实验目的：

1. 了解图像水印攻击算法和效果，掌握通过stirmark软件进行图像水印攻击的方法。
2. 掌握机器学习的相关知识，学习使用TensorFlow深度学习平台，搭建卷积神经网络。
3. 掌握模型训练和优化的方法，得到拥有较快速度和较高准确率的分类模型。

实验原理：

数字水印技术是将一些标识信息直接嵌入数字载体当中，但不影响原载体的使用价值，也不容易被人的知觉系统察觉或注意到。对数字水印的攻击可分为三大类型：

1. 未经授权的删除
2. 未经授权的嵌入
3. 未经授权的检测

本次实验使用的图像水印攻击软件stirmark可以从多方面测试水印算法的鲁棒性，用于测试的攻击手段包括线性滤波、非线性滤波、剪切/拼接攻击、同步性破坏攻击等。

利用卷积神经网络强大的特征学习和分类能力，将其应用到水印攻击这一领域，快速准确地区分出各种水印攻击的类型。

实验所需环境及软件

1. Windows系统
2. Anaconda3
3. Python3.6
4. JetBrains PyCharm
5. Stirmark

实验流程：

1. 建立水印攻击数据库

将原图片放入stirmark中的Media\Input文件夹下。

修改stirmark软件中的SMBsettings.ini文件，将攻击方式设置为Test\_AddNoise、Test\_JPEG、Test\_MedianCut、Test\_ConvFilter。

运行StirMark Benchmark.exe文件，开始对原图片进行图像水印攻击，攻击后的图片保存在Media\Output文件夹下。

上传所有经过图像水印攻击的图片，建立水印攻击数据库。