project2 实验说明

Part 1:基于数字水印的图片泄露检测

1、实验内容

编程实现图片水印嵌入和提取（可依托开源项目二次开发），并进行鲁棒性测试，包括不限于翻转、平移、截取、调对比度等。

2、实验原理

本实验采用频域嵌入方法，核心是在图像 DCT 系数中嵌入水印信息。

2.1 离散余弦变换（DCT）

DCT 是将图像从空间域转换到频率域的常用工具，其核心思想是将图像分解为不同频率的余弦分量。对于数字图像，通常采用分块 DCT 降低计算复杂度。

8x8 块的 DCT 变换公式为：

$$F(u,v) = \frac{2}{N}C(u)C(v)\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\cos\left(\frac{(2i+1)u\pi}{2N}\right)\cos\left(\frac{(2j+1)v\pi}{2N}\right)$$

其中，f(i,j)为空间域像素值，F(u,v)为频率域系数，N=8 为块大小，C(k)为归一化系数。

2.2 中频系数选择的原理

DCT 系数按频率从低到高分布（左上角为低频，右下角为

高频）。

低频系数对应图像的平滑区域，能量集中，对视觉效果影响大（修改会导致明显失真）。

高频系数对应图像的细节（边缘、纹理），能量低，易受噪声、压缩等攻击影响（鲁棒性差）。

中频系数平衡了不可见性与鲁棒性 —— 既不会导致明显视觉失真，又能抵抗常见攻击，因此是水印嵌入的最优选择。

实验中通过 pattern 参数指定中频位置（如[(4,1), (3,2)]），即选择 DCT 系数矩阵中坐标为 (4,1) 和 (3,2) 的位置嵌入水印。

2.3 水印嵌入与提取

当 w(二值水印）=1 时，系数增加 strength；当 w=0 时，系数减少 strength，通过正负偏移区分水印比特。

要注意 strength 需权衡，过大会导致图像失真（不可见性差），过小则水印易被攻击破坏（鲁棒性差）。

3、实验过程（大致的实验思路，具体代码见 cpp 文件）

实验流程分为预处理、水印嵌入、水印提取、质量评估、鲁棒性测试五个阶段，核心代码通过 DCTWatermark 类和 RobustnessTester 类实现。

3.1 预处理

对输入图像的格式、尺寸进行调整：确保图像宽高为 block_size（实验中为 8）的整数倍，若不满足则通过填充处理。

对水印也要进行预处理。水印图像采用二值图像，尺寸需与嵌入位置数量匹配。

3.2 水印嵌入（DCTWatermark.embed）

调用_get_dct_blocks 方法，将预处理后的载体图像分割为 8x8 块，对每个块执行 DCT 变换。根据 pattern 参数定位每个 DCT 块中的系数位置。遍历所有图像块，按嵌入规则修改选中的中频系数（根据水印比特值加减 strength）。对修改后的 DCT 块执行 IDCT 变换，通过_merge_blocks 方法将块合并为完整的含水印图像。

3.3 水印提取（DCTWatermark.extract）

对含水印图像执行与嵌入阶段相同的分块和 DCT 变换。

3.4 质量评估（DCTWatermark.evaluate_quality）

通过 PSNR 和 SSIM 评估嵌入水印后的图像质量。

3.5 鲁棒性测试（RobustnessTester 类）

对含水印图像施加常见攻击，提取水印并通过归一化相关系数（NC） 评估鲁棒性。

$$NC = \frac{\sum_{i,j} w(i,j)\hat{w}(i,j)}{\sqrt{\sum_{i,j} w(i,j)^2}\sqrt{\sum_{i,j} \hat{w}(i,j)^2}}$$

其中w为原始水印，$\hat{w}$为提取水印。

3.6 具体攻击类型及实现

3.6.1 旋转攻击（apply_rotation）

将图像旋转指定角度（如 ±10°、±30°），模拟图像被旋转

后泄露的场景。

3.6.2 平移攻击（apply_translation）

沿 x/y 轴平移指定像素（如 ±5、±10 像素），模拟图像位置偏移。

3.6.3 裁剪攻击（apply_cropping）

按比例裁剪图像边缘（如 5%、10%），模拟图像被部分截取。

3.6.4 对比度调整（apply_contrast）

通过系数调整对比度。

3.6.5 高斯噪声（apply_gaussian_noise）

添加均值为 mean、方差为 sigma 的高斯噪声，模拟传输噪声。

3.6.6 缩放攻击（apply_resizing）

按比例缩放图像（如 0.5 倍、1.5 倍），模拟分辨率变化。

Part 2:实验总结

本次实验完成了基于 DCT 中频系数的水印算法，能有效平衡不可见性与鲁棒性。嵌入强度 strength 和嵌入位置 pattern 是关键参数，需根据实际场景（如图像类型、攻击风险）调整。

后续可通过采用更复杂的频率域进一步提升鲁棒性。