory of Multimodal Cognitive Computation, School of Computer Science and Technology, Anhui University, Hefei* 230601)

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

Abstract With the growing demand of cloud storage for user privacy protection, RDHEI (Reversible Data Hiding in Encrypted Images), as a technology that can embed secret information in encrypted domain, has attracted more and more attention. A good RDHEI method expects to find the best balance between the number of erroneous extracted bits of the secret information, the embedding rate and the quality of the reconstructed image after data-extraction. General RDHEI methods ensure that the embedded secret information can be extracted without error and the original plaintext image can be restored losslessly, thus the embedding rate is the key index to evaluate the performance of an RDHEI method. This paper proposes an effective reversible data hiding method in encrypted images via an adaptive Huffman Encoding strategy, which utilizes diverse Huffman codewords for various images to free up space to accommodate secret information. The proposed method follows EPE-HCRDH (High-Capacity Reversible Data Hiding with Embedded

收稿日期:2020-04-07;在线发布日期:2020-11-20.本课题得到国家重点研发计划项目(2018AAA0100400)、国家自然科学基金项目(61872003,61860206004)资助.**吴友情**,硕士,讲师,主要研究方向为信息隐藏、多媒体安全.E-mail:wuyq.hfnu@qq.com.**郭玉堂**,博士,教授,主要研究领域为模式识别与图像处理.**汤 进**,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为图像处理、模式识别、机器学习和计算机视觉.**罗 斌**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为模式识别与图像处理.**殷赵霞**(通信作者),博士,副教授,中国计算机学会(CCF)会员,主要研究方向为信息隐藏、多媒体安全.E-mail:yinzhaoxia@ahu.edu.cn.

Prediction Errors) method and is an improved method based on MPHC(multi-MSB Prediction and Huffman Coding) method, which provides a high-security level to protect the original image content. Firstly, by exploiting the correlation between the pixels of a natural image, each pixel can be predicted by its neighbors, so as to obtain the entire prediction image. Next, from MSB (Most Significant Bit) to LSB(Least Significant Bit), the same number of bits between each pair of original and predicted pixels is identified and stored in a label map. Then, the label map is compressed by adaptive Huffman encoding with diverse codewords for various images. Using an encryption key, the original plaintext image is encrypted with stream cipher, and the compressed label map is embedded into encrypted image. Finally, according to the extracted label map, after using a data-hiding key, multi-bit secret information can be embedded adaptively in each encrypted pixel through multi-MSB substitution. Due to the reversibility of Huffman encoding and decoding, the secret information can be extracted error-free and the original plaintext image can be restored losslessly by MSB prediction. For different keys, image-recovery and data-extraction can be performed separately. Compared with the experimental results of several state-of-the-art methods, the proposed method has better security performance and achieves higher embedding rate. The average embedding rate of the proposed method outperforms MPHC method 0.09 bpp, 0.062 bpp and 0.06 bpp on three datasets BOSSBase, BOWS-2 and UCID, respectively. In addition, the texture complexity of the original plaintext image has a significant effect on the embedding rate. Generally speaking, smooth images have a satisfactory embedding rate, while texture images have a less ideal embedding rate. For both smooth images and texture images, the proposed method achieves higher embedding rate and outperforms the competitors. On the three datasets, the embedding rate of the proposed method is 0.958 bpp, 0.797 bpp, 0.320 bpp higher than MPHC method in the best case, and 0.01 bpp, 0.039 bpp, 0.061 bpp higher than MPHC method in the worst case, respectively. It is shown that the proposed method of adaptive Huffman codewords encoding has better performance than the MPHC method of predefined Huffman codewords encoding.

Keywords　encrypted domain; reversible data hiding; Huffman encoding; adaptively; separately

1　引　言

信息隐藏是现代互联网信息社会一项具有十分重要意义与商业价值的技术.传统的信息隐藏技术主要有数字水印和隐写术两个分支,数字水印主要用于多媒体的版本保护和完整性保护,而隐写术主要用于通信双方的隐蔽通信,侧重于信息的存在性和隐蔽性,其对应的攻击技术为隐写分析[1].传统信息隐藏技术在信息嵌入时或多或少都会对原始载体造成无法修复的失真,与传统的信息隐藏技术不同,可逆信息隐藏(Reversible Data Hiding,RDH)要求在秘密信息被提取后,能无损地恢复原始载体[2-4].由于可逆性的特点,可逆信息隐藏在军事、医学和法律等特殊多媒体应用领域发挥着重要作用.早期的数字图像可逆信息隐藏是通过无损压缩来实现的[5-6].一般来说,在给定的嵌入载荷下,一个好的可逆信息隐藏算法是期望最小化载体图像因嵌入数据而引起的失真.为了获得更好的率失真性能,近二十年来研究者们陆续提出了基于差分扩展[7-9]和基于直方图平移[10-11]的方法.差分扩展是通过扩大两个像素点之间的差异来嵌入数据,而直方图平移是利用图像直方图的峰值点来嵌入数据.这些可逆信息隐藏算法都获得了良好的率失真性能,但只能在图像的明文域实现.

近年来,随着云存储和云计算技术的日益成熟,人们的数据存储、图像处理等工作已经从原来的本地 PC(Personal Computer)转移到云服务器,导致出现了严重的安全问题,机密性、身份验证和完整性不断受到威胁.云存储和隐私保护的普及促使了密文域可逆信息隐藏(Reversible Data Hiding in Encrypted Images,RDHEI)技术的兴起.为了保护

云存储的数据和用户隐私，人们将数据发送到云服务器之前对其进行加密，从而催生了密文检索、密文去重等密文信号处理[1,12]技术，而 RDHEI 为这类密文图像处理提供了另一种途径和可能.

由于之前对隐私保护需求的关注不足，很多 RDHEI 的方法还停留在实验室研究层面，但随着人们对隐私保护需求的日益重视，这些信号处理与隐私保护的交叉性研究成果很快会从实验室走到实际应用中. RDHEI 是将秘密信息嵌入到加密图像而非明文图像[13-16]，该技术首先利用图像加密算法对原始明文图像进行加密，然后将秘密信息嵌入到加密图像中，且保证嵌入的秘密信息能够正确提取，并且原始明文图像能够无损恢复. 具体涉及到三方：内容所有者、信息隐藏者和接收者. 原始图像提供者(即内容所有者)在将原始图像发送到云服务器之前对其进行加密. 云服务管理者(即信息隐藏者)在不知道原始明文图像或加密密钥的情况下将秘密信息嵌入到加密图像中. 对于合法的接收方，他既可以提取秘密信息，又可以恢复原始的明文图像.

RDHEI 技术具有图像内容隐私保护和可逆信息隐藏的双重功能. 加密的目的是通过完全或部分随机化原始图像的内容来保护用户的隐私. 加密算法的广泛应用使得密文域信号处理被推广，但加密算法为 RDHEI 技术提供了良好平台的同时也提出了新的挑战：密文域信号丧失了明文域的结构冗余，导致明文域的可逆信息隐藏算法在密文域失效. 目前已发表的 RDHEI 技术主要分为三类：(1)加密后腾出空间的 VRAE(Vacating Room After Encryption)方法[13,17]；(2)加密的同时腾出空间的 VRBE(Vacating Room By Encryption)方法[18]；(3)加密前预留空间的 RRBE(Reserving Room Before Encryption)方法[19-23]. 由于加密操作破坏了原始明文图像的空间相关性，因此 VRAE 方法很难获得令人满意的有效载荷. VRBE 方法是利用一些特殊的加密方案对原始明文图像进行加密，同时在加密后的图像中保留了部分空间相关性. 由于 VRBE 方法没有充分利用原始明文图像的空间冗余，因此其有效载荷也受到限制. 与 VRAE 和 VRBE 方法不同，RRBE 方法充分利用原始明文图像的空间相关性，在图像加密前预留空间. 其优点是提高了密文域可逆信息隐藏的有效载荷，并且原始明文图像和秘密信息可实现分离的无损恢复和提取. 不足之处是由于在图像加密前预留秘密信息的嵌入空间，增加了内容所有者的计算负担，一定程度上降低了用户体验. 但随着用户端计算能力的大幅度提升，这个不足之处的影响也逐步被忽略.

