**项目编号：201809060**

**东 南 大 学**

**大学生创新训练计划**

**成果简介**

**项目名称：**  图像水印中攻击类型分类方法研究

**项目级别：** □国家级 □省级 □校级 √院级 □基于教师科研

**项目负责人：** 吕健坤 学号：（ 71116333 ）

**电话：**  17302502357

**E-mail：**  sonatalv@qq.com

**项目参加者：** 陈玥 （学号：71116308）

井劭杰 （学号：71116234）

叶绵和 （学号：71116236）

张炯 （学号：71116334）

**项目指导教师：** 章品正 **（所属院系：计算机科学与工程学院** **）**

**电话：**  13770836015

**E-mail：**  luckzpz@seu.edu.cn

**项目迄止时间：**  2017 年 12 月-- 2018 年 11 月

**东 南 大 学 教 务 处**

# 项目背景

# 项目内容

## 图像水印攻击数据库的构建

要构建图像水印攻击数据库，我们首先要对目标图片集进行图像水印攻击处理，在本项目中我们决定使用Stirmark作为水印攻击测试软件。

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。许多公开发表的数字水印方面的论文都以Stirmark的攻击结果作为衡量水印算法好坏的标准。

要得到经过水印攻击处理的图片要进行以下几步操作：

1. 将原图片放入Stirmark中的Media\Input文件夹下；
2. 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；
3. 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。

进行上述操作后，我们就可以得到经过水印攻击处理的图片。

但是在使用Stirmark的过程中我们却遇到了不小的问题。当Stirmark一次处理的图片数量很大时，处理的速度会越来越慢，同时软件本身非常容易崩溃，而我们有数十万张图片需要进行四种不同的图像水印攻击，如果这个问题得不到解决我们建立受攻击数据库的效率就会非常低下。为了解决这个问题，我们仔细研究了Stirmark软件的崩溃日志并进行了大量的黑盒测试，发现了Stirmark处理速度下降的原因和发生崩溃的规律：前三种水印攻击方式的处理速度非常快，而第四种攻击方式的处理速度非常慢，从而拖慢了程序整体的速度；一次处理中的图片编号位数的变动会导致了崩溃。发现了问题的根源，我们决定采用分批分类的方法来对图片集进行水印攻击处理，而结果也符合我们预期，软件的处理速度有了大幅的提高，崩溃率也有了大幅的下降。

经过Stirmark的水印攻击处理，我们成功得到了数十万张经过水印攻击的、符合我们需要的图片，在将图片全部上传后，我们就构建出了后续用来训练和测试的图像水印攻击数据库。

## tfrecord数据集的制作

## 神经网络结构的选择及调参、优化

# 总结与展望