任务书

|  |  |  |  |
| --- | --- | --- | --- |
| 题目 | 抗攻击图像检索技术研究 | | |
| 姓名 | 彭佳真 | 学号 | 22920162204033 |
| 指导  教师 | 孙晓帅 | 职称 | 副教授 |
| 类型 | ☑论文 □设计 | 写作语言 | ☑中文 □其他\_\_\_\_\_\_ |
| 来源 | □纵向项目 ☑横向项目  □其它 | 选题方式 | ☑导师指定 □自选 |
| 论文写作要求 | （对论文写作目标、思路、方法、进度安排等提出要求）  本课题拟融合深度学习、图像检索及其相关的对抗攻击技术，研究并实现图像抗攻击检索的方法，增强图像检索的鲁棒性。在课题设计过程中，要求学生通过学习图像识别与检索及其对抗攻击防御技术的相关模型和算法，理解并掌握算法的原理，并将模型和算法应用到本研究课题中。毕业设计过程包含四个阶段：资料阅读和思路整理（3 个月）、毕业课题框架和算法设计（1 个月）、毕业课题编码与实验调优（2 个月）、论文撰写、修改与定稿（1 个月） | | |
| 支持条件 | （可提供必要的资料和数据支持）   1. 信息学院 MAC实验室深度学习服务器1台 2. 深度神经网络开发环境（Pytorch） 3. 数据支持：<https://github.com/theFool32/UAP_retrieval> 4. 熟悉掌握python编程 | | |
| 文献阅读要求 | （可列出推荐参考文献）   1. Database：ImageNet, Oxford5K, Paris6k，SfM 2. CNN Models: ResNet, AlexNet, VGGNet 3. Visual Features：GIST, VLAD, FV， Neural codes，DELF等 4. Adversarial Examples：Black-box attack，White-box attack, FGSM，UAP,DeepFool, AdvGAN等 | | |
| 签名 | 指导教师签名： 年 月 日 | | |

注：不足部分可加页。

开题报告

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 题目 | 抗攻击图像检索技术研究 | | | |
| 姓名 | 彭佳真 | 学号 | | 22920162204033 |
| 研究目标 | 本次毕业设计课题是融合了深度学习、图像检索及其相关的对抗攻击技术的综合性项目。这个项目主要研究抗攻击图像检索方法，使得图像在被经过一般的反检索（反识别）处理后，依然能被有效索引并检索到。在这个项目里要求学生能够熟练掌握深度学习相关知识，以便后续模型的修改与调试。项目成果主要应用于敏感图像的检测、搜索和过滤。  本次毕设项目要求学生设计实现的系统能够对图像检索系统的UAP攻击有效地防御，使得对给定图片检索时，能够保持一定的准确率。 | | | |
| 研究思路 | 1. 积累以下理论知识基础：卷积神经网络（CNN）、图像特征的提取、图像检索算法、对抗样本生成及其攻防技术。要求：阅读相关文献，了解其发展历程，学习其算法原理。 2. 重点研究论文《Universal Perturbation Attack Against Image Retrieval》，弄懂其对图像检索的攻击原理及其代码，根据所积累的系列原理，选择合适的算法并对其进行改进，使其可以嵌入在检索代码中，增强图像的鲁棒性，以防御该文中提到的攻击技术。 3. 为了将抗攻击图像检索方法移植到计算资源受限的应用环境中，针对另一种轻量化神经网络模型进行调整以适配使用的抗攻击图像检索方法，并进行训练、优化，使得本课题的抗攻击方法可应用于移动设备或嵌入式设备中敏感图像的检测、搜索和过滤。 | | | |
| 研究方法 |  | | | |
| 具体进度安排 | 起讫时间 | | 计划完成内容  (一般可分为资料文献搜索、拟定方案（提纲）、试验或初稿、定稿等阶段) | |
| 2019年11月10日-2020年2月10日 | | 资料文献收集整理与阅读 | |
| 2020年2 月11日-2020年3月10日 | | 拟定总体设计方案 | |
| 2020年3月11日-2020年4月 15日 | | 图像特征提取与模型训练 | |
| 2020年4月16日-2020 年4月31日 | | 防御功能实现与算法调优 | |
| 2020年4月20日-2020年5月 15日 | | 论文撰写、修改与定稿 | |
| 签名 | 学生签名： 年 月 日 | | | |
| 指导教师签名： 年 月 日 | | | |

注：不足部分可加页。

教师指导记录

|  |  |  |  |
| --- | --- | --- | --- |
| 题目 |  | | |
| 姓名 |  | 学号 |  |
| 第一阶段指导 | 指导教师签名： 年 月 日 | | |
| 第二阶段指导 | 指导教师签名： 年 月 日 | | |
| 第三阶段指导 | 指导教师签名： 年 月 日 | | |
| 第四阶段指导 | 指导教师签名： 年 月 日 | | |
| 第五阶段指导 | 指导教师签名： 年 月 日 | | |

注：不足部分可加页。

指导教师评语

|  |  |  |  |
| --- | --- | --- | --- |
| 题目 |  | | |
| 姓名 |  | 学号 |  |
| （从论文的选题、基本写作规范、文献综述、原创性、工作量、所取得的成果、学生的知识和能力，以及完成论文的态度等方面进行总体评价） | | | |
| 拟评成绩：  是否具备答辩资格：□具备 □不具备  指导教师签名： 年 月 日 | | | |

注：不足部分可加页。

答辩记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 题目 |  | | | | | |
| 学院 |  | | | 专业 |  | |
| 学生姓名 |  | | | 学号 |  | |
| 指导教师 | 张三（校外），王五（校内） | | | 职称 | 教授（校外），教授（校内） | |
| 答辩日期 | 年 月 日 | | | 答辩地点 |  | |
| 答辩小组 | 姓名 |  |  |  |  |  |
| 职称 |  |  |  |  |  |
| 答辩记录 | （包括论文陈述、答辩小组成员提出的主要问题及学生答辩的简要情况） | | | | | |
| 答辩记录 | （包括论文陈述、答辩小组成员提出的主要问题及学生答辩的简要情况） | | | | | |
| 答辩小组意见 | 是否通过答辩：□是 □否  答辩成绩：  组长签名：  成员签名：  秘书签名： 年 月 日 | | | | | |

|  |  |
| --- | --- |
| 论文总评成绩 | 总评成绩评定规则：  总评成绩：  院长（系主任）签名： 年 月 日 |

2029320381452802095400

**本 科 毕 业 论 文 （设 计）**

**（主修 / 辅修专业）**

面向非结构化企业指标信息的

智能处理和可视分析

**Indicators of the Unstructured Enterprise Information for Intelligence Processing and Visualization**

姓 名：

学 号：

学 院：

专 业：

年 级：

校内指导教师： (姓名) (职称)

校外指导教师： (姓名) (职务)

二〇 年 月 日**厦门大学本科学位论文诚信承诺书**

本人呈交的学位论文是在导师指导下独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合相关法律规范及《厦门大学本科毕业论文（设计）规范》。

该学位论文为（ ）课题（组）的研究成果，获得（ ）课题（组）经费或实验室的资助，在（ ）实验室完成（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明）。

本人承诺辅修专业毕业论文（设计）（如有）的内容与主修专业不存在相同与相近情况。

学生声明（签名）：

年 月 日