

基于预测误差与位平面编码的密文域可逆信息隐藏算法

王海勇, 吉梦凝

(南京邮电大学计算机学院, 江苏 南京 210023)

摘要: 随着云计算技术的发展,越来越多的用户使用云备份的方式存储一些重要文件,与此同时,人们对于隐私保护的要求日益增长。密文域可逆信息隐藏是一种可以在密文图像中嵌入秘密信息,保证无错提取秘密信息以及无损恢复原始图像的技术,该技术既保护了载体图像的安全性,又有效地在网络中传递隐私信息,能够应用于云环境实现对用户的隐私保护,受到研究者的广泛关注。针对现有密文域可逆信息隐藏算法嵌入率较低的问题,提出了基于预测误差与位平面编码的密文域可逆信息隐藏算法,该算法重点研究如何在保证安全性和可逆性的同时,实现高嵌入容量。所提算法对图像进行预处理,根据位平面分布的不同分别使用不同的方式编码,在图像中预留出大量空间,通过重排列将预留的空间放在低位平面中;使用密钥生成随机矩阵,对图像进行加密,以保证图像的安全性;将秘密信息嵌入预留的空间中。在接收端,合法接收者能够根据密钥可分离来实现秘密信息的无错提取以及原始图像的无损恢复。与现有算法相比,所提算法具有更高的嵌入率,在 BOWS-2、BOSSBase 和 UCID 这 3 个数据集上平均嵌入率分别达到了 3.769 bit/pixel、3.874 bit/pixel 和 3.148 bit/pixel,分别比同类算法中性能最好的算法提升了 12.5%、6.9%和 8.6%。实验结果表明,所提算法能够充分利用图像的冗余性,有效提升嵌入率。

关键词: 可逆信息隐藏; 密文域; 游程编码; 分离; 信息安全

中图分类号: TP391

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023081

Reversible data hiding algorithm in encrypted images based on prediction error and bitplane coding

WANG Haiyong, JI Mengning

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: With the increasing use of cloud backup methods for storing important files, the demand for privacy protection has also grown. Reversible data hiding in encrypted images (RDHEI) is an important technology in the

收稿日期: 2023-02-16; 修回日期: 2023-08-18

通信作者: 王海勇, whynjupt@njupt.edu.cn

基金项目: 国家自然科学基金(61872190); 江苏省博士后科研资助计划项目(2020Z058)

Foundation Items: The National Natural Science Foundation of China (61872190), The Jiangsu Planned Projects for Postdoctoral Research Funds (2020Z058)

引用格式: 王海勇, 吉梦凝. 基于预测误差与位平面编码的密文域可逆信息隐藏算法[J]. 网络与信息安全学报, 2023, 9(6): 34-45.

Citation Format: WANG H Y, JI M N. Reversible data hiding algorithm in encrypted images based on prediction error and bitplane coding[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 34-45.

field of information security that allows embedding secret information in encrypted images while ensuring error-free extraction of the secret information and lossless recovery of the original plaintext image. This technology not only enhances image security but also enables efficient transmission of sensitive information over networks. Its application in cloud environments for user privacy protection has attracted significant attention from researchers. A reversible data hiding method in encrypted images based on prediction error and bitplane coding was proposed to improve the embedding rate of existing RDHEI algorithms. Different encoding methods were employed by the algorithm depending on the distribution of the bitplanes, resulting in the creation of additional space in the image. The image was rearranged to allocate the freed-up space to the lower-order planes. Following this, a random matrix was generated using a key to encrypt the image, ensuring image security. Finally, the information was embedded into the reserved space. The information can be extracted and the image recovered by the receiver using different keys. The proposed algorithm achieves a higher embedding rate compared to five state-of-the-art RDHEI algorithms. The average embedding rates on BOWS-2, BOSSBase, and UCID datasets are 3.769 bit/pixel, 3.874 bit/pixel, and 3.148 bit/pixel respectively, which represent an improvement of 12.5%, 6.9% and 8.6% compared to the best-performing algorithms in the same category. Experimental results demonstrate that the proposed algorithm effectively utilizes the redundancy of images and significantly improves the embedding rate.

Keywords: reversible data hiding, encrypted domain, run-length coding, separate, information security

0 引言

可逆信息隐藏 (RDH, reversible data hiding) 是信息安全领域的重要技术之一, 能够利用载体的冗余性, 将秘密信息嵌入载体中, 并且可以无损地恢复载体^[1]。随着信息技术的飞速发展, 网络传输速率大大提高, 人们可更加方便地使用网络进行交流, 在享受网络带来的便利的同时, 遭受隐私信息在传输过程中被窃取、篡改等信息安全威胁, 数字图像在人们的网络生活中占据了重要的比例, 图像同样包含一些隐私信息, 需要被保护。密文域可逆信息隐藏 (RDHEI, reversible data hiding in encrypted images) 技术将 RDH 技术与加密技术结合, 为秘密信息的安全性提供了双重保障, 在医学、司法等领域发挥着重要作用。现有的密文域可逆信息隐藏算法可以分为 3 类: 加密后预留空间 (VRAE, vacating room after encryption)^[1-4]、加密的同时预留空间 (VRBE, vacating room by encryption)^[5-8]和加密前预留空间 (RRBE, reserving room before encryption)^[9-19]。

VRAE 方案需要先对图像加密再预留空间, 加密会破坏原始图像的空间相关性, 使得可嵌入的空间减少, 因此使用该方案难以获得理想的嵌入率。这一类型的方案被 Zhang^[1]提出, 方案首先

利用流密码加密原始图像, 然后将加密图像分成大小相同的块, 通过翻转块中部分像素的最低有效位来嵌入秘密信息, 利用波动函数提取信息和恢复图像, 但是可能会出现不可逆的图像失真的情况。Hong 等^[2]利用像素之间的强相关性对波动函数改进, 降低了该方案出现失真的概率, 提升了该方案的嵌入容量。Yi 等^[3]通过块置换和流密码加密图像, 然后利用预测误差扩展嵌入秘密信息。Wang 等^[4]提出了一种自适应编码策略, 需要将加密图像中的块分为不同的类型, 在加密之前, 分析最佳的标记方式, 尽可能地提高压缩比, 预留嵌入空间。

VRBE 方案会使用一些特殊的加密方法, 保留了部分的空间相关性, 相对 VRAE 方案而言嵌入容量有所提高。Yin 等^[5]使用块置乱的方式对图像进行加密, 因此块内的空间相关性被保留下来, 在块内生成直方图, 通过直方图位移的方式嵌入信息。Huang 等^[6]通过对每个分块使用相同的密钥加密, 保留了块内的空间相关性, 然后结合传统的 RDH 技术嵌入信息。Yi 等^[7]通过块置乱加密图像, 在每个块中选定一个像素作为参考像素, 计算块内其他像素与参考像素的差值, 根据差值使用二叉树编码将像素标记为可嵌入像素和不可嵌入像素, 其中可嵌入像素用来嵌入秘密信息。上述方案只利用了图像局部的相关性, Wu 等^[8]针对该问题进行了改进, 使用中值预测器计算预测