在早期的 RDHEI 方法中，图像恢复和秘密信息的提取是需要同时进行的[13]. 为了分离图像恢复和秘密信息提取的过程，文献[18-23]等提出了分离的密文域可逆信息隐藏算法.

文献[19]首次提出使用图像的最高位平面 MSB(Most Significant Bit)替换来嵌入秘密信息，文中提出了两种方法：CPE-HCRDH(High-Capacity Reversible Data Hiding with Correction of Prediction Errors)方法和 EPE-HCRDH(High-Capacity Reversible Data Hiding with Embedded Prediction Errors)方法. 在 CPE-HCRDH 方法中，为了避免所有的预测误差，对原始明文图像进行了轻微的修改. 流密码加密后，通过替换加密图像中的 MSB 平面，有效载荷能达到 1 位/像素. 在 EPE-HCRDH 方法中，通过分析原始明文图像的内容，以 8 个像素为一块，突出显示预测误差，建立误差定位二值图，并先将预测误差位置信息根据误差定位二值图存储到加密图像中. 因此，通过替换加密图像中的大部分 MSB 值，有效载荷能接近 1 位/像素. 由于原始明文图像的 MSB 预测比 LSB(Least Significant Bit)预测更容易，且在密文域图像质量恶化不是问题，因此文献[19]获得了较高的有效载荷. 在数据提取阶段，可以直接从 MSB 平面中提取秘密信息并解密. 在图像恢复阶段，由于明文图像的空间相关性，可以根据 MSB 预测来恢复原始图像. 在 CPE-HCRDH 方法中，原始明文图像由于被修改不能完全恢复，但图像的重构质量也很高. EPE-HCRDH 方法嵌入了预测误差位置信息，可以无损地恢复原始明文图像.

然而在文献[19]中，只使用了一个 MSB 平面来嵌入秘密信息，所以有效载荷等于或低于 1 位/像素. 基于文献[19]，文献[20]提出 TMP(Two-MSB Prediction)算法，通过两个 MSB 平面(即最高位 MSB 和次高位 MSB)替换来嵌入秘密信息，使得有效载荷可以超过 1 位/像素.

文献[21]将原始明文图像分成 8 个位平面，重新排列位平面中的比特流生成一个可以有效压缩的比特流，提出 ERLC-BMPR(Extended Run-Length Coding and Block-based MSB Plane Rearrangement)算法. 因并不是所有的位平面都可以被有效压缩，所以该方法只压缩前面连续可压缩的高位位平面. 在 ERLC-BMPR 方法中，选择使用行程编码压缩算法来压缩比特流，在腾出的空间嵌入低位位平面，使用

流密码加密已包含可嵌入空间的图像，最后将加密的秘密信息通过比特替换嵌入到已腾出空间的低位位平面中. 当收到已嵌入秘密信息的载密图像时，接收方可以直接提取加密的秘密信息，并通过数据隐藏密钥对其进行解密，得到原始秘密信息. 如果接收方拥有图像的加密密钥，则可以对图像进行解密，并对压缩的位平面进行解压缩以恢复原始明文图像.

文献[18]提出了一种 VRBE 可分离的 PBTL (Parametric Binary Tree Labeling)算法，利用小图像块内的局部相关性和参数二叉树标记来嵌入秘密信息. 然而，文献[18]使用的图像冗余只局限在小图像块而非整个原始图像，因此有效载荷也不是很理想. 基于文献[18]的方法，文献[22]提出了一种改进的基于参数二叉树标记的密文域可逆信息隐藏算法(Improved Parametric Binary Tree Labeling，IPBTL). 该方法利用整个图像的空间冗余，进一步提高了有效载荷. IPBTL 使用参数二叉树将加密后的图像像素标记为两个不同的类别，并结合预测误差对加密后的像素分组为参考像素、特殊像素、可嵌入像素和不可嵌入像素；最后，在可嵌入像素的分组中通过比特替换来嵌入秘密信息. 在数据提取阶段，IPBTL 方法检测二叉树的标记信息，从可嵌入像素分组中提取信息并解密. 在该方法中，图像的恢复即对参考像素、特殊像素、可嵌入像素和不可嵌入像素四个分组的恢复. 由于参考像素在数据嵌入过程并未改变，可以直接解密恢复. 根据辅助信息，恢复不可嵌入像素和特殊像素. 按照从左往右、从上往下的先行后列顺序，参考已恢复的邻居像素，由中值预测器可获得当前像素的预测值，结合二叉树标记的预测误差，IPBTL 方法即可恢复当前可嵌入像素的像素值，从而恢复了整个原始图像.

文献[23]突破了文献[18]和文献[22]的等长编码思想，提出利用变长哈夫曼编码实现具有更高有效载荷的 MPHC(multi-MSB Prediction and Huffman Coding)算法. 该方法采用预定义的 9 个哈夫曼码字{00，01，100，101，1100，1101，1110，11110，11111}来编码压缩像素的位图. 将原始像素值和预测像素值分别转换成 8 位二进制形式，从最高位有效位到最低位有效位，逐位比较两个二进制，直到某对比特值不相同，相同的比特数即为该像素点的位图标记值. 统计整个图像的位图标记值，将较短的码字分配给较多的标记值，将较长的码字分配给较少的标记值. 最后将预定义的 9 个码字信息以及编码生成的位图二进制序列作为辅助信息，并在编码压缩后得到的冗余空间嵌入秘密信息. 在数据提取与图像恢复阶段，MPHC 算法首先根据提取的辅助信息恢复整个图像的位图. 按照从左往右、从上往下的先行后列顺序从载密图像中提取相应比特位的秘密信息，由数据隐藏密钥解密得到原始的秘密信息. 原始明文图像的恢复只需要根据预测像素值和位图即可恢复，其中预测像素值由中值预测器检测获得.

但文献[23]采用的是预定义的 9 个哈夫曼编码码字，这对不同的图像来说，并非是最优的变长编码. 本文基于文献[23]，提出了一种基于自适应哈夫曼编码的密文域可逆信息隐藏算法，对不同的图像采用的是不同的码字，而非统一的预定义码字. 具体来说，该方法首先利用自然图像相邻像素间的相关性对原始明文图像进行像素值预测，从最高有效位开始，每对原始像素值和预测像素值的相同比特位被存储到位图中并进行自适应的哈夫曼编码标记. 然后，利用流密码对原始明文图像进行加密. 最后在腾出的空间中，通过位替换来自适应地嵌入秘密信息. 利用自适应的哈夫曼码字编码可以更好地压缩位图，同时由于编码和解码的可逆性，合法接收者可以对原始明文图像和秘密信息实现分离的无损恢复和提取.

本文基于自适应的哈夫曼编码方案设计了一种 RRBE 的 RDHEI 算法，主要贡献包括以下 3 个方面：

(1) 可以探索更大的数据嵌入空间，从而获得更高的有效载荷；

(2) 根据概率分布分配不同长度的码字，可使平均码长最短，实现了最优编码的选择；

(3) 对不同的图像采用不同的码字，增强了信息嵌入过程的安全性.

