

基于多向梯度预测的密文域可逆信息隐藏

王文丽¹
WANG Wenli

摘要

针对现有基于预测误差扩展的密文图像可逆信息隐藏算法存在的像素预测器准确度不高、灵活性不够、编码冗余的问题,文章提出了一种多向梯度像素预测器结合动态二叉树标记的密文图像可逆信息隐藏算法。在该算法中,首先根据目标位置不同方向的相邻像素对预测过程作出的贡献,赋予不同的权重计算预测值,以适应图像的不同纹理;其次,利用动态二叉树进行编码压缩,提高嵌入容量。实验结果表明,所提出的算法预测性能优于常用的 MED 像素预测器,并在 BOSSbase 和 BOWS-2 两个数据集的平均嵌入率分别达到了 3.97 bpp 和 3.82 bpp。

关键词

多向梯度预测;二叉树标记;密文域可逆信息隐藏

doi: 10.3969/j.issn.1672-9528.2025.10.003

0 引言

密文域可逆信息隐藏(reversible data hiding in encrypted images, RDHEI)是一种在加密载体信号中嵌入附加信息的技术,在保护原始数据隐私的同时实现数据的隐蔽传输,从而拓展了传统信息隐藏的应用范围。

基于预测误差扩展(prediction error expansion, PEE)的可逆数据隐藏方案(PEE-RDH)因其高嵌入容量和良好的兼容性而备受关注。近年来,研究者将 PEE 策略与 RDHEI 相结合,提出了 PEE-RDHEI 方法。Yin 等人^[1]利用自然图像高位平面的强可预测性,通过逐像素标签生成策略实现数据嵌入,但该方法产生了较多辅助信息。为提高预测误差高位平面的利用率,Chen 等人^[2]提出了一种多 MSB 压缩方法,有效提升了嵌入容量。文献[3]则采用游程编码压缩预测误差位平面,但在预测精度较低时,编码效率受限。Yu 等人^[4]提出了一种分层嵌入策略,通过位平面级标签映射增加可嵌入位数,但未能充分利用局部图像相关性。Wu 等人^[5]受分叉树启发,提出一种基于参数二叉树标记的方法,利用全局空间相关性减少标签数量。Liu 等人^[6]则采用二叉树编码优化位平面块压缩,通过四分量编码策略提高嵌入空间利用率。

目前,中值边缘检测器(median-edge detector, MED)因其计算简单且预测精度较高,被广泛地用于 RDHEI 方法中。然而,现有像素预测器还存在预测精度不够理想,预测方式不够灵活从而难以适应图像纹理变化的问题。因此,本文针对以上问题提出基于多向梯度像素预测的密文域可逆信息隐

藏算法,具体如下:

(1) 提出多向梯度像素预测器(hybrid gradient pixel predictor, HGP),考虑目标像素 4 个方向对其预测值的影响程度赋予不同权重,以更好地适应图像的纹理变化;

(2) 改进动态二叉树编码,解决相邻位平面的编码冗余问题,进一步提升嵌入容量。

1 相关工作

1.1 MED

MED 是基于目标像素 $I(i, j)$ 的上邻像素 I_h 、左邻像素 I_v 以及主对角像素 I_{dig} 进行预测的,由于其计算简单,被广泛用于 PEE-RDDHEI,具体用公式表示为:

$$\hat{I}(i, j) = \begin{cases} \max(I_h, I_v) & I(i, j) \leq \min(I_h, I_v) \\ \min(I_h, I_v) & I(i, j) \geq \max(I_h, I_v) \\ I_h + I_v - I_{\text{dig}} & \text{其它} \end{cases} \quad (1)$$