误差,利用图像整体的相关性,使更多的块被划分为可嵌入块,嵌入容量得到提升。

RRBE 方案在加密前预留空间,能够充分利用图像的空间相关性,嵌入容量有了极大提升。RRBE 方案被 Ma 等^[9]提出,该方案使用最低有效位(LSB, least significant bit)替换的方法实现图像的自嵌入,从而能够预留空间用于嵌入秘密信息。Yi 等^[10]提出了一种稀疏矩阵编码,将图像分块,比较块中“0”和“1”的个数,记录较少元素的位置,实现了对块的压缩。袁源等^[11]对文献[10]的方案进行了改进,使用相邻位平面异或的方式减小位平面之间的冗余度,使得位平面变得更加平滑,减少了不能压缩的块的个数,得到了较大的嵌入空间。早期的算法考虑到嵌入秘密信息后会造成图像失真,往往在 LSB 平面嵌入信息,而 RDHEI 算法不需要考虑失真的问题。Puteaux 等^[12]提出了使用最高有效位(MSB, most significant bit)平面存储信息,该方案对最高位平面进行预测,对预测错误的位置进行标记,预测正确的位置用来存储秘密信息,由于只使用了一个位平面嵌入信息,得到的嵌入率低于 1 bit/pixel。Yang 等^[13]对上述方案进行了改进,增加了一个位平面嵌入信息,嵌入容量得到提升。Ren 等^[14]提出了一种针对二值图像的 RDHEI 算法,该算法将图像分块,根据块内像素取值将块划分为均匀块和非均匀块,均匀块使用位替换嵌入信息,非均匀块使用像素预测的方式嵌入信息。Chen 等^[15]提出了一种扩展游程编码,由于相邻像素的相关性,扫描 MSB 平面能够得到连续相同的长比特流,使用游程编码能够有效地压缩位平面,预留部分空间。Yin 等^[16]在文献[15]的基础上进行了改进,对预测误差图像进行压缩,扫描预测误差位平面能够得到更长的连续比特流,压缩效果更好,嵌入容量得到了提升。文献[17]也对文献[15]的方案进行了改进,原方案中扩展游程编码无法对短比特流压缩,改进方案使用哈夫曼编码代替定长编码,使得位平面能够被更加充分地压缩,极大地提升了嵌入容量,但是仍然有进一步提高的空间。文献[18]利用了哈夫曼编码,首先用位图记录原始像素与预测像素相同的比特数,然后利用哈曼编码对位图进行压缩,从而预

留空间,获得了较高的嵌入容量。

RRBE 方案能够充分利用图像的冗余性,得到较大的嵌入容量,具有更高的实用价值。本文基于文献[14]方案的思想,结合文献[15]提出的扩展游程编码提出了一种位平面编码,利用该编码方案设计了基于预测误差与位平面编码的密文域可逆信息隐藏算法。本文的主要贡献如下:① 使用中值预测器对图像进行预处理,保证图像完全可逆的同时,使更多的块被划分为均匀块,提高了图像的利用率,得到了较高的嵌入率;② 提出了一种位平面编码,该编码方案能够有效地压缩图像,提升嵌入容量。

1 相关知识

文献[15]提出了一种扩展游程编码,该编码方案将编码方式分为可变长度编码和固定长度编码两种类型, L 表示相同比特的长度,当 $L>4$ 时使用可变长度编码,否则使用固定长度编码。

可变长度编码:可变长度编码由前缀、长度符号和尾缀组成。前缀长度 $L_{pre} = \lfloor \lg L \rfloor$,其中 $\lfloor * \rfloor$ 为向下取整,前缀由 $(L_{pre}-1)$ 位“1”和1位“0”组成。长度符号的长度与前缀一致,取值为 $L-2^{L_{pre}}$,尾缀的值为对应的重复比特值。

固定长度编码:固定长度编码由前缀和长度为 L_{fix} 的尾缀组成。前缀固定为0,尾缀由当前位向后截取 L_{fix} 的比特流组成, L_{fix} 由用户在编码前预先设置。

2 本文算法

本文提出的可逆信息隐藏算法框架如图1所示,主要分为3个部分:预处理、信息隐藏、信息提取与图像恢复。原始图像所有者对图像进行预处理,使用流密码加密图像。信息嵌入者使用信息隐藏密钥加密秘密信息,将秘密信息嵌入加密图像。接收方使用图像加密密钥恢复原始图像,使用信息隐藏密钥提取秘密信息。

2.1 预处理

2.1.1 像素预测

假设原始图像大小为 $M \times N$,使用文献[20]提出的中值预测器(如图2所示)计算原始图像中每个像素 x 的预测像素 px ,计算方式如式(1)所示。

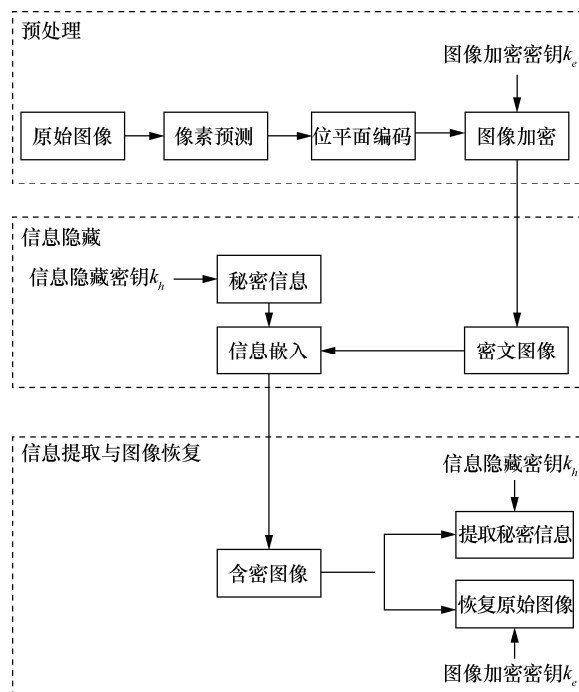


图 1 可逆信息隐藏算法框架

Figure 1 Framework of the reversible data hiding algorithm

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

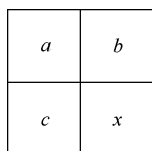


图 2 中值预测器

Figure 2 Median predictor

式(1)中 a 、 b 、 c 分别为当前像素 x 的左上方、上方和左侧相邻像素，通过比较 3 个相邻像素之间的关系，可以计算得到 x 的预测值 px ，使用中值预测器预测图像，只需要将第一行和第一列的像素作为参考像素保持不变，其他像素均可以用来嵌入信息，使图像中的空间能够被充分利用。根据式(2)计算预测误差 ex ，其中， i, j 分别代表行号与列号。对于第一行和第一列的像素，无法使用中值预测器进行预测，为了提高图像的利用率，第一行中的像素的预测误差计算为当前像素与左侧相邻像素的差值，第一列中的像素的预测误差计算为当前像素与上方像素的差值，(1,1)位置的像素的预测误差置为 0，并将该位置的原始像素