2　哈夫曼编码

哈夫曼编码依据出现的概率来构造平均长度最短的码字，是一种异字头的可变字长编码. 它的基本方法是先扫描信源符号，统计出各符号出现的概率，按概率的大小分配不同长度的码字，由此构造一张该信源符号平均长度最短的编码表. 若信源符号有 u_1，u_2，u_3 三种，对应概率分别为 $P_1=0.1$，$P_2=0.1$，$P_3=0.8$. 编码时，首先将三种符号按照概率从小到大排队，从两个最小概率的符号开始，可选标记其中一个支路为 0，另一个支路为 1. 再将已编码的两条支路的概率合并，重新排队. 重复上述过程，直至合并概率归一时为止. 最后将路线上所遇到的 0 和 1 逆序排序，就是该符号的哈夫曼码字. 如图 1 所示，u_2 的哈夫曼码字为‘01’.

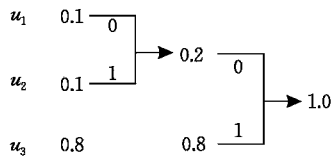


图 1 哈夫曼编码原理

哈夫曼编码后记录的是每个符号的码字，而码字与实际符号的对应关系记录在码表中，图 1 的码表如图 2 所示.

信源符号	概率分布	码字	码长
u_1	0.1	00	2
u_2	0.1	01	2
u_3	0.8	1	1

图 2 哈夫曼码表

然而，哈夫曼编码的结果并不是唯一的，其原因之一是概率统计时，可能出现相等的概率，造成排队方法不唯一；另一原因是在编码标记过程中，0 和 1 的分支选择不固定，导致可以出现不同的编码结果. 但出现概率高的字符都被分配较短的码字，反之出现概率低的则都被分配较长的码字，哈夫曼编码保证了按概率分布分配码字，可使平均码长最短，从而达到无损压缩数据的目的.

3 本文算法

本文提出的基于自适应哈夫曼编码的密文域可逆信息隐藏算法的结构如图 3 所示，包括图像预测、自适应的哈夫曼编码、图像加密、位图嵌入、信息嵌入、信息提取和图像恢复 7 个部分.

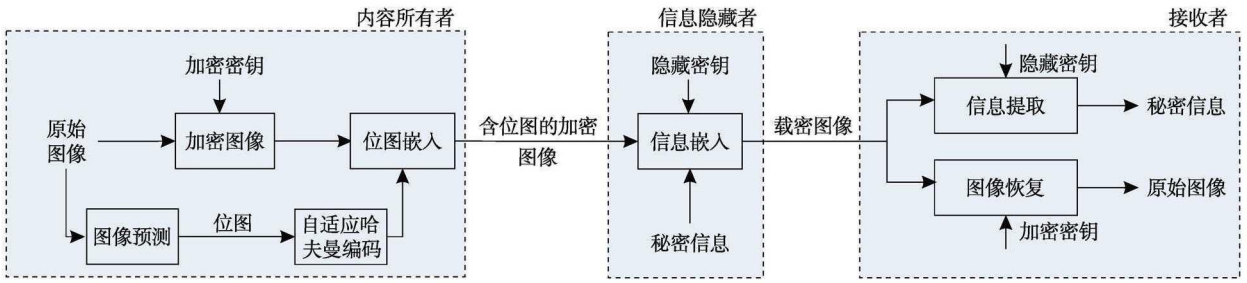


图 3 算法框架示意

原始图像所有者利用自然图像相邻像素间的相关性对原始明文图像进行像素值预测；从最高有效位到最低有效位，每对原始像素值和预测像素值的相同比特位被存储到位图中并进行自适应的哈夫曼编码标记. 利用流密码对原始明文图像进行加密，将已编码压缩的位图嵌入到加密图像中.

信息隐藏者获得含位图的加密图像后，在腾出的空间，根据隐藏密钥，通过位替换来自适应地嵌入秘密信息.

在信息提取和图像恢复阶段，由于哈夫曼编码和解码的可逆性，拥有数据隐藏密钥的合法接收者可以提取加密的秘密信息，并通过密钥对其进行解密，得到原始秘密信息. 拥有图像加密密钥的合法接收者可以无损地恢复原始明文图像. 当同时拥有两把密钥时，合法接收者既能提取原始秘密信息，也能无损恢复原始明文图像.

3.1 图像预测

在本文的算法中，采用中值预测器 MED(Median Edge Detector)[8]对原始明文图像进行像素值预测. 该预测器将图像中的第 1 行和第 1 列作为参考像素，并根据当前像素的左、上和左上相邻像素来预测当前像素.

如图 4 所示，c,b,a 为 x 的左、上和左上三个相邻像素，由式(1)，则可得 x 的预测值 px.

$$px=\begin{cases}\max(b,c), & a\leq\min(b,c)\\ \min(b,c), & a\geq\max(b,c)\\ b+c-a, & \text{其他}\end{cases} \tag{1}$$

a	b
c	x

图 4 中值预测器

3.2 自适应的哈夫曼编码

本小节以实例来说明自适应哈夫曼编码的标记过程. 图 5 为 8×8 的来自 Lena 图像中的像素块，代

162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
164	164	158	155	161	159	159	160
160	160	163	158	160	162	159	156
159	159	155	157	158	159	156	157

图 5 原始图像

表原始图像 I. 由 3.1 节可知，图 6 为图 5 的预测像素值，其中第 1 行和第 1 列为参考像素，在像素值预测过程中保持不变.

162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
162	162	162	161	162	157	163	161
164	164	164	158	156	157	163	159
160	160	158	160	161	159	162	160
159	159	162	155	159	160	159	156

图 6　预测图像

由式(2)将图 5 和图 6 中对应的原始像素值 x 和预测像素值 px 分别转换为 8 位二进制形式：

$$x^k(i,j)=\lfloor x(i,j)/2^{k-1}\rfloor \bmod 2,\ k=1,2,\cdots,8 \quad (2)$$

其中$\lfloor\ \rfloor$为向下取整运算，$2\le i\le m$，$2\le j\le n$，$m\times n$ 为图像的大小，这里 $m=8$，$n=8$，k 为转化后二进制的 8 个相应比特位，$x(i,j)$为转化前的整数像素值，$x^k(i,j)$为对应 $x(i,j)$转换后的 8 位二进制.

从最高有效位到最低有效位，逐位比较 x 和 px 转换后的 8 位二进制，直到某对比特位不相同，相同的比特位数即为该像素点的标记值，如图 7 所示.

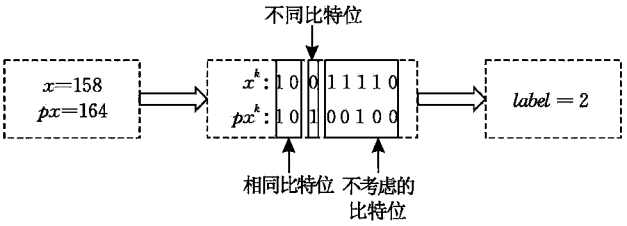


图 7　像素标记过程

将图 5 与图 6 中的每对原始像素值和预测像素值的相同比特位逐一标记后，可得位图如图 8(a)所示. 因参考像素不参与标记，可将其标记值记为−1. 统计图 8(a)中各标记值的分布概率并进行自适应哈夫曼码字编码，如图 8(b)所示. 由此可知位图转换成二进制序列长度[23]为

$$Lm=\sum_{t=0}^{8}(g_t\times\lambda_t) \quad (3)$$

−1	−1	−1	−1	−1	−1	−1	−1
−1	8	8	8	8	8	8	8
−1	8	8	8	8	8	8	8
−1	8	8	8	8	8	8	8
−1	8	8	8	8	8	8	8
−1	8	2	5	2	6	2	2
−1	8	2	2	7	2	2	2
−1	8	2	5	7	2	6	7

(a) 位图

信源符号	个数统计	概率分布	码字	码长
2	11	0.2245	01	2
5	2	0.0408	0010	4
6	2	0.0408	0011	4
7	3	0.0612	000	3
8	31	0.6327	1	1

(b) 哈夫曼码表

图 8　位图及对应的哈夫曼码表

其中 g_t为码表中标记值 t 的个数，λ_t为对应的码长. 则码表中码字 h_t与实际标记值 t 的对应关系、位图的二进制序列长度 Lm 和位图具体的 Lm 位二进制序列构成了位图信息，即存储结构构成如图 9 所示.