1.2 流加密

流密码加密通过改变像素值大小实现图像内容保护,又称为异或加密。以灰度图像为例,核心思想是利用密钥生成与载体图像尺寸一致的伪随机序列 M ,然后将载体图像像素值与伪随机序列对应的数值采取异或计算得到加密图像 E ,用公式表示为:

$$E_{i,j}(k) = I_{i,j}(k) \oplus M_{i,j}(k), k = 0, 1, \dots, 7 \quad (2)$$

2 本文算法

算法框架如图 1 所示,参与角色分为内容所有者、数据隐藏者和合法接收者三部分,分别实现图像的预处理、数据嵌入和信息提取以及图像恢复。

1. 西藏民族大学信息工程学院 陕西咸阳 712000

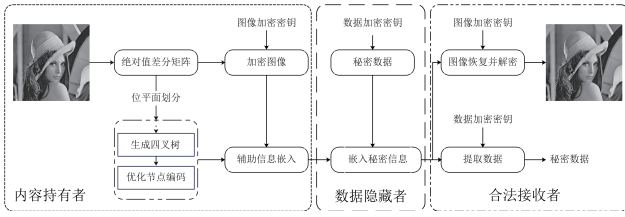


图1 算法流程图

2.1 图像预处理

首先，内容持有者利用 HGP 对自身持有图像进行预处理操作，然后利用优化节点编码的四叉树标记方法对处理过的图像进行预处理操作，具体细节如下：

(1) HGP 预处理

HGP 会将待预测的图像分为参考区域、边缘区域、梯度判别区域三部分进行像素预测，具体分区规则如图2所示。

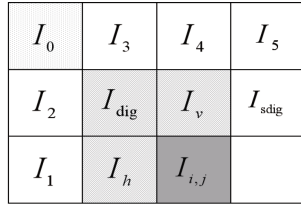


图2 像素分区规则

图2中，左、右和上侧作为参考区域，处理时需要保留 I_0 的像素值。其中，横向像素预测为其左侧相邻像素值，竖向像素预测为其上侧相邻像素值；浅色下划线是边缘区域，采用 MED 像素进行预测；深色是梯度判别区域，利用其相邻像素 I_h 、 I_v 、 I_{dig} 和 I_{sdig} 计算不同方向的局部梯度 Lg ，用公式表示为：

$$\begin{cases} Lg_h = \frac{2|I_1 - I_h| + |I_2 - I_{dig}| + 2|I_{dig} - I_v| + |I_v - I_{sdig}|}{6} \\ Lg_v = \frac{2|I_h - I_{dig}| + |I_{dig} - I_3| + 2|I_v - I_4| + |I_{sdig} - I_5|}{6} \\ Lg_{dig} = \frac{|I_2 - I_h| + |I_0 - I_{dig}| + |I_3 - I_v| + |I_4 - I_{sdig}|}{4} \\ Lg_{sdig} = \frac{|I_3 - I_2| + |I_4 - I_{dig}| + |I_5 - I_v| + |I_v - I_h|}{4} \end{cases} \quad (3)$$

为了排除预测像素所在区域高频变化对预测值的影响，在预测时考虑加入全局梯度 Wg 平衡计算，用公式表示为：

$$\begin{cases} Wg_h = \frac{\sum_{i=2}^m \sum_{j=2}^n |I_{i,j} - I_{i,j-1}|}{m \times (n-1)} \\ Wg_v = \frac{\sum_{i=2}^m \sum_{j=1}^n |I_{i,j} - I_{i-1,j}|}{(m-1) \times n} \\ Wg_{dig} = \frac{\sum_{i=2}^m \sum_{j=2}^n |I_{i,j} - I_{i-1,j-1}|}{(m-1) \times (n-1)} \\ Wg_{sdig} = \frac{\sum_{i=2}^m \sum_{j=1}^{n-1} |I_{i,j} - I_{i-1,j+1}|}{(m-1) \times (n-1)} \end{cases} \quad (4)$$

为保证算法的可逆性，全局梯度大小作为辅助信息得

以保留，因此利用公式(5)计算得到一个 $[0,100]$ 范围内的整数作为全局梯度值参与权重计算。

$$\hat{W}g_d = \left\lfloor \frac{1}{\sum_d Wg_d} 100 Wg_d \right\rfloor, d \in \{h, v, dig, sdig\} \quad (5)$$