作为辅助信息记录下来。其中，部分预测误差小于 0，所以需要使用最高位作为符号位。当预测误差 $ex \geq 128$ 或者 $ex \leq -128$ 时，标记该像素为溢出像素，并保持其像素值不变，记录溢出像素的个数和位置，像素预测过程如图 3 所示。

$$ex_{i,j} = \begin{cases} 0, & i=1, j=1 \\ p_{i,j} - p_{i,j-1}, & i=1, j>1 \\ p_{i,j} - p_{i-1,j}, & i>1, j=1 \\ x_{i,j} - p_{i,j}, & i>1, j>1 \end{cases} \quad (2)$$

2.1.2 位平面编码

将预测误差图像分为 8 个位平面，将每个位平面划分成 n 个不重叠的块，每个块的大小为 $S \times S$ ，将全由“0”组成的块定义为均匀块 (HB, homogeneous block)，其他的块定义为非均匀块 (NB, non-homogeneous block)。使用“1”标记 HB，使用“0”标记 NB，因此，所有的标签可以构成一个大小为 $(M/S) \times (N/S)$ 的标签映射图 (LM, label map)，假设 HB 的数量为 n_{hb} 。

根据位平面的分布特性将其分为 3 类，如表 1 所示。

表 1 位平面分类
Table1 The classification of bitplane

条件	类型	标志	编码结构
$4n_{hb} \leq (M/S)(N/S)$	I	0	0+原始位平面比特流
$4n_{hb} > (M/S)(N/S)$ 且 $l + \lceil \lg(M/S)(N/S) \rceil \geq (M/S)(N/S)$	II	10	10+LM+NB
$4n_{hb} > (M/S)(N/S)$ 且 $l + \lceil \lg(M/S)(N/S) \rceil < (M/S)(N/S)$	III	11	11+l+LM+NB

若 $4n_{hb} \leq (M/S)(N/S)$ ，则说明位平面中的均匀块数量较少，均匀块中的空间无法容纳 LM，达不到压缩的效果，将该位平面划分为类型 I，使用 0 标记。若 $4n_{hb} > (M/S)(N/S)$ ，则说明该位平面能够预留空间，嵌入秘密信息，需要根据 LM 进一步分类。由于预测误差的分布集中在 0 附近，高位平面具有较强的相关性，因此在高位平面中的非均匀块仅占极少的一部分，生成的 LM 具有稀疏特征，能够利用扩展游程编码将 LM 有效地压缩。将压缩后的 LM 记为 LM'，假设 LM' 长度为 l ，

162	162	161	162	157	163	161	166	162	162	161	162	157	163	161	166	0	0	-1	1	-5	6	-2	5
164	158	155	161	159	159	160	161	164	164	158	156	157	163	159	165	2	6	3	5	2	-4	1	4
160	163	158	160	162	159	156	159	160	158	160	161	159	162	160	157	-4	5	-2	-1	3	-3	4	2
159	155	157	158	159	156	157	159	159	162	155	159	160	159	156	159	-1	-7	2	-1	-1	-3	1	0
155	158	158	159	160	157	157	163	155	155	158	158	159	157	157	159	-4	3	0	1	1	0	0	4
155	157	158	155	154	155	157	161	155	158	157	159	156	154	155	163	0	-1	1	-4	-2	1	2	-2
156	156	160	156	155	155	152	159	156	157	157	157	155	155	157	156	1	-1	3	-1	0	0	-5	3
156	156	159	159	155	150	148	160	156	156	160	156	158	155	150	155	0	0	-1	3	-3	-5	-2	5

(a) 原始图像

(b) 预测图像

(c) 预测误差

00000000	00000000	10000001	00000001	10000101	00000110	10000010	00000101
00000010	10000110	00000010	10000100	10000100	00000101	10000010	10000001
00000011	10000011	10000001	10000111	00000010	10000001	10000001	10000011
00000001	00000000	10000100	00000011	00000000	00000001	00000001	00000000
00000000	00000100	00000000	10000001	00000001	10000100	10000010	00000001
00000001	10000001	00000011	10000001	00000000	00000000	10000001	00000011
10000011	10000011	00000101	00000001	10000100	10000100	00000010	00000010
10000010	10000101	00000011	00000000	00000000	10000101	10000010	00000101

(d) 预测误差的二进制表示

图3 像素预测过程

Figure 3 The process of pixel prediction

为了方便后续解码,使用 $\lceil \lg(M/S)(N/S) \rceil$ 位记录长度信息 l 。若 $1 + \lceil \lg(M/S)(N/S) \rceil \geq (M/S)(N/S)$,则不对LM压缩,将位平面划分为类型II,标记为10,否则划分为类型III,标记为11。

图4给出了当块大小 $S=2$,定长编码长度 $L_{\text{fix}}=3$ 时,3种类型的位平面编码示例。图4(a)中位平面仅有3个HB,能够提供的空间为12 bit,小于LM的长度16 bit,根据表1中的分类规则,该位平面的类型为I,编码由标志位0和原始位平面比特流构成。图4(b)和图4(c)中的位平面中HB的数量均为14,预留的空间大小为56 bit,大于LM的长度,分别为类型II或类型III。图4(b)中的LM经过游程编码压缩后的长度为18 bit, $18 + \lg 16 > 16$,因此,图4(b)被划分为类型II,编码由标志位10、LM以及NB比特流构成。图4(c)中LM经过游程编码压缩后的长度 l 为11 bit, $11 + \lg 16 < 16$,所以该位平面被划分为类型III,编码由标志位11、长度信息 l 、LM'以及NB比特流构成。

2.1.3 位平面重排列

压缩后的位平面需要进行重排列,将预留的空间放在低位平面。图5给出了位平面重排列过程,首先在最高位平面存储辅助信息 A ,包括块大小 S (4 bit)、定长编码的长度 L_{fix} (4 bit)、左上角第一个像素的原始像素(8 bit)、溢出点的个数 n_{over} ($\lceil \lg MN \rceil$ bit)以及每个溢出点位置($n_{\text{over}} \lceil \lg MN \rceil$ bit),接着依次存储各个位平面的编码,剩余空间用于存储秘密信息。因此,图像的净嵌入容量 C 为

$$C = 8MN - \text{len}(A) - \sum_{i=1}^8 \text{len}(P_i) - \lceil \lg 8MN \rceil \quad (3)$$