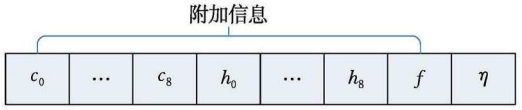


图 9　位图信息存储结构

其中，$c_t(t=0,1,\cdots,8)$为 λ_t对应的二进制形式，分别用 4 位可足够存储，由 $c_t(t=0,1,\cdots,8)$和$h_t(t=0,1,\cdots,8)$可确定码字 h_t与实际标记值 t 的对应关系；f 为整数 Lm 对应的二进制形式，对 $m\times n$ 的图像用$\lceil\log_2 m\rceil+\lceil\log_2 n\rceil+2$ 位存储，$\lceil\ \rceil$为向上取整运算；则 $c_t(t=0,1,\cdots,8)$，$h_t(t=0,1,\cdots,8)$和 f 可视为附加信息；η 为位图具体的 Lm 位二进制序列.

3.3　图像加密

对原始明文图像进行像素值预测和自适应哈夫曼编码位图后，采用流密码对原始明文图像 I 进行加密. 利用图像加密密钥 k_e，生成一个和原始明文图像同样大小 $m\times n$ 的伪随机矩阵 $\boldsymbol{R}$. 根据式(2)将 I 和 $\boldsymbol{R}$ 转化为二进制形式 $x^k(i,j)$和 $r^k(i,j)$，则

$$x_e^k(i,j)=x^k(i,j)\oplus r^k(i,j),\ k=1,2,\cdots,8 \quad (4)$$

其中，$\oplus$为按位异或操作，$1\le i\le m$，$1\le j\le n$，$x_e^k(i,j)$表示加密后的 8 位二进制. 最终，加密图像 I_e的像素 $x_e(i,j)$为

$$x_e(i,j)=\sum_{k=1}^{8}x_e^k(i,j)\times 2^{k-1},\ k=1,2,\cdots,8 \quad (5)$$

3.4 位图嵌入

为了腾出嵌入秘密信息的空间，需要在信息隐藏之前先嵌入位图信息. 在加密图像 I_e 中，为了保证嵌入后的位图信息能够正确提取，需要先将部分位图信息存储在第 1 行和第 1 列的参考像素中(在一些纹理粗糙的图像中，为了在后续的操作中能完全提取位图信息，可以设置多个行和列作为参考像素). 然后，按照从左往右、从上往下的先行后列顺序，将另一部分位图信息和参考像素嵌入到加密图像 I_e 中的非参考像素部分[23]：

$$x'_e(i,j)=\begin{cases}x_e(i,j)\bmod 2^{7-t}+\sum_{s=0}^{t}(b_s\times 2^{7-s}), & 0\le t\le 6\\ \sum_{s=1}^{8}(b_s\times 2^{8-s}), & 7\le t\le 8\end{cases} \quad (6)$$

其中 b_s 为要嵌入的信息，t 为 I_e 中当前像素 $x_e(i,j)$ 的位图标记值. 在嵌入位图信息和参考像素后，得到加密图像 I'_e.

3.5 信息嵌入

在信息隐藏前，从加密图像 I'_e 中提取位图信息. 首先，从第 1 行和第 1 列中提取部分位图信息，得到码表中码字 h_t 与实际标记值 t 的对应关系和位图的二进制序列长度 Lm 及部分位图的具体二进制序列. 然后按照从左往右、从上往下的先行后列顺序，根据已有的位图信息得到当前像素的标记值 t，继续提取 s 位的位图信息[23]：

$$s=\begin{cases}t+1, & 0\le t\le 7\\ t, & t=8\end{cases} \quad (7)$$

在获取完整的位图信息后，由码字 h_t 与实际标记值 t 的对应关系恢复位图. 最后，为了进一步提高信息隐藏的安全性，在嵌入秘密信息前使用数据隐藏密钥 k_d 对其进行加密. 根据位图和式(6)，将加密后的秘密信息嵌入到加密图像 I'_e 的预留空间中，生成最终载密图像 I_{ew}.

对于给定的一幅 $m\times n$ 的原始图像，由 MED 生成的预测图像是确定的，对原始图像和预测图像的像素逐一标记后可得该图像的位图. 当获得图像的位图后，根据标记值 t 及其对应的统计个数 g_t，就可以计算出该图像的总嵌入容量 N：

$$N=\sum_{t=0}^{6}g_t\times(t+1)+\sum_{t=7}^{8}g_t\times 8 \quad (8)$$

则净嵌入容量 N_r 为式(9)所示，最终的嵌入率 r 由式(10)计算：

$$N_r=N-\left(4\times 9+\sum_{t=0}^{8}\lambda_t+\lceil\log_2 m\rceil+\lceil\log_2 n\rceil+2\right)-Lm \quad (9)$$

$$r=\frac{N_r}{m\times n}=\frac{N-\left(4\times 9+\sum_{t=0}^{8}\lambda_t+\lceil\log_2 m\rceil+\lceil\log_2 n\rceil+2\right)-Lm}{m\times n} \quad (10)$$

可见该类算法的嵌入率上界为

$$r=\frac{N_r}{m\times n}<\frac{N}{m\times n} \quad (11)$$

采用更优的自适应哈夫曼码字编码，以获得更短的位图二进制序列长度 Lm，进而使得 N_r 更加逼近 N，可提高嵌入率.

3.6 信息提取

合法接收者在提取秘密信息前，先从载密图像 I_{ew} 第 1 行和第 1 列中提取部分位图信息. 通过这些位图信息，用 3.5 节同样的方法提取全部位图信息、参考像素和加密的秘密信息. 将提取的参考像素放回第 1 行和第 1 列，得图像 I'_{ew}. 如果接收者只拥有数据隐藏密钥 k_d，则可以通过解密已提取的秘密信息来获取原始的秘密信息. 然而，由于没有图像加密密钥 k_e，原始明文图像无法重建.

