

Project2 图片的数字水印

一. 项目说明

基于数字水印的图片泄露检测 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

二. 项目原理

1. 总体思路

目标：把一个水印图像 w_m 嵌入到一张封面图像 $cover$ 中，使嵌入后图片肉眼几乎无差别，但在遭受攻击后仍能提取出可辨认的水印。

实现方式：不是直接在像素（空域）里改值，而是先把图片变换到频域（比如小波变换 DWT 或离散余弦变换 DCT），然后在低频或中频成分里嵌入水印，再逆变换回去。

2. 嵌入水印

1. 预处理

封面图和水印图灰度化、缩放到合适尺寸（保证比例一致），把像素值归一化到 $[0, 1]$ 或 $[0, 255]$ 。

2. 频域变换

对封面图做 DWT（离散小波变换），得到 LL（低频）、LH、HL、HH 四个子带。在低频 LL 区域嵌入水印，因为低频部分在压缩、模糊等攻击下更稳定。

3. 奇异值分解（SVD）嵌入

对 LL 子带做 SVD 分解，对水印图做 SVD 得到，修改封面图的奇异值。设 α 为嵌入强

度，强度越高水印越明显，鲁棒性越高，但画质降低

4. 逆变换

用修改后的奇异值 S' 重构 LL' ，再与原来的 LH 、 HL 、 HH 合成，做逆 DWT 得到嵌有水印的图像。

3. 提取原理

提取过程就是嵌入的逆过程：

1. 对水印图（可能被攻击）做 DWT + SVD
2. 得到估计的水印奇异值矩阵
3. 再用水印的 U_w 、 V_w 重构水印图

因为奇异值对多种攻击有稳定性，所以即使图片被旋转、压缩、模糊，水印仍能被一定程度恢复。

4. 鲁棒性原因

低频嵌入：低频信息在 JPEG 压缩、模糊中损失少，所以有鲁棒性。

SVD 稳定性：图像的奇异值在噪声和部分几何变换下变化不大，所以能保留水印信息。

三.代码运行结果

输入图片：cover.jpg wm.png

翻转、平移、截取、调对比度后得到图片：

1. flip（翻转）

攻击后：



提取得到水印：



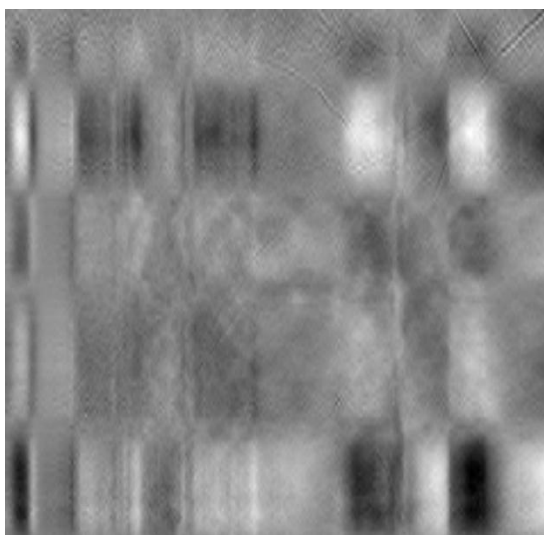
总结：纯翻转不会改变像素值分布，对提取水印影响小。

2. translate（平移）

攻击后：



提取得到水印：



总结：对大小不覆盖整张图的水印影响大

3. crop25（裁剪 25%）

攻击后：



提取得到水印：



总结：直接丢失一部分嵌有水印的像素，鲁棒性挑战大

4. contrast50（对比度调整 50%）

攻击后：



提取得到水印：



总结：影响较大，但能看出整体轮廓

5. jpeg40 (JPEG 压缩质量 40%)

攻击后：



提取得到水印：



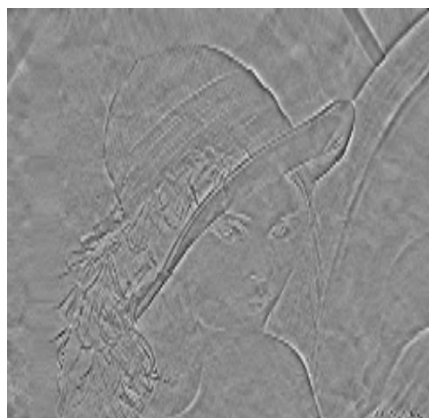
总结：对嵌入水印影响较小，能够辨认提取出的水印

6. blur5（模糊，核大小 5×5）

攻击后：



提取得到水印：



总结：影响较大，不过能看出轮廓

具体数据见 result.csv,其中各项意义：

1. PSNR_cover（峰值信噪比）

衡量嵌入水印后，图像的失真程度。值越大，说明嵌入过程对原图破坏越小。

- 范围：
 - 40 dB：人眼几乎看不出差异
 - 30 ~ 40 dB：视觉上有轻微差异
 - < 30 dB：差异明显

2. SSIM_cover（结构相似性）

从亮度、对比度、结构三方面综合衡量原始封面图与 水印嵌入后的图两张图的相似度，范围是 $[0, 1]$ ，越接近 1 越相似。

- 范围：
 - 0.98 ~ 1.00：几乎完全一致
 - 0.95 ~ 0.98：高相似度，肉眼几乎察觉不到
 - < 0.90：结构差异明显

3. NCC_wm（归一化互相关）

衡量水印提取的正确性，范围通常是 $[-1, 1]$ （但实际多在 $0 \sim 1$ 之间）。

- 范围：
 - 1.0 表示两张水印完全相同
 - 0.9+ 表示高度一致

- < 0.7 可能说明水印遭到较大破坏