Project 2: 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

一. 开源项目

依托 github 开源项目 [GitHub - RobinDavid/LSB-Steganography: Python program to steganography files into images using the Least Significant Bit.]
项目简介：本项目基于最低有效位（LSB, Least Significant Bit）隐写技术，实现了在数字图像中隐藏秘密信息的功能。通过修改图像像素 RGB 分量的最低位来嵌入数据，在保证视觉质量基本不变的前提下，将文本、图片或二进制文件等信息隐藏在载体图像中。

二. 验证基本水印功能

编写基础功能验证模块 test_basic.py 验证基本的水印功能
运行结果：

```python
# 1. 嵌入文本水印
carrier_img = cv2.imread("test.png")
steg = LSBSteg(carrier_img)
watermarked_img = steg.encode_text("basictest")
cv2.imwrite("watermarked.png", watermarked_img)

# 2. 提取水印
steg = LSBSteg(cv2.imread("watermarked.png"))
print("提取的水印:", steg.decode_text())
```

```
test_basic
C:\Users\涂佳桦\MobileFile\Scripts\python.exe D:\sdusummer\project2\LSB-Steganography\test_basic.py
提取的水印: basictest
```

三. 鲁棒性测试

攻击类型	实现代码	理论影响
几何攻击	cv2.flip(img, 1)	破坏像素空间关系
噪声攻击	cv2.add(img, np.random.normal(0,15,img.shape))	改变 LSB 位分布
压缩攻击	cv2.imencode(".jpg", img, [cv2.IMWRITE_JPEG_QUALITY, 50])	有损压缩破坏低位数据
色彩攻击	cv2.convertScaleAbs(img, alpha=1.3, beta=30)	改变像素值分布
滤波攻击	cv2.GaussianBlur(img, (5,5), 0)	导致像素值平均化

主要使用 OpenCV 和 Numpy 库中的函数实现攻击
实现攻击后尝试提取水印并计算 PSNR
最后输出测试结果

四．实验结果

```
C:\Users\涂佳桦\MobileFile\Scripts\python.exe D:\sdusummer\project2\LSB-Steganography\robustness_test.py
[1.水平翻转] 错误: SteganographyException: No available slot remaining (image filled)
[2.高斯噪声(σ=15)] 错误: SteganographyException: No available slot remaining (image filled)
[3.中心裁剪50%] 错误: SteganographyException: No available slot remaining (image filled)
[4.JPEG压缩(Q50)] PSNR: 32.61dB | 提取成功但数据为空
[5.亮度增强(α=1.3,β=30)] 错误: SteganographyException: No available slot remaining (image filled)
[6.高斯模糊(5x5)] 错误: SteganographyException: No available slot remaining (image filled)
```

问题分析

测试用例	问题分析
水平翻转	几何变换导致像素位置错乱，破坏 LSB 存储结构
高斯噪声	噪声直接修改像素 LSB 位，15 的σ值已超出容错范围
中心裁剪	有效数据区域损失 50%，水印信息不完整
JPEG 压缩	有损压缩破坏部分 LSB，但未触发异常（需检查水印嵌入量是否不足）
亮度增强	像素值线性变换导致 LSB 位系统性改变
高斯模糊	邻域像素平均化破坏孤立 LSB 信息

因为 LSB 水印直接放在特定坐标的像素上，所以一旦发生图片的反转，像素位置发生改变，就会无法识别有效水印。而且 LSB 只影响最低位，只要有像素值变化操作水印就不可识别。

结论：LSB 方法对几何变换的攻击方式几乎没有抵抗能力 需要改用更加复杂安全，鲁棒性更强的水印方法。