3.7 图像恢复

拥有图像加密密钥 k_e 的接收者可以由 k_e 生成伪随机矩阵 $\boldsymbol{R}$，由式(4)对 I'_{ew} 进行解密处理，得到解密后的图像 I''_{ew}. 此时，除参考像素完全恢复外，其它每一个非参考像素的前 t 位或 $(t+1)$ 位与原始像素不同. 因为这些像素根据位图中相应标记值 t 嵌入了 t 位或 $(t+1)$ 位信息. 按照从左往右、从上往下的先行后列顺序，依次恢复 I''_{ew} 中的非参考像素. 由式(1)计算当前像素 $x''_{ew}(i,j)$ 的预测值 $px(i,j)$，当 $t\le 7$ 时，原始像素 $x(i,j)$ 的高 t 位 MSB 等于对应的 $px(i,j)$，而第 $(t+1)$ 位 MSB 可以通过对 $px(i,j)$ 的第 $(t+1)$ 位 MSB 求反得到. 当 $t=8$ 时，原始像素 $x(i,j)$ 与其预测值 $px(i,j)$ 相同. 重构过程如下[23]：

$$x(i,j)=\begin{cases}g_1+g_2+x''_{ew}(i,j)\bmod 2^{7-t}, & 0\le t\le 7\\ px(i,j), & t=8\end{cases} \quad (12)$$

其中 $g_1=px(i,j)^{tMSB}$ 为 $px(i,j)$ 的高 t 位 MSB 值，$g_2=(px(i,j)^{t+1}\oplus 1)\times 2^{7-t}$，$px(i,j)^{t+1}$ 为 $px(i,j)$ 的第 $(t+1)$ 位 MSB 值，$\oplus$ 为位异或运算. 由此恢复每一个非参考像素，最后得到无损的原始明文图像 I.

本文算法可以对原始明文图像和秘密信息实现

分离的无损恢复和提取，拥有数据隐藏密钥 k_d 的合法接收者可以提取原始的秘密信息，拥有图像加密密钥 k_e 的合法接收者能无损地恢复原始明文图像. 当同时拥有数据隐藏密钥 k_d 和图像加密密钥 k_e 时，合法接收者既能正确地提取原始的秘密信息，也能无损地恢复原始明文图像.

4　实验结果与分析

为了验证本文所提算法的有效性，在仿真实验中对 5 幅标准的 512×512 灰度图像进行了性能测试，如图 10 所示. 此外，还分别测试了 BOSSBase[24]、BOWS-2[25] 和 UCID[26] 三个数据集，其中 BOSSBase 数据集和 BOWS-2 数据集各有 10 000 张 512×512 的灰度图像，UCID 数据集有 1388 张灰度图像，图像大小有 512×384 和 384×512 两种. 密文域可逆信息隐藏算法的目标是在秘密信息提取的错误比特数、有效载荷和重构图像质量之间找到最佳的平衡. 本文算法可以对原始明文图像和秘密信息实现分离的无损恢复和提取，所以本文的目标是追求更高的嵌入率. 为了定量说明算法的性能，使用峰值信噪比 *PSNR*(Peak Signal-to-Noise Ratio) 和结构相似度 *SSIM*(Structural Similarity) 两个指标来评价原始明文图像的恢复质量，并使用平均每像素所嵌入的比特数(bit per pixel，bpp)，即嵌入率作为客观评判有效载荷的关键指标.

(a) Lena　(b) Baboon　(c) Jetplane　(d) Airplane　(e) Tiffany

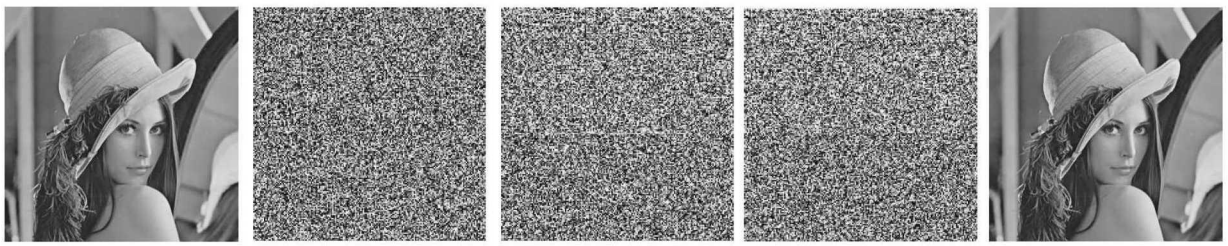
图 10　测试图像

4.1　安全性分析

图 11 以 Lena 图像为例，给出了本文算法在不同阶段所产生的不同图像. 图 11(a) 为原始图像 I. 图 11(b) 为利用加密密钥 k_e 得到的加密图像 I_e. 嵌入位图信息后的图像 I'_e 如图 11(c) 所示. 图 11(d) 为最终载密图像 I_{ew}，嵌入率为 2.617 bpp. 恢复后的图像如图 11(e) 所示，与原始图像图 11(a) 间的 $PSNR\to+\infty$，$SSIM=1$，表示与其完全相同.

本文利用流密码对原始图像进行加密，可以隐藏图像的特征信息. 对于一个 $m\times n$ 的灰度图像，伪随机矩阵 $\boldsymbol{R}$ 中的二进制序列长度为 $m\times n\times 8$，序列中的每位可能是 0 或 1，即该伪随机序列总共有 $2^{m\times n\times 8}$ 种可能. 在没有加密密钥 k_e 的情况下，获得一个完全正确的加密序列概率为 $1/2^{m\times n\times 8}$，如此低的概率说明本文的加密方法在安全性方面得到了保证. 同理，为提高信息隐藏的安全性，本文在嵌入秘密信息前使用数据隐藏密钥 k_d 对其进行流加密，对于长度为 num 的秘密信息，k_d 的密钥空间为 2^{num}，获得一个完全正确的加密序列概率为 $1/2^{num}$，同样能确保秘密信息的安全.

密文可逆信息隐藏需要保护原始图像内容不被泄露，图 11(b)、(c) 和 (d) 是图 11(a) 的三个加密版本，可以看出，从图 11(b)、(c) 和 (d) 中很难检测到图 11(a) 的内容. 其中图 11(c) 和 (d) 中因有位图信息的嵌入可能呈现出一定的特征，但与原始图像内容无关，无法从图 11(c) 和 (d) 中得到原始图像内容. 为了进一步定量测试算法的安全性，表 1～表 3 给出了测试图像的三个加密版本与对应原始图像间



(a) 原始图像　(b) 加密图像　(c) 含位图的加密图像　(d) 载密图像 (嵌入率 r=2.617bpp)　(e) 恢复的图像 ($PSNR\to+\infty$, $SSIM$=1)

图 11　本文算法对 Lena 图像的实验结果

的 *PSNR* 和 *SSIM* 值. 表 4、表 5 给出了数据集中三个加密版本图像与对应原始图像间的平均 *PSNR* 和 *SSIM* 值. 可以看出每个 *PSNR* 值都非常低，*SSIM* 值几乎为 0，这意味着本文算法具有较高的安全级别，可以有效地保护原始图像内容所有者的隐私.

表 1 加密图像与对应原始图像的 *PSNR* 和 *SSIM* 值

加密图像 I_e	*PSNR*/dB	*SSIM*
Lena	9.2255	0.0341
Baboon	9.5108	0.0299
Jetplane	8.0077	0.0346
Airplane	8.9521	0.0403
Tiffany	6.8839	0.0389

表 2 含位图的加密图像与对应原始图像的 *PSNR* 和 *SSIM* 值

含位图的加密图像 I'_e	*PSNR*/dB	*SSIM*
Lena	9.1754	0.0351
Baboon	9.4678	0.0361
Jetplane	8.3378	0.0361
Airplane	9.2331	0.0407
Tiffany	7.2487	0.0389

表 3 载密图像与对应原始图像的 *PSNR* 和 *SSIM* 值

载密图像 I_{ew}	*PSNR*/dB	*SSIM*
Lena	9.1676	0.0331
Baboon	9.4689	0.0382
Jetplane	8.3506	0.0374
Airplane	9.2403	0.0403
Tiffany	7.2520	0.0371

表 4 数据集中三个加密版本图像与对应原始图像的平均 *PSNR* 值

数据集	加密图像 I_e	含位图的加密图像 I'_e	载密图像 I_{ew}
BOSSbase	7.7203	7.5032	7.5053
BOWS-2	8.2902	8.3092	8.3140
UCID	7.8876	7.8299	7.8361