得到全局梯度和局部梯度后，根据进一步计算目标像素在不同方向上的梯度权重，具体计算公式为：

$$k = \frac{1}{c_d (Lg_d + 0.1) \hat{W}g_d}, d \in \{h, v, dig, sdig\} \quad (6)$$

式中： c_d 表示相邻像素与目标像素的距离，即 $c_h = c_v = 1$ ， $c_{dig} = c_{sdig} = \sqrt{2}$ 。常数项 0.1 的设置是为了防止出现局部梯度值为 0 的情况影响权重计算。相反，平方项的设置是为了将高频区域急速变化的像素权重变得更小而减少像素预测的误差。最后对权重进行归一化得到 $\bar{k}$ ，即可完成梯度判别区域的像素预测，具体计算公式为：

$$\hat{I}(i, j) = \left\lfloor \sum_d \bar{k}_d \cdot I(i, j) \right\rfloor, d \in \{h, v, dig, sdig\} \quad (7)$$

为了后续的大容量数据嵌入以及图像的无损恢复，内容持有者还需要获取绝对值误差矩阵和其符号标记，用公式分别表示为：

$$|e(i, j)| = I(i, j) - \hat{I}(i, j), 1 \leq i \leq m, 1 \leq j \leq n \quad (8)$$

$$\text{Sign}(i, j) = \begin{cases} 1 & e(i, j) < 0 \\ 0 & e(i, j) \geq 0 \end{cases} \quad (9)$$

为方便理解，图3给出一个示例。

180	179	180	180	180
175	176	180	178	176
176	180	177	178	177
175	178	179	180	175

(a) 原始像素值

180	180	179	180	180
180	175	177	180	180
175	176	179	177	176
176	179	178	178	177

(b) 预测像素值

0	-1	1	0	0
-5	1	3	-2	-3
1	4	-2	1	1
-1	-1	1	2	-2

(c) 预测误差值

0	1	1	0	0
5	1	3	2	3
1	4	2	1	1
1	1	1	2	2

(d) 绝对值误差

0	1	0	0	0
1	0	0	1	1
0	0	1	0	0
1	1	0	0	1

(e) 误差符号标记

图3 多向梯度像素预测示例图

(2) 四叉树标记

为充分利用绝对值误差图像的各个位平面，使用公式将其划分为 8 个不同的位平面 $b^8, b^7, \dots, b^1$ ：

$$b^k(i, j) = \left\lfloor \frac{|e(i, j)| \bmod 2^k}{2^{k-1}} \right\rfloor, k = 1, 2, \dots, 8 \quad (10)$$

为了压缩每个比特平面的大小，通过四叉树标记依次将 MSB 到 LSB 的比特平面转化为压缩比特流 s^k 。四叉树标记是将图像分解为分层树结构，其中树的每个节点表示图像的特定方块，并具有 4 个不同的子节点。首先，以整个图像作为初始图像块，根据是否满足预定义的标准进行划分。

如果满足,则将其节点标记为“叶节点”,并且不再进行进一步的细分,否则,其节点标记为“中间节点”,并将图像块递归划分为4个更小的块,通过不断将图像块划分为左上角、右上角、左下角和右下角四部分,直到设定的最小尺寸 2×2 为止,如图4所示。当块内元素全为0时,视为可嵌入块(usable block, UB),标记为叶节点;否则,视为不可嵌入块(non-usable block, NB),进一步递归划分为更小的子块标记,以左上角子块为例,划分如图5所示。

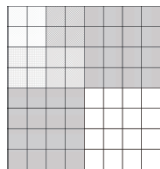


图4 图像递归分块

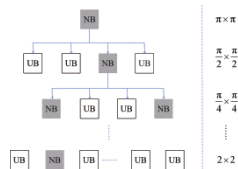
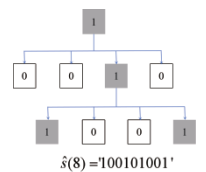