其中, $\text{len}(\cdot)$ 为信息的长度, P_i ($i=1,2,\dots,8$)为第 i 个位平面的编码,8为最高位平面。为了方便信息嵌入者嵌入信息,需要在最低位平面下方的 $\lceil \lg 8MN \rceil$ bit存储图像的净嵌入容量 C 。

2.2 图像加密

经过上述预处理的图像表示为 I ,利用图像加密密钥 k_e 生成大小为 $M \times N$ 的随机矩阵 R ,通

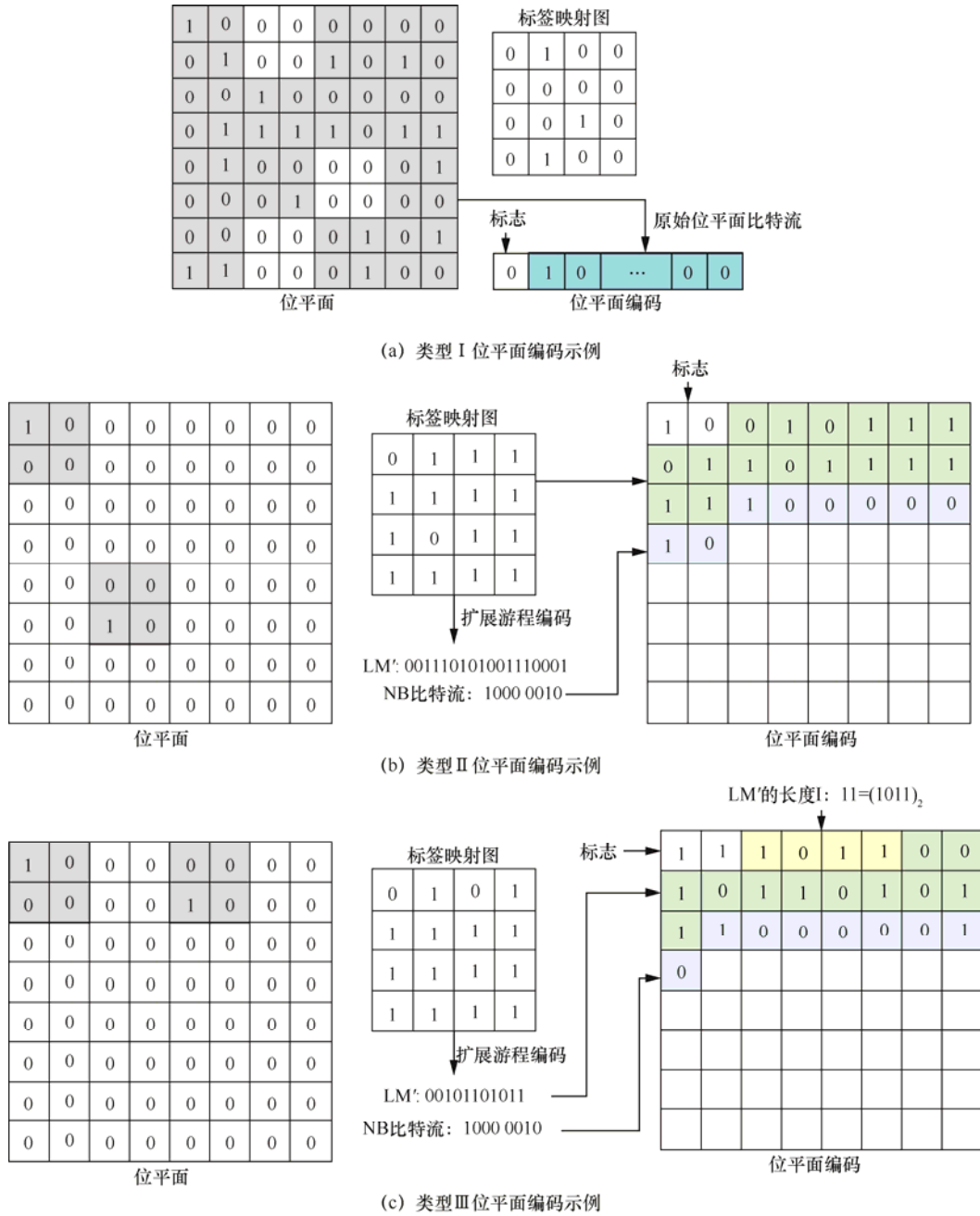


图4 位平面编码示例
Figure 4 The example of bitplane coding

过式(4)以及式(5)将 I 中像素值以及 R 中的元素转化为二进制。

$$I_{i,j}^k = \left\lfloor \frac{R_{i,j}}{2^{k-1}} \right\rfloor \bmod 2, k=1,2,\dots,8 \quad (4)$$

$$R_{i,j}^k = \left\lfloor \frac{R_{i,j}}{2^{k-1}} \right\rfloor \bmod 2, k=1,2,\dots,8 \quad (5)$$

其中, i, j 分别表示行号和列号, k 为二进制表示的第 k 位, $1 \leq i \leq M, 1 \leq j \leq N, 1 \leq k \leq 8$ 。然后, 根据式(6)对图像进行异或加密操作, 为了方便后续嵌入秘密信息, 嵌入容量信息位不进行加密处理。最后, 根据式(7)重构得到加密图像 E 。

$$E_{i,j}^k = \begin{cases} I_{i,j}^k, & \text{嵌入容量信息位} \\ I_{i,j}^k \oplus R_{i,j}^k, & \text{其他} \end{cases}, k=1,2,\dots,8 \quad (6)$$

$$E_{i,j} = \sum_{k=1}^8 E_{i,j}^k \cdot 2^{k-1} \quad (7)$$

2.3 信息嵌入

信息嵌入者收到加密图像 E 后, 根据具体的需求, 将特定的秘密信息嵌入加密图像中, 生成含密图像。例如, 在远程医疗中, 患者不希望将医学图像以及与个人相关的隐私信息泄露给他人, 就可以将医学图像加密, 然后将个人隐私信息嵌入密文图像。从图像的最低位平面最下方的 $\lceil \lg 8MN \rceil$ 位中提取图像的净嵌入容量 C , 由图 5 可知, 预留的空间连续分布在图像的低位平面中, 每个位平面的容量为 MN , 可以根据式(8)计算出预留空间开始位置所在的位平面次序 k , 从图 5 可以看出, 该位平面并非所有空间都可以嵌入秘密信息, 需要进一步计算行和列, 该位平面所包含的嵌入容量为 $(c + \lceil \lg 8MN \rceil) \bmod MN$, 根据式(9)以及式(10)可以计算出嵌入信息开始位置所在的行 r 和列 c 。