表 5 数据集中三个加密版本图像与对应原始图像的平均 *SSIM* 值

数据集	加密图像 I_e	含位图的加密图像 I'_e	载密图像 I_{ew}
BOSSbase	0.0273	0.0266	0.0269
BOWS-2	0.0327	0.0327	0.0331
UCID	0.0279	0.0275	0.0277

4.2 性能分析

在本文和文献[23]的 MPHC 算法中，当获得图像的位图后，就可以计算出该图像的总嵌入容量 N. 哈夫曼编码压缩位图后由码表映射关系可以计算出位图信息长度，从而得到净嵌入容量 N_r 和嵌入率 r. 表 6 还是以 Lena 图像为例，给出了本文和 MPHC 算法的具体编码压缩过程. 表 6 中第 1 行的 −1 代表参考像素的标记值，不参与编码；第 2 行和第 3 行是相应标记值 t 的个数统计 g_t 与概率分布；第 4 行显示了各标记值能嵌入的比特数(bits)；第 5 行计算了 Lena 图像的总嵌入容量 N，即 1 470 568 bits；MPHC 算法对位图编码的码字 h_t 和码长 λ_t 如表中第 6、7 行所示；第 8 行计算出了 MPHC 算法中位图编码后的二进制序列长度 Lm 为 793 304 bits；本文对位图编码的码字 h_t 和码长 λ_t 如表中第 9、10 行所示；第 11 行由式(3)计算出了本文算法对位图编码后的二进制序列长度 Lm 为 784 371 bits，比 MPHC 算法多压缩了 8933 bits. 表 7 给出了 5 幅测试图像的哈夫曼编码码字. 由表 7 可知，MPHC 算法对任意图像统一采用预定义的 9 个哈夫曼码字，该方法根据位图中标记值的个数统计来分配 9 个码字，将较短的码字分配给较多的标记值，将较长的码字分配给较少的标记值；而本文考虑到标记值统计的概率分布，根据概率分布采用自适应的哈夫曼码字，可使平均码长最短，实现了最优编码的选择，能更充分地压缩位图，从而可提高净嵌入容量 N_r 和嵌入率 r. 此外，由于 MPHC 算法统一采用预定义的 9 个哈夫曼码字，对某一幅图像的合法接收者在解密该幅图像而获取了该幅图像编码码字的同时，也相当于获取了其它图像的编码码字，导致其它图像被非法获取解密的可能性增加. 而本文方法对不同的图像采用不同的码字，这样无法从已解密的图像中来获取其它图像的编码码字，相对 MPHC 算法提高了编码安全性，即增强了信息嵌入过程的安全性.

表 6 Lena 图像的哈夫曼编码压缩过程

位图中的标记值 t		−1	0	1	2	3	4	5	6	7	8
个数统计 g_t		1023	9818	9742	15247	33246	44509	53359	41758	24353	29089
概率分布		/	0.0376	0.0373	0.0584	0.1273	0.1705	0.2043	0.1599	0.0933	0.1114
容量/bits		/	1	2	3	4	5	6	7	8	8
总嵌入容量 N/bits		9818×1+9742×2+15247×3+33246×4+44509×5+53359×6+41758×7+24353×8+29089×8=1470568									
MPHC 算法	码字 h_t	/	11110	11111	1110	101	01	00	100	1101	1100
	码长 λ_t	/	5	5	4	3	2	2	3	4	4
	位图长度 Lm/bits	9818×5+9742×5+15247×4+33246×3+44509×2+53359×2+41758×3+24353×4+29089×4=793304									
本文算法	码字 h_t	/	10111	10110	1010	100	111	00	110	010	011
	码长 λ_t	/	5	5	4	3	3	2	3	3	3
	位图长度 Lm/bits	9818×5+9742×5+15247×4+33246×3+44509×3+53359×2+41758×3+24353×3+29089×3=784371									

表 7　5 幅标准测试图像的哈夫曼编码码字

测试图像	码字	
	MPHC 算法	本文算法
Lena	00, 01, 100, 101, 1100, 1101, 1110, 11110, 11111	00, 111, 110, 100, 011, 010, 1010, 10110, 10111
Baboon	00, 01, 100, 101, 1100, 1101, 1110, 11110, 11111	00, 111, 110, 101, 011, 010, 1000, 10011, 10010
Jetplane	00, 01, 100, 101, 1100, 1101, 1110, 11110, 11111	00, 111, 110, 101, 100, 010, 0110, 01111, 01110
Airplane	00, 01, 100, 101, 1100, 1101, 1110, 11110, 11111	0, 111, 101, 100, 1101, 11001, 110001, 1100001, 1100000
Tiffany	00, 01, 100, 101, 1100, 1101, 1110, 11110, 11111	00, 111, 110, 101, 100, 010, 0111, 01101, 01100

位图信息除了编码后的 Lm 位二进制序列，还包括用于存储哈夫曼码表中码字 h_t 与实际标记值 t 的对应关系和整数 Lm 对应二进制形式的附加信息. 表 8 给出了 5 幅测试图像的总嵌入容量、位图信息和有效载荷. 仍以 Lena 图像为例，MPHC 算法位图信息中的附加信息为 52 bits，而本文自适应于图像内容编码，要用更多的位来存储哈夫曼码表中码字 h_t 与实际标记值 t 的对应关系，共有 87 bits 附加信息，其中 36 bits($4\times9=36$，每个码字长度用 4 bits 存储)用于存储 9 个码字的长度，31 bits 用于存储自适应的 9 个码字信息，另 20 bits 用于存储整数 Lm 对应的二进制形式. 由表 8 可知，在 MPHC 算法中，Lena 图像最后的净嵌入容量为 677 212 bits，即嵌入率为 2.583 bpp，而本文算法的净嵌入容量为 686 110 bits，即嵌入率为 2.617 bpp. 其它几幅标准测试图像的结果，如表 8 所示，本文算法的有效载荷比 MPHC 算法均有提高.

为了不受选取测试图像随机性的影响，表 9 给出了三个数据集的测试结果. 对于纹理平滑的图像来说，位图中的标记值大概率分布在偏大的 6、7 和 8 值上，有效载荷较大. 相反，对于纹理粗糙的图像，位图中的标记值大概率分布在偏小的 0、1、2 值上，有效载荷较小. 如在数据集 BOSSBase 中，嵌入率在最佳情况下为 6.856 bpp，而在最差情况下仅有 0.674 bpp. 同样，数据集 BOWS-2 中嵌入率在最佳情况下为 6.419 bpp，最差情况下为 0.667 bpp；数据集 UCID 中嵌入率在最佳情况下为 5.330 bpp，最差情况下为 0.458 bpp. 三个数据集的平均嵌入率分别为 3.451 bpp、3.308 bpp 和 2.748 bpp. 相对 MPHC 算法，三个数据集的最高嵌入率、最低嵌入率和平均嵌入率均有所提高，尤其是对纹理平滑的图像，在最佳情况下，本文算法的嵌入率比 MPHC 算法分别高出 0.958 bpp、0.797 bpp 和 0.320 bpp. 在最差情况下，本文算法的嵌入率比 MPHC 算法也分别高出 0.01 bpp、0.039 bpp 和 0.061 bpp. 平均嵌入率比 MPHC 算法分别提高了 0.09 bpp、0.062 bpp 和 0.06 bpp. 另表 9 中的 $PSNR\to+\infty$ 和 $SSIM=1$，说明只要拥有图像加密密钥，本文和 MPHC 算法都可以实现对原始明文图像的无损恢复.