图5 四叉树示意图

为了改善NB块编码冗余的问题,提出当某区域的高位平面已被标记为NB块,且其相邻的低位平面同属于NB块,则不再进行类型标记,以生成压缩后的比特流 $\hat{s}^k$ 。这种优化策略有效减少了辅助信息的长度。为了更好地理解优化过程,在图6中给出相邻的两个位平面编码压缩示例。

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0

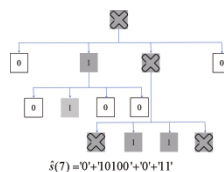
(a) b^8



(b) b^8 的压缩比特流

0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0
1	0	0	1	0	0	0	0

(c) b^7



(d) b^7 的压缩比特流

图6 相邻位平面编码压缩示例

首先对MSB位平面进行四叉树编码得到比特流 $\hat{s}^8 = s^8 = '100101001'$ 。根据 s^8 序列和 b^7 位平面共同生成 $\hat{s}^7$ 序列,具体地首先扫描 s^8 ,当遇到比特1时,继续扫描下一位;当遇到比特0时,需要根据四叉树编码算法扫描 b^7 位平面对应的子块,生成子树,依次递归,生成 $\hat{s}^7 = '0' + '10100' + '0' + '11'$ 。递归遍历所有位平面,即可得到整个图像的压缩比特流,为了提高嵌入容量,进一步使用霍夫曼编码压缩子节点所有出现的组合。最后,利用 K_e 流加密技术对图像实施加密,获得加密图像并进行传输。

2.2 数据嵌入

利用比特替换进行数据嵌入,首先需要内容持有者将辅助信息嵌入到加密图像中,其中包含可嵌入的位平面个数 n 、辅助信息长度、全局梯度 W_{gd} 、所有位平面的压缩比特流

SI、 $I(1,1)$ 、 b^8 中的NB块,以及各位平面的霍夫曼编码规则。最后数据隐藏者将秘密信息利用 K_d 进行加密,提取辅助信息以确定初始嵌入位置,进行比特替换完成数据嵌入。

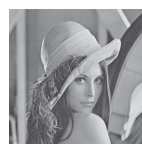
2.3 数据提取和图像恢复

如果接收者仅持有 K_d ,则从最高位平面提取UB中的比特,并以栅格扫描顺序所有像素,最后通过 K_d 解密获取秘密数据;如果接收者仅持有 K_e ,首先根据辅助信息恢复NB块中的原始比特位,利用密钥对图像进行解密,再根据SI重建四叉树获取所有位平面,根据和全局梯度 W_{gd} 恢复原始图像;如果接收者同时拥有 K_d 、 K_e ,可同时根据上述两种情况提取秘密数据和恢复原始图像。

3 实验与结果分析

3.1 实验环境与数据集

本文实验基于Windows11操作系统、Intel Core i9-12900HX CPU@2.3 GHz、16 GB RAM的PC端和Matlab2022(b)编程软件。选取6幅标准灰度图以及BOSSbase和BOWS-2两个灰度图像数据集作为实验对象,测试图像如图7所示。



(a) Lena



(b) Jetplane



(c) Man



(d) Baboon



(e) Tiffany



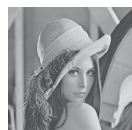
(f) Airplane

图7 测试图像

3.2 安全性分析

密文图像信息隐藏的安全性分析主要指嵌入秘密信息后不能破坏原始加密图像的安全性。

以Lena图像为例,图8显示了不同状态下的图像视觉效果以及不同阶段对应的像素分布直方图。



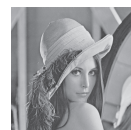
(a)



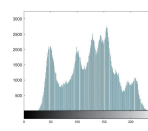
(b)



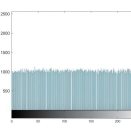
(c)



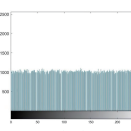
(d)



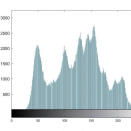
(e)



(f)



(g)



(h)