$$k = \left\lceil \frac{(C + \lceil \lg 8MN \rceil)}{MN} \right\rceil \quad (8)$$

$$r = M - \left\lfloor \frac{(C + \lceil \lg 8MN \rceil) \bmod MN}{N} \right\rfloor \quad (9)$$

$$c = N + 1 - ((C + \lceil \lg 8MN \rceil) \bmod MN) \bmod N \quad (10)$$

以图 5 为例, 从最低位平面下方的 9 bit 中可以得到图像的净嵌入容量为 117 bit, 图像的大小为 8×8 , 可以计算得到秘密信息嵌入的开始位置为第 2 个位平面 (最低位平面为第 1 个位平面) 的第 1 行第 3 列。得到起始位置后, 信息嵌入者利用信息隐藏密钥 k_h 加密秘密信息, 通过位替换的方式将加密

的秘密信息嵌入预留的空间, 得到含密图像。

2.4 信息提取与图像恢复

接收者在接收到含密图像后, 根据自己所拥有的密钥进行不同的操作。

1) 当接收方只拥有图像加密密钥 k_e 时, 可以恢复原始明文图像。首先利用图像加密密钥 k_e 生成随机矩阵 R , 通过位异或操作解密图像, 然后从最高位平面开始依次提取块大小 S 、定长编码的长度 L_{fix} 、(1,1)位置的原始像素等辅助信息, 接着提取各个位平面的编码, 根据辅助信息对位平面解码, 从而恢复原始图像。

2) 当接收者只拥有信息隐藏密钥 k_h 时, 可以从最低位平面提取出图像容量信息, 通过容量计算得到秘密信息嵌入的开始位置, 然后将秘密信息提取出来, 最后使用信息隐藏密钥 k_h 解密得到原始秘密信息。

3) 当接收者同时拥有图像加密密钥 k_e 和信息隐藏密钥 k_h 时, 既可以提取秘密信息, 也可以无损恢复原始图像。

3 实验结果分析

为了验证本文算法的性能, 本节选取了 6 幅标准测试图像 (如图 6 所示) 以及 3 个数据集 BOSSBase^[21]、BOWS-2^[22]和 UCID^[23], 使用随机生成的比特流作为秘密信息进行实验。现有的算法通常满足秘密信息的无错提取和原始明文图像的无损恢复, 因此, 嵌入率是评价 RDHEI 算法的关键指标。

3.1 算法的安全性分析

安全性是指保证原始载体的内容不被非法攻击者获取的能力, 以下将从视觉效果、暴力攻击、

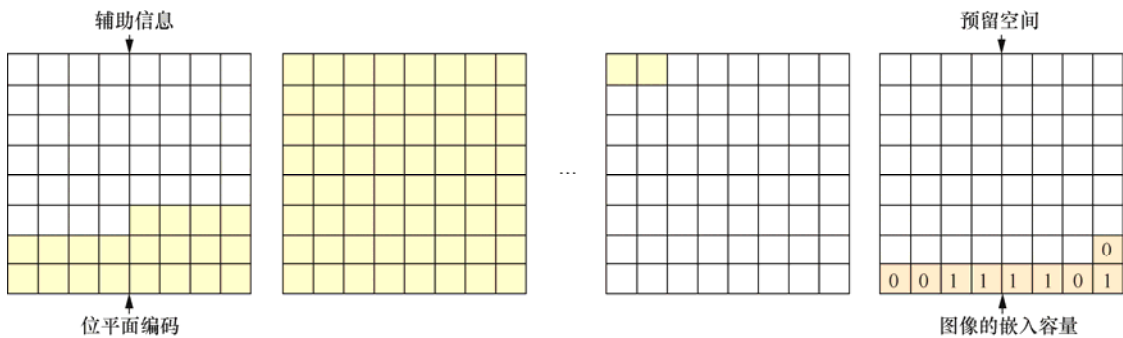


图5 位平面重排列过程
Figure 5 The process of bitplane rearrangement

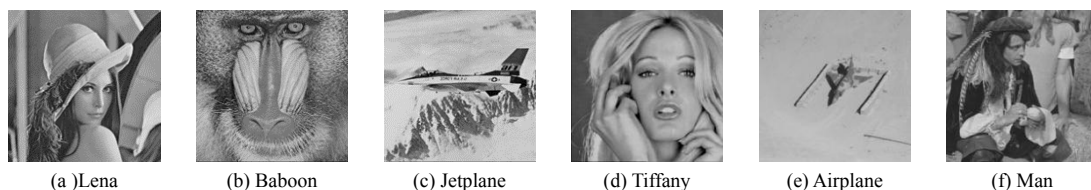


图6 测试图像
Figure 6 Test images

统计分析攻击、差分攻击以及密文图像与原始图像的相似度 5 个方面来分析。

以 Lena 图像为例, 本文算法对 Lena 图像的实验结果如图 7 所示, 图 7(b)为图 7(a)对应的加密图像, 图 7(c)为图 7(b)嵌入秘密信息后生成的含密图像, 用人眼观察, 加密图像与原始图像具有较大的视觉差异, 不具有相似性。

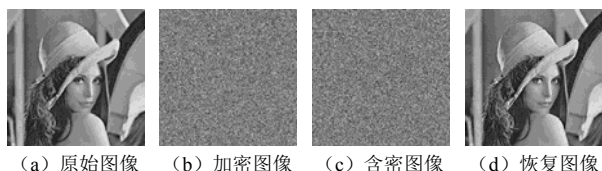


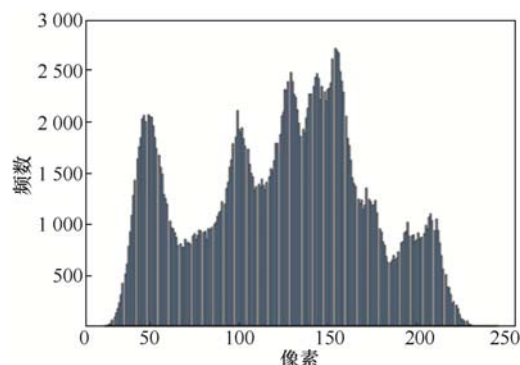
图7 本文算法对 Lena 图像的实验结果
Figure 7 Experiment results of Lena image generated by the proposed algorithm

