

说明文档

本实验的目标是通过在图片中嵌入水印，并在图片经过各种破坏性处理后，依然能够提取出水印，从而验证图片的归属和防止泄露。

实验原理与方法

实验采用了基于 DCT（离散余弦变换）的水印嵌入方法：

1. 将原图分块后进行 DCT，选择中频段系数进行微调来嵌入水印信息。这样既能保持较高的图像质量，又能提高对压缩和噪声的抵抗力。
2. 每个水印比特会重复嵌入多次，并在提取时采用多数投票法，以减少单点失真的影响。
3. 针对旋转、平移、翻转、裁剪、压缩、亮度和对比度调整等攻击，先用 ORB 特征匹配结合相位相关法，对被攻击图片进行几何校正，然后再提取水印。

提取过程

将校正后的图片进行 DCT，读取嵌入位置的系数变化来判断每一位是 0 还是 1，并将二进制序列还原成字符串。

实验结果

```
嵌入水印...

提取原始水印...
原始水印： 2025hh1605
提取水印： 2025hh1605

进行鲁棒性测试...

鲁棒性测试结果（位级/字符级准确率）：
noise       : bit_acc=97.50%, char_acc=80.00%, extracted='2 2µhh1605'
rotate_5    : bit_acc=100.00%, char_acc=100.00%, extracted='2025hh1605'
rotate_15   : bit_acc=95.00%, char_acc=60.00%, extracted='2025hl14°µ'
rotate_30   : bit_acc=90.00%, char_acc=50.00%, extracted=' 025hh34 µ'
crop_10     : bit_acc=62.50%, char_acc=0.00%, extracted='&c+¢04 ±'
brightness  : bit_acc=57.50%, char_acc=0.00%, extracted='µp0S' 0& '
contrast    : bit_acc=56.25%, char_acc=0.00%, extracted=' b0q" 0< '
flip        : bit_acc=100.00%, char_acc=100.00%, extracted='2025hh1605'
jpeg_q70    : bit_acc=98.75%, char_acc=90.00%, extracted='"025hh1605'
jpeg_q40    : bit_acc=87.50%, char_acc=40.00%, extracted=' p:5hh14¹9'
shift_5_5   : bit_acc=100.00%, char_acc=100.00%, extracted='2025hh1605'
```