图8 Lena不同阶段像素分布图

其中(a~d)分别对应Lena图像的原始图像、加密图像、载密图像和重构图像,(e~h)对应像素分布直方图。结果显示,加密和载密图像均以噪声点呈现,难以观察其原始状态下的任何信息,保证了图像的安全性。

除了对图像的视觉效果进行分析以外,实验进一步使用统计指标评估。表1显示了Lena的原始图像、加密图像以及载密图像的相关性分析。

表 1 Lena 图像的相关性分析

Lena 图像	相关系数			信息熵
	水平	垂直	对角线	
原始图像 (a)	0.977	0.987	0.962	7.445
加密图像 (b)	0.004	0.002	0.006	7.999
载密图像 (c)	0.006	0.001	0.005	7.994

数据显示,加密和载密后的图像相关系数均接近0,且信息熵接近灰度图像的理想值8,证明加密是有效的,且信息的嵌入并不影响图像的安全性。

3.3 可逆性分析

本节对6幅测试图像的原始图像和重构图像进行相似程度判定。结果显示均方误差均为0、峰值信噪比均为以及结构性相似度均为1,分别达到了理想值,因此二者之间不存在差异,即算法具有完全可逆性。

3.4 嵌入容量分析

为验证所提算法在嵌入容量方面的优势,本文选取Wu等人^[5]、Liu等人^[6]、Chen等人^[2]、Yu等人^[4]及Yin等人^[3]的可逆信息隐藏算法进行对比分析,以嵌入率(bpp)作为主要评价指标。如图9所示,横轴为测试图像,纵轴为嵌入率。

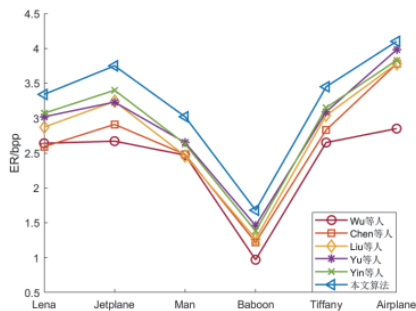


图 9 不同算法在测试图像上的嵌入率比较

值得注意的是,在纹理复杂的Baboon图像上,本算法取得了1.68 bpp的优异表现,明显优于现有方法。

最后,为了减少随机选择造成的实验结果误差,本文继续以BOSSbase和BOWS-2作为测试数据集进一步验证算法的普适性。结果如图10所示,纵轴表示平均嵌入率,本文所提出的算法在嵌入率方面能够取得比其他方法更好的结果。

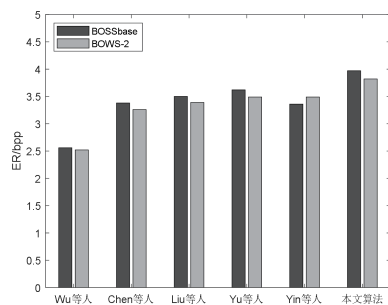


图 10 不同算法在数据集上的平均嵌入率比较

4 总结

本文针对现有密文域信息隐藏算法中预测精度不高、灵活性不够,难以应付复杂纹理变化图像的问题提出了多方向梯度预测器并改进了动态二叉树编码,提高了算法的嵌入容量。

参考文献:

- [1]YIN Z X, XIANG Y Z, ZHANG X P. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding[J]. IEEE transactions on multimedia, 2019, 22(4): 874-884.
- [2]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, 2020, 31(3): 905-916.
- [3]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.
- [4]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, 2021, 32(2): 451-466.
- [5]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, 2019, 22(8): 1929-1938.
- [6]LIU Y, FENG G D, QIN C, et al. High-capacity reversible data hiding in encrypted images based on hierarchical quad-tree coding and multi-MSB prediction[J]. Electronics, 2021, 10(6): 664.

【作者简介】

王文丽(1998—),女,山东临沂人,硕士研究生,研究方向:图像处理、信息隐藏。

(收稿日期:2025-03-31 修回日期:2025-09-24)