本文使用流密码对图像加密, 对于大小为 $M \times N$ 的图像, 密钥空间大小为 $2^{8 \times M \times N}$ 。一般认为当密钥空间大于 2^{100} 时, 可以抵抗暴力攻击^[24]。本文实验中使用的图像大小为 512×512 , 密钥空间大小为 $2^{8 \times 512 \times 512}$, 在如此大的密钥空间之下, 非法攻击者想要通过暴力穷举的方式来破解密码是不可行的, 因此本文算法能够抵抗暴力攻击。

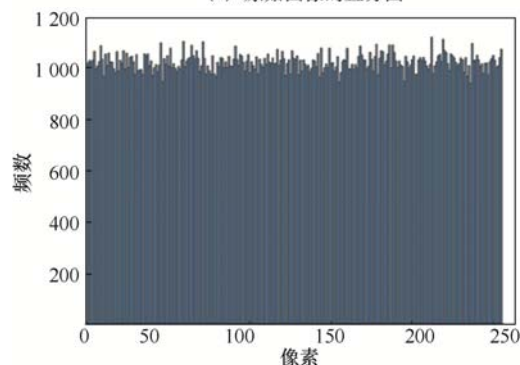
图 8(a)为 Lena 原始图像对应的直方图, 呈现出不规则的分布, 而图 8(b)为这幅图像加密后的直方图, 分布均匀, 难以从中获取原始图像的特征, 说明本文算法能够有效地隐藏图像的特征信息, 可以抵抗统计分析攻击。

差分攻击是一种常见的密码学攻击方法, 其基本思想是通过对明文图像进行细微的改动, 观察密文图像改动前后的差别。如果使用相同的密钥对多幅不同的图像进行加密, 那么这些密文图像之间会存在差异, 攻击者可能尝试通过比较不同图像的密文来发现这些差异, 获取有关密钥或加密算法的信息, 从而解密出原始图像。虽然使用流密码加密图像能够保护原始图像的信息特

征, 但是当使用同一个密钥加密多个图像时, 可以分析使用相同密钥加密的图像, 破解出相应的流密码。因此, 为了保证算法的安全性, 要尽可能避免使用相同的密钥加密大量的图像。



(a) 原始图像的直方图



(b) 加密图像的直方图

图8 Lena 图像的直方图
Figure 8 Histogram of Lena image

峰值信噪比 (PSNR, peak signal-to-noise ratio) 和结构相似度 (SSIM, structural similarity) 是广泛使用的图像评估指标。两幅图像越相似, PSNR 的值越大, 当 PSNR 为 $+\infty$ 时, 说明两幅图像完全一致。SSIM 的取值在 -1 和 1 之间, 当两幅图像相同时, 值为 1 。为了进一步验证本文算法的安全性, 表 2 给出了 6 幅加密图像的 PSNR 值和 SSIM 值, 可以看出, 所有图像的 PSNR 值都非常低, SSIM 值都非常接近于 0 , 说明加密图

像与原始图像的相似度极低,无法从中获取原始图像的任何信息,从而表明本文算法能够安全地保护原始图像的信息。

表2 加密图像的 PSNR 和 SSIM($S=2, L_{\text{fix}}=4$)

Table 2 The PSNR and SSIM($S=2, L_{\text{fix}}=4$) on encrypted images

加密图像	PSNR	SSIM
Lena	9.2337	0.0273
Baboon	9.5295	0.0681
Jetplane	8.3216	0.0301
Tiffany	9.4796	0.0332
Airplane	8.9663	0.0142
Man	9.103	0.0346

3.2 可逆性分析

可逆性是指算法将密文图像无损恢复为原始明文图像的能力。本文算法是基于中值预测器和位平面编码实现的,从高位平面中可以读取(1,1)位置的原始像素,利用中值预测器以及预测误差图像就可以无损恢复原始图像,而预测误差图像使用了位平面编码压缩,所以本文算法的可逆性取决于位平面编码的可逆性,位平面编码的可逆性分析如下。

如表1所示,类型I的位平面编码由标志位和原始位平面比特流构成,在图像预处理以及信息隐藏的过程中,图像的大小没有发生变化,因此,只需要根据图像大小 $M \times N$ 在符号位之后读取相应长度的比特流就可以得到原始位平面。类型II的位平面编码由标志位、LM以及NB比特流构成,LM的长度可以由 $(M/S)(N/S)$ 计算得到,其中块大小 S 可以从最高位平面中读取;根据LM中“0”的个数可以获取非均匀块的数量 n_{nb} ,从而计算得到NB比特流的长度 $S \times S \times n_{\text{nb}}$;根据长度依次提取出LM和NB之后,可以通过LM与原始位平面的映射关系将位平面无损恢复,“1”对应的块恢复为全由“0”构成的块,“0”对应的块信息则需要依次从NB比特流中提取。在类型III的位平面编码中,LM'为压缩之后的LM,长度不固定,因此需要先读取 $\lceil \lg(M/S)(N/S) \rceil$ bit 获得LM'的长度 l ,从而可以通过 l 读取LM',LM'需要根据扩展游程编码的规则解码,从而无损恢复LM,扩展游程编码的可逆性在文献[15]中已经被验证,接下来的步骤与

类型II相同。综上所述,3种类型的位平面编码都是完全可逆的,因此预测误差图像能够被无损恢复,进而说明本文算法是具有可逆性的。

如表3和表4所示,3个数据集以及6幅测试图像对应的恢复图像的PSNR均为 $+\infty$,SSIM均为1,表明重构图像与原始图像完全一致,不存在失真的情况,由此可以验证本文算法是完全可逆的。

表3 本文算法在不同数据集上的峰值信噪比和结构相似度

Table3 The PSNR and SSIM of the proposed method on different datasets

数据集	PSNR	SSIM
BOWS-2	$+\infty$	1
BOSSBase	$+\infty$	1
UCID	$+\infty$	1

表4 本文算法在不同测试图像上的峰值信噪比和结构相似度

Table 4 The PSNR and SSIM of the proposed method on different test images

测试图像	PSNR	SSIM
Lena	$+\infty$	1
Baboon	$+\infty$	1
Jetplane	$+\infty$	1
Tiffany	$+\infty$	1
Airplane	$+\infty$	1
Man	$+\infty$	1

3.3 嵌入容量分析

嵌入容量是指图像能够携带秘密信息的最大值,为了避免图像大小的影响,使用单位像素隐藏比特数进行衡量。

文献[14]提出了一种基于二值图像的RDHEI算法,灰度图像的每个位平面可以看作一个二值图像,因此该算法也可以应用于灰度图像。本文结合文献[14]算法的思想,提出了一种位平面编码方案,基于该编码方案设计了一种针对灰度图像的RDHEI算法。从表5可以看出,本文算法产生的均匀块数量远大于文献[14]算法,这是因为本文在预测误差图像中嵌入信息,预测误差的分布相较于原始像素更加集中。并且,文献[14]算法将全为“0”和全为“1”组成的块划分为均匀块,为了保证算法的可逆性,每个块右下角的元素需要保持不变;而本文算法考虑到预测误差位平面中“1”的占比较低,只将全由“0”构成的