本文采用自适应的哈夫曼码字编码，根据位图

表 8　5 幅标准测试图像的总嵌入容量、位图信息和有效载荷

测试图像	总嵌入容量 N/bits	位图长度 Lm/bits		附加信息/bits		净嵌入容量 N_r/bits		嵌入率 r/bpp	
		MPHC	本文	MPHC	本文	MPHC	本文	MPHC	本文
Lena	1470568	793304	784371	52	87	677212	686110	2.583	2.617
Baboon	1074384	794941	786599	52	87	279391	287698	1.066	1.098
Jetplane	1587880	793441	778244	52	87	794387	809549	3.030	3.088
Airplane	1659203	682803	657136	52	95	976348	1001972	3.724	3.822
Tiffany	1526934	786527	769862	52	87	740355	756985	2.824	2.888

表 9　三个数据集的测试结果

评价指标		数据集								
		BOSSbase			BOWS-2			UCID		
		嵌入率 r/bpp	$PSNR$/dB	$SSIM$	嵌入率 r/bpp	$PSNR$/dB	$SSIM$	嵌入率 r/bpp	$PSNR$/dB	$SSIM$
最佳	MPHC 算法	5.898	$+\infty$	1	5.622	$+\infty$	1	5.010	$+\infty$	1
	本文算法	6.856	$+\infty$	1	6.419	$+\infty$	1	5.330	$+\infty$	1
	载荷增量	0.958	/	/	0.797	/	/	0.320	/	/
最差	MPHC 算法	0.664	$+\infty$	1	0.628	$+\infty$	1	0.397	$+\infty$	1
	本文算法	0.674	$+\infty$	1	0.667	$+\infty$	1	0.458	$+\infty$	1
	载荷增量	0.010	/	/	0.039	/	/	0.061	/	/
平均	MPHC 算法	3.361	$+\infty$	1	3.246	$+\infty$	1	2.688	$+\infty$	1
	本文算法	3.451	$+\infty$	1	3.308	$+\infty$	1	2.748	$+\infty$	1
	载荷增量	0.090	/	/	0.062	/	/	0.060	/	/

中标记值的概率分布对不同的图像采用不同的编码码字，相对采用预定义码字编码的 MPHC 算法，提高了编码安全性，同时也提高了嵌入率.

4.3 与其它同类算法的对比

图 12 和图 13 给出了本文和其它 5 种同类算法的对比结果. 为了客观公平比较，设置最佳参数以使得对比算法能获得更好的性能，仿真实验中将 PBTL 算法的参数 α 和 β 分别设置为 5 和 2，块大小设置为 3×3；IPBTL 算法中的 α 和 β 同样设置为 5 和 2；ERLC-BMPR 算法中块的大小设置为 4×4，并且固定码字长度设置为 3.

图 12 对 5 幅标准测试图像的嵌入率进行比较，在 EPE-HCRDH 方法中，嵌入率小于 1 bpp，这是因为 EPE-HCRDH 算法只替换了一位 MSB 来嵌入秘密信息. TMP 算法通过替换 2 位 MSB，使得嵌入率可高于 1 bpp. PBTL 算法、ERLC-BMPR 算法和 IPBTL 算法在 5 幅标准测试图像上都获得了较高的嵌入率. 而本文采用自适应的哈夫曼码字编码来压缩位图，只有 Lena 图像的嵌入率略逊于 IPBTL 算法，其它测试图像，包括纹理粗糙的 Baboon 图像，相对同类算法，本文算法均获得了最高嵌入率. 图 13 比较了本文和该 5 类算法在三个数据集上的平均嵌入率. 如图 13 所示，本文算法均取得了最高嵌入率，进一步说明了本文算法具有更好的性能.

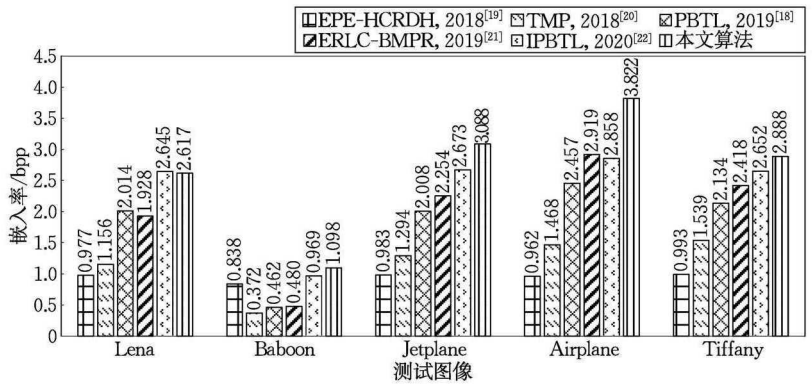


图 12 不同方法在 5 幅标准测试图像上的嵌入率

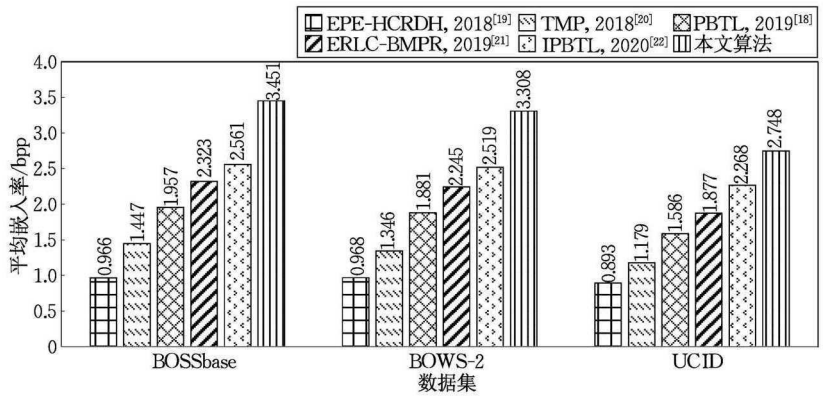


图 13 不同方法在三个数据集中的平均嵌入率

4.4 运行时间分析

密文域可逆信息隐藏涉及到内容所有者、信息隐藏者和接收者三方. 其中内容所有者的运行时间将直接影响用户体验. 本文算法主要包括图像预测，自适应的哈夫曼编码，图像加密，位图嵌入、信息嵌入，信息提取和图像恢复 7 个部分，其中前 4 个部分由内容所有者完成. 为了测试本文和相关算法内容所有者的运行时间，在 CPU 为 Intel(R) Core(TM) i5-6200U，主频为 2.30 GHz，内存为 4.00 GB(3.89 GB 可用)的硬件配置环境，在 Windows 10 操作系统和 Matlab R2016a 实验平台，对数据集中不同大小的图像取 10 次运行的平均时间，结果如表 10 所示.

