**项目编号：201809060**

**东 南 大 学**

**大学生创新训练计划**

**文献综述**

**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**

**数字水印技术与数字水印攻击**

数字水印技术（Digital Watermark）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（如听觉或视觉系统）察觉或注意到。目前主要有两类数字水印，一类是空间数字水印，另一类是频率数字水印。空间数字水印的典型代表是最低有效位（LSB）算法，其原理是通过修改表示数字图像的颜色或颜色分量的位平面，调整数字图像中感知不重要的像素来表达水印的信息，以达到嵌入水印的目的。频率数字水印的典型代表是扩展频谱算法，其原理是通过时/频分析，根据扩展频谱特性，在数字图像的频率域上选择那些对视觉最敏感的部分，使修改后的系数隐含数字水印的信息。

当前，图像数字水印技术已经发展到了一定的程度，作为版权保护的一种手段，数字水印势必受到各种形式的攻击，攻击是对水印强壮型的一个直观的评估方法。这就像传统密码学所经历的加密——解密的否定之否定的螺旋提高过程一样。我们有必要对水印攻击进行综合研究，从而能更深入了解和发现现有水印嵌入技术的弱点，进而促进更完善更强壮的水印技术的开发。

数字水印攻击自从1995年首次被提出，至今已经过了二十余年的发展，产生了大量的水印攻击方法，主要可分为三大类型：

1. 未经授权的删除
2. 未经授权的嵌入
3. 未经授权的检测

对数字水印的攻击需要对水印的嵌入和检测过程进行深入的分析和研究、从理论上来说，嵌入的水印信息总是可以被找到的，有些水印攻击方法就是在图像中寻找这些水印信息，并设法去除他们。这些攻击方法一般只对早期比较简单的水印算法有效。在一些较新的水印算法中吗，水印的嵌入过程中并不是直接修改图像的像素或频域系数，而是利用了图像空域或领域的局部或全局特征，并考虑了视觉模型的影响，这些水印算法具有较好的鲁棒性。对于这类水印算法，攻击者即使找到了水印信息也难以把它们完全去除，因此就出现了另一类水印攻击算法，不以完全去除水印信息为目的，而是通过对含水印图像做各种修改的方法破坏水印检测与嵌入信息之间的同步性，使得相对于水印检测算法来说攻击够图像中的水印不存在，从而达到攻击的目的。另外，还有一些水印攻击方法是以攻击水印应用概念和协议为目的而设计的。

**Stirmark水印攻击测试软件**

Stirmark是剑桥大学计算机实验室编写的一个用于测试图像水印技术鲁棒性的免费工具软件。

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。

Stirmark基准测试程序具有以下特征：

1. 使用用户提供的动态链接库作为水印标记方案函数；
2. 对在INI文件中指定的文件夹所包含的所有媒体文件执行测试；
3. 每个测试都可自定义，且测试参数可在INI文件中设置；
4. 在LOG文件中导出量化测试结果，同时在输出文件夹中导出失真图像；
5. 用户可容易地编写自定义的测试和攻击。

**参考文献**

[1]张新红，数字水印的攻击与反攻击，中国科技论文在线

[2]白梅，数字图像的水印攻击与对策研究，西安，西安建筑科技大学

[3]邹玉蓉，数字图像水印技术及其应用研究，上海，同济大学

[4]2001 Attack modelling towards a second generation watermarking benchmark

[5]2016 Beyond a gaussian Denoiser-Residual Learning of Deep CNN for Image Denoising