表 5 6 幅标准测试图像的均匀块数量、标签映射图长度和净嵌入容量 ($S=2, L_{\text{fix}}=4$)
Table 5 The number of HB、length of LM and embedding capacity on 6 standard test images

测试图像	能够压缩的位平面数量		HB 数量		LM 的总长度/bit		净嵌入容量/bit	
	文献[14]算法	本文算法	文献[14]算法	本文算法	文献[14]算法	本文算法	文献[14]算法	本文算法
Lena	4	5	191 894	250 987	262 144	165 465	313 446	838 427
Baboon	3	3	100 459	137 063	196 608	134 035	104 697	414 079
Jetplane	6	6	249 925	283 759	393 216	207 185	356 427	927 780
Tiffany	4	4	182 534	214 437	262 144	133 508	285 366	724 080
Airplane	6	5	280 806	294 212	393 216	130 269	449 070	1 046 404
Man	4	5	181 523	238 940	262 144	198 585	282 333	757 097

块划分为均匀块, 因此不需要在每个块中保留原始像素, 块内所有空间都能被充分利用, 进一步提升了嵌入容量。由表 5 可知, 文献[14]算法中, 能够压缩的位平面越多, LM 的总长度就越大。而本文利用 LM 的分布特征, 结合扩展游程编码, 在压缩位平面数量相同或者更多的情况下, 得到的 LM 的总长度远小于文献[14]。表 5 中的数据表明, 相较于文献[14]算法, 在 6 幅不同的测试图像上, 本文算法的嵌入容量均有显著提升。

图 9 展示了测试图像在不同定长编码长度和不同短比特串长度上的嵌入率。在块大小 (S) 和定长编码长度 (L_{fix}) 取值相同时, Baboon 的嵌入率最低, 其他图像嵌入率均能达到 2 bit/pixel 以上, 相较于平滑图像, 预测器预测纹理图像的准确度下降, 预测误差较大, 导致均匀块的数量减少, 并且溢出点的个数会较多, 需要更多的空间用来存储辅助信息。可以看出, 当 $S=2$ 时, 嵌入率最高, 这是因为当块较小时, 均匀块的数量

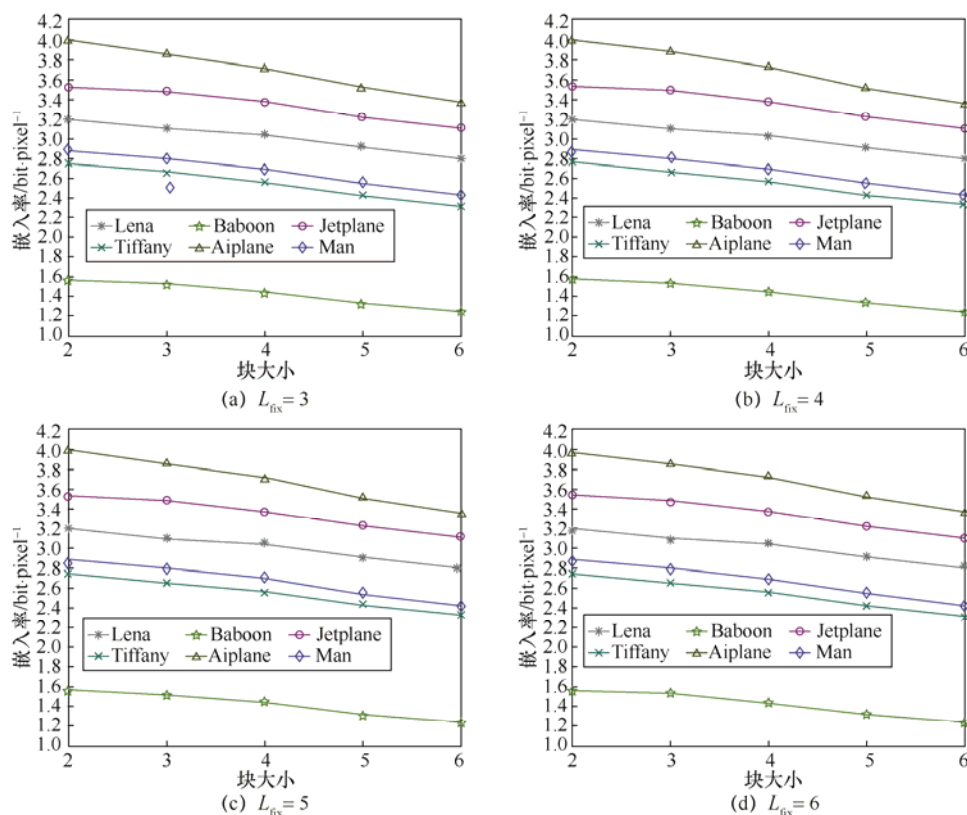


图 9 测试图像在不同定长编码长度和不同短比特串长度上的嵌入率
Figure 9 Embedding rates under different L_{fix} and S on test images

较多,虽然此时 LM 的长度较大,但是使用游程编码对 LM 压缩,极大地缩短了 LM 的长度。而当块增大时,均匀块的数量会减少,使得嵌入容量降低。而对于 L_{fix} ,该参数对嵌入率的影响相对较小,不同图像取得最佳效果的 L_{fix} 取值不同,纹理区域较多的图像,会产生较长的不连续比特流,定长编码的长度较大时压缩效果更好,而对于平滑图像则相反,定长编码过长反而会增加过多的额外比特,压缩效果较差。

为了验证算法的普适性,本文选取了 BOWS-2、BOSSBase、UCID 这 3 个数据集进行实验,选取块大小 $S=2$, $L_{\text{fix}}=4$ 。本文算法在不同数据集上的嵌入率如表 6 所示,3 个数据集的平均嵌入率都能达到 3 bit/pixel 以上,BOWS-2 的最高嵌入率为 7.262 bit/pixel,最低嵌入率 0.812 bit/pixel,BOSSBase 最高嵌入率 7.841 bit/pixel,最低嵌入率 0.917 bit/pixel,只有 UCID 的最低嵌入率为 0 bit/pixel,无法嵌入秘密信息,但将 S 修改为 4, L_{fix} 修改为 3 时,该图像的嵌入容量能够达到 2 438 bit,也能够嵌入秘密信息,说明本文算法具有良好的性能,在大部分图像上适用并且能够得到较高的嵌入率。

表 6 本文算法在不同数据集上的嵌入率
Table 6 The embedding rate of the proposed method on different datasets