表 10 内容所有者的运行时间对比 (单位：s)

图像大小	EPE-HCRDH，2018[19]	TMP，2018[20]	PBTL，2019[18]	ERLC-BMPR，2019[21]	IPBTL，2020[22]	MPHC，2020[23]	本文算法
512×384	0.29	0.39	0.06	26.94	0.20	1.80	1.52
384×512	0.24	0.43	0.06	22.25	0.19	1.82	1.39
512×512	0.37	0.49	0.13	33.07	0.30	2.30	2.18

可以看出，文献[18]的 PBTL 算法为 VRBE 方法，内容所有者只需执行图像加密操作，所需时间最短. 在剩下均为 RRBE 的方法中，文献[19]的 EPE-HCRDH 算法和文献[20]的 TMP 算法，内容所有者在执行图像加密前需分别预测 1 位 MSB 和 2 位 MSB 并将预测误差位置信息存储到加密图像中，也有较高的运行效率；而文献[21]的 ERLC-BMPR 算法需要内容所有者对高位位平面的比特流进行重排和压缩，所需时间较长；文献[22]的 IPBTL 算法需由内容所有者根据预测误差进行二叉树标记，总体运行时间较短；而本文和文献[23]的 MPHC 算法在图像加密前对多位 MSB 进行位图标记，二者的主要区别在于位图压缩的编码方式，本文考虑位图标记值的概率分布，采用自适应码字的哈夫曼编码方式，而 MPHC 算法采用预定义码字的哈夫曼编码方式，其需要用一定的时间来确定预定义码字与实际标记值的对应关系，由表 10 可知，本文算法在运行时间上优于预定义码字的 MPHC 算法. 在图像大小为 512×512 时，本文算法的内容所有者运行时间为 2.18 s，在用户可接受的范围，可用于现实的应用场景.

5　总　结

当前制约密文域可逆信息隐藏发展的瓶颈之一是有效载荷低，而本文基于文献[23]提出了一种基于自适应哈夫曼编码的密文域可逆信息隐藏算法，可以探索更大的数据嵌入空间. 与现有的几种方法相比，本文利用位图中标记值的概率分布分配不同长度的码字，采用自适应的哈夫曼码字编码，能更充分地压缩位图，增强了信息嵌入过程的安全性，也达到了更高的嵌入率. 此外，由于哈夫曼编码和解码的可逆性，合法接收者可以对原始明文图像和秘密信息实现分离的无损恢复和提取. 未来的工作可从引入预测性能更优越的预测器和更适合位图压缩的编码方式两个方向来进一步提高有效载荷.

参　考　文　献

[1] Zhang Xin-Peng, Yin Zhao-Xia. Data hiding in multimedia. Chinese Journal of Nature, 2017, 39(2): 87-95(in Chinese)
(张新鹏，殷赵霞. 多媒体信息隐藏技术. 自然杂志，2017，39(2)：87-95)

[2] Chen X, Sun X, Sun H, et al. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. Journal of Systems and Software, 2013, 86(10): 2620-2626

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

[4] Li X, Zhang W, Gui X, et al. Efficient reversible data hiding based on multiple histograms modification. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 2016-2027

[5] Fridrich J, Goljan M, Du R. Lossless data embedding—New paradigm in digital watermarking. EURASIP Journal on Applied Signal Processing, 2002, 2002(2): 185-196

[6] Celik M U, Sharma G, Tekalp A M, et al. Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing, 2005, 14(2): 253-266

[7] Alattar A M. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Transactions on Image Processing, 2004, 13(8): 1147-1156

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

[9] 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

[10] Luo L, Chen Z, Chen M, et al. Reversible image watermarking using interpolation technique. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 187-193

[11] Li X, Zhang W, Gui X, et al. A novel reversible data hiding scheme based on two-dimensional difference-histogram modification. IEEE Transactions on Information Forensics and Security, 2013, 8(7): 1091-1100

[12] Puech W, Chaumont M, Strauss O. A reversible data hiding method for encrypted images//Proceedings of the 2008 Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Bellingham, USA, 2008, 6819: 68191E

[13] 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, 2016, 26(3): 441-452

[14] Wang Ji-Jun, Li Guo-Xiang, Xia Guo-En, Sun Ze-Rui. A separable and reversible data hiding algorithm in encrypted domain based on image interpolation space. Acta Electronica Sinica, 2020, 48(1): 92-100(in Chinese)
(王继军，李国祥，夏国恩，孙泽锐. 图像插值空间完全可逆可分离密文域信息隐藏算法. 电子学报，2020，48(1)：92-100)

[15] Xiang Shi-Jun, Luo Xin-Rong, Shi Shu-Xie. A novel reversible image watermarking algorithm in homomorphic encrypted domain. Chinese Journal of Computers, 2016, 39(3): 571-581(in Chinese)
(项世军，罗欣荣，石书协. 一种同态加密域图像可逆水印算法. 计算机学报，2016，39(3)：571-581)

[16] Liao X, Li K, Yin J. Separable data hiding in encrypted image based on compressive sensing and discrete Fourier

transform. Multimedia Tools and Applications, 2017, 76(20): 20739-20753

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

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

[19] Puteaux P, Puech W. An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1670-1681

[20] Puyang Y, Yin Z, Qian Z. Reversible data hiding in encrypted images with two-MSB prediction//Proceedings of the 2018 IEEE International Workshop on Information Forensics and Security (WIFS). Hong Kong, China, 2018: 1-7

[21] Chen K, Chang C C. High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement. Journal of Visual Communication and Image Representation, 2019, 58(2019): 334-344

[22] Wu Y, Xiang Y, Guo Y, et al. An improved reversible data hiding in encrypted images using parametric binary tree labeling. IEEE Transactions on Multimedia, 2020, 22(8): 1929-1938

[23] Yin Z, Xiang Y, Zhang X. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding. IEEE Transactions on Multimedia, 2020, 22(4): 874-884

[24] Bas P, Filler T, Pevný T. "Break our steganographic system": The ins and outs of organizing BOSS//Proceedings of the 13th International Workshop on Information Hiding. Prague, Czech Republic, 2011: 59-70

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

[26] Schaefer G, Stich M. UCID: An uncompressed color image database//Proceedings of the 2003 Storage and Retrieval Methods and Applications for Multimedia. Bellingham, USA, 2003: 472-481

WU You-Qing, M. S., lecturer. Her main research interests include information hiding and multimedia security.

GUO Yu-Tang, Ph. D., professor. His main research interests include pattern recognition and image processing.

TANG Jin, Ph. D., professor. His main research interests include image processing, pattern recognition, machine learning and computer vision.

LUO Bin, Ph. D., professor. His main research interests include pattern recognition and image processing.

YIN Zhao-Xia, Ph. D., associate professor. Her main research interests include information hiding and multimedia security.

Background

Reversible data hiding (RDH) in the plaintext image is a technique for hiding secret information by modifying the original cover image. After extracting the secret information, the original cover image can be completely restored. In the last decade, with the growing demand of cloud storage for user privacy protection, reversible data hiding in encrypted images (RDHEI) has aroused extensive research interest from the information hiding community, due to its potential applications when images are not allowed to be disturbed.

The RDHEI technology embeds secret information into encrypted images rather than plaintext images. In general, the reported RDHEI techniques can be classified into three categories, namely vacating room after encryption (VRAE), vacating room by encryption (VRBE) and reserving room before encryption (RRBE). In the previous RDHEI methods, data-extraction and image-recovery should be processed jointly. To separate the process of data-extraction and image-recovery, separable RDHEI methods have been studied.

In this paper, the authors provide an RRBE separable RDHEI method that follows Puteaux et al.'s work and is an improved method based on Yin et al.'s work. As with these methods, our proposed method allows perfect reversibility and error-free data-extraction. We aim to obtain the largest embedding rate. The experimental results show that the average embedding rate of the proposed method outperforms Yin et al.'s work 0.09 bpp, 0.062 bpp and 0.06 bpp on three datasets BOSSBase, BOWS-2 and UCID, respectively.

The research work in this paper is supported by the Major Project for New Generation of AI under Grant No. 2018AAA0100400, and by the National Natural Science Foundation of China (61872003, 61860206004). Under these supports, we are interested in finding the best balance between the number of erroneous extracted bits of the secret information, the embedding rate and the quality of the reconstructed image after data-extraction. In this area, we have published many papers in top journals and conferences, such as Refs. [20], [22] and [23].