数据集	嵌入率/bit·pixel ⁻¹		
	最高嵌入率	最低嵌入率	平均嵌入率
BOWS-2	7.262	0.812	3.769
BOSSBase	7.841	0.917	3.874
UCID	5.63	0	3.148

3.4 与其他算法比较

为了证明本文算法在嵌入率方面的优越性,图 10 展示了本文算法与同类相关算法在 BOWS-2、BOSSBase 和 UCID 这 3 个数据集上的平均嵌入率的比较。文献[7]算法和文献[15]算法分别使用二叉树编码和扩展游程编码预留空间,由于上述两个算法都是在原始位平面嵌入信息,相较于预测误差,原始像素的分布更加分散,所以得到的嵌入率较低。文献[17]算法结合了哈曼夫编码,改进了游程编码无法对短比特流有效压缩的缺陷,嵌入率高于文献[15]算法。而文献[16]

算法和文献[18]算法对预测误差位图像进行编码压缩,所以嵌入率高于上述 3 个算法。从图 10 可以直观地看出,相较于其他 5 个同类算法,本文算法具有更高的嵌入率。与性能最好的算法相比,嵌入率在数据集 BOWS-2 上提升了 12.5%,在数据集 BOSSBase 上提升了 6.9%,在数据集 UCID 上提升了 8.6%。本文算法的高嵌入率在于使用了基于预测误差的位平面编码机制,尽可能地压缩位平面,预留出更多嵌入空间。

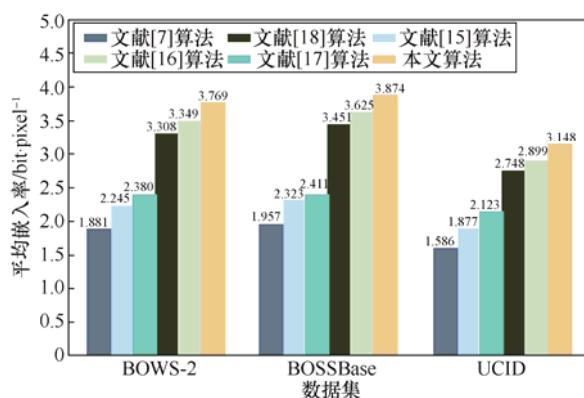


图 10 本文算法与同类算法在 3 个数据集上的平均嵌入率的比较
Figure 10 Comparison of average embedding rate of the proposed method and similar algorithm on three datasets

4 结束语

本文提出了基于预测误差与位平面编码的密文域可逆信息隐藏算法。该算法充分地利用了预测误差位平面的分布特性,将位平面分为均匀块和非均匀块,使用标签映射图记录位平面中块的分布情况,根据分布情况,将位平面分为 3 种类型进行编码压缩,预留出较多的嵌入空间。实验结果表明,本文算法具有较高的嵌入容量,能够分离地提取秘密信息 and 无损恢复图像。本文算法在平滑图像上能够获得高嵌入率,在纹理图像上获得的嵌入率相对较低,这是因为本文算法的嵌入率主要依赖于位平面编码的压缩效果,而位平面编码的压缩效果会受到预测器的精确度影响;在纹理图像上中值预测器的效果较差,会有较多的溢出点,且预测误差偏离 0 值,进而导致位平面中 0 元素的数量减少,从而影响位平面编码的压缩效果。未来可以通过研究准确率更高的预测器,提升算法在纹理图像上的嵌入率。

参考文献：

- [1] ZHANG X P. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.
- [2] 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.
- [3] YI S, ZHOU Y, HUA Z. Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion[J]. Signal Processing: Image Communication, 2018, 64: 78-88.
- [4] WANG Y, HE W. High capacity reversible data hiding in encrypted image based on adaptive MSB prediction[J]. IEEE Transactions on Multimedia, 2022, 24: 1288-1298.
- [5] 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.
- [6] HUANG F J, HUANG J W, SHI Y Q. New framework for reversible data hiding in encrypted domain[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2777-2789.
- [7] 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.
- [8] WU Y Q, XIANG Y Z, GUO Y T, et al. An improved reversible data hiding in encrypted images using parametric binary tree labeling[J]. IEEE Transactions on Multimedia, 2020, 22(8): 1929-1938.
- [9] MA K, MING Z W, FENG Z X, 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.
- [10] YI S, ZHOU Y C. Binary-block embedding for reversible data hiding in encrypted images[J]. Signal Processing, 2017, 133: 40-51.
- [11] 袁源, 和红杰, 陈帆. 减少相邻位平面间冗余度的加密图像可逆信息隐藏[J]. 中国图象图形学报, 2019, 24(1): 13-22.
YUAN Y, HE H J, CHEN F. Reduction of the redundancy of adjacent bit planes for reversible data hiding in encrypted images[J]. Journal of Image and Graphics, 2019, 24(1): 13-22.
- [12] 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.
- [13] YANG Y P, YIN Z, QIAN Z. Reversible data hiding in encrypted images with two-msb prediction[C]//Proceedings of 2018 IEEE International Workshop on Information Forensics and Security(WIFS). 2018: 1-7.
- [14] REN H L, LU W, CHEN B. Reversible data hiding in encrypted binary images by pixel prediction[J]. Signal Processing, 2019, 165: 268-277.
- [15] 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.
- [16] 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, 19(2): 992-1002.
- [17] 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.
- [18] 吴友情, 郭玉堂, 汤进, 等. 基于自适应哈夫曼编码的密文可逆信息隐藏算法[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 image using adaptive Huffman encoding strategy[J]. Chinese Journal of Computers, 2021, 44(4): 846-858.
- [19] 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.
LI J W, ZHANG X Y, YAO Y Z, 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.
- [20] WEINBERGER M J, SEROUSSI G, SAPIRO G. The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS[J]. IEEE Transactions on Image Processing, 2000, 9(8): 1309-1324.
- [21] BAS P, FILLER T, PEVN T. Break our steganographic system: the ins and outs of organizing BOSS[C]//Proceedings of the 13th International Workshop on Information Hiding. 2011: 59-70.
- [22] BAS P, FURON T. Image database of BOWS-2[EB].
- [23] GERALD S, MICHAL S. UCID-an uncompressed colour image database[C]//Proceedings of the International Conference on Storage Retrieval Methods Applications for Multimedia. 2004: 472-480.
- [24] YE R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism[J]. Optics Communications, 2011, 284(22): 5290-5298.

[作者简介]



王海勇(1979-), 男, 江苏连云港人, 博士, 南京邮电大学副研究员, 主要研究方向为计算机网络安全、计算机视觉。



吉梦凝(1999-), 女, 湖北随州人, 南京邮电大学硕士生, 主要研究方向为可逆信息隐藏。