一、专业实践训练整体情况

<table>
<tr><td>实践单位
名称</td><td colspan="3">招银网络科技（杭州）有限公司</td></tr>
<tr><td>实践单位
地点</td><td colspan="3">杭州市滨江区信诚路 567 号</td></tr>
<tr><td>实践岗位
名称</td><td colspan="3">软件开发工程师</td></tr>
<tr><td rowspan="2">专业实践
训练时间</td><td rowspan="2">集中进行</td><td colspan="2">2021 年 10 月 01 日开始　至　2022 年 03 月 31 日结束</td></tr>
<tr><td colspan="2">专业实践训练累计　181　天（单位考核前），其中项目研究天数　150　天（单位考核前）</td></tr>
<tr><td colspan="4">（1）基本概况（含实践单位简介、实习实践内容等）

实践单位：
招银网络科技（杭州）有限公司
实践内容：
参与对人脸图像伪造技术以及检测此类伪造的方法进行研究</td></tr>
<tr><td colspan="4">（2）项目研究概述（含项目名称、项目来源、项目经费、主要研究目标和技术难点等）

项目名称：人脸图像伪造技术研究。
项目来源：实践单位。
项目经费：　无。
研究目标：针对不同类型的人脸图像伪造技术找到合适的检测方法。
技术难点：换脸算法的多样性导致检测方法对换脸算法及数据集不具有鲁棒性，只要稍微修改一下，检测算法的效果就会降低很多</td></tr>
</table>

（3）项目开展情况（含项目研究内容、研究方案及技术路线，研究团队分工、本人承担任务及完成情况，存在问题与改进建议等，不少于 500 字。）

研究内容：

人脸伪造技术对隐私，社会安全和民主的危害越来越大。现在有不同的算法生成换脸图像，甚至以后会有越来越多的新算法生成更逼真的换脸图像。这种威胁刚出现时，就已经提出了检测人脸伪造的方法。早期的尝试是基于从伪造的图片和伪造的图片合成过程的不一致性中获得的手工特征。后来的方法中引入了深度学习将其应用于自动提取突出特征和判别特征。项目主要研究了在人脸图像伪造和检测领域取得进展和未来趋势。

方案：

在图像采集过程中，每一张图像都有其独特的特征，它们可能来源于拍摄硬件，或者处理软件。只要不是一体生成的图像，它们在融合的过程中都会留下线索，这些线索人眼看不到，但深度学习能捕获。希望借助深度学习能检测到图像融合阶段产生的误差。

技术路线：

Java，python， SpringBoot， mysql， redis， kafka

团队分工：

数据团队协调各部门图像数据，完成数据搜集和存储；算法团队负责图像数据处理以及图像识假分析；基础团队负责基础平台建设以及业务组件开发。

本人承担任务：

本人参与基础平台的搭建与设计，负责基础设施能力开发以及业务组件设计开发工作。

完成情况：

项目启动初期，充分调研数据团队和算法团队的业务需求，梳理业务场景，分析技术要点，实现功能模块的设计和基础能力的下沉；项目实施过程中保持与数据、算法团队的有效沟通，合理划分功能迭代版本，及时跟进项目阻碍和风险，保证了项目进度正常按计划推进，同时负责基础模块功能的开发和测试，参与基础功能平台的搭建和发布，保证工程交付质量。

二、专业实践训练收获

（一）围绕考核评价指标体系，举例说明以下收获（不少于 800 字）

1.知识掌握。

了解了人脸伪造技术的常见类型：人脸合成可以创建完全不存在的人脸；换脸技术用于将一个人的脸换成另一个人的脸；人脸属性操纵可以修改人脸的诸如发色、肤色、性别、年龄、是否戴眼镜等属性；人脸表情操纵则用于修改人脸表情。人脸图像伪造技术通过“自动编码器”接收数据输入，提取面部图像的潜在特征，然后使用解码器重建面部图像来完成替换。常用检测技术会计算一张灰度图，如果模型检测出换脸的痕迹，它就会在灰度图上画出边界，检测模型需要经过生成训练样本以及训练模型两个阶段。

掌握了微服务框架的 6 大基础能力，服务发现、服务网关、统一配置中心、负载均衡、服务调用以及服务降级，学习了对基础框架进行定制化设计的思想和方法论，并能在项目中不同业务场景的要求中使用合适的设计模式。

2.能力提升。

需求分析以及系统设计能力有所提升：针对同一个业务需求，能够提供多种合理的实现方案，并能够在需求分析时有意识的进行灵活的设计，全盘考虑系统后期的可扩展性以及可维护性。

软件开发以及定位解决问题能力得以加强：保持良好的软件开发习惯，坚持定期进行代码检视和系统重构，学会了将大问题拆分成小问题再逐个进行分析解决，在解决问题后及时总结经验，避免相似的问题重复发生。

沟通协调以及项目管理能力得到锻炼：有机会组织各个团队定期进行沟通，协调不同团队间的信息不对称以及进度偏差，掌握了的从项目整体交付要求出发，合理安排各个迭代版本具体的工作量和实现功能范围，减少团队之间以及模块之间的耦合性。

3.素质养成。

项目实施过程中能够独立的思考和看待问题并坚持用科学的思想进行知识的探索和研究。清醒地认识自己在项目中所担负的责任，明确了自己的职业理想和发展目标，并持有坚定的信心和勇气。

通过学习和查阅相关专业文献和资料使我对专业的前沿知识有了更清晰的了解。学习过程中能态度端正、目的明确、刻苦专研，根据自身研究方向的要求，有针对性的认真研读了有关技术的核心内容。

在日常生活中，为人处世诚恳踏实，待人接物和善热情，生活朴实节俭，与同事关系融洽；在工作方面，保持认真负责的态度，实事求是，严格要求自己；而在空闲时间用心培养自己的业务爱好和兴趣，积极参加集体活动，努力弥补自身的不足。

（二）取得成效

1.通过技术应用创新、成果转化、解决企业工程实际问题等取得的经济和社会效益。

如今互联网信息中包含了大量的人脸图像数据，而且大型公共图像数据库也对外提供免费访问，再加上深度学习技术，特别是生成对抗网络的迅猛发展，伪造的人脸合成图像已经达到难以分辨真假的程度。人们发现将这种技术用于不道德和恶意的应用非常容易，而且深度伪造图片的质量一直在提高，检测方法的性能也需要相应提高。换脸与换脸检测是矛与盾的关系，两者相互促进与发展，使用高级机器学习创建深度仿造的人们与努力检测深度仿造的人们之间的斗争是长期共存的。

在投资理财、保险理赔、证券交易等安全性要求高的金融场景，运用人脸实名认证方案，将线下业务转为线上自助模式，满足远程开户、保险回执单等业务需求。但是人像图片和身份证图片存在 P 图伪造风险，人证很有可能为非真实信息。此时需要借助合适的校验机制确保真人且为本人，便于快速完成用户身份核验，减少企业人工审核成本的同时，提升用户体验。同时还可以辅助密码找回等密保措施，降低用户身份信息被恶意篡改、顶替冒用等风险，提升信息安全管理。

基础平台致力于提供既方便快捷又安全准确的人脸伪造识别解决方案，不仅提供管理分布在分布式存储和云中的数据以及保护数据隐私的能力，同时支持自定义设置人脸质量参数，识别拒绝率的阈值也可根据业务需求灵活配置；此外，依托于分布式系统架构强大的数据处理能力，基础平台可以实现统一的任务调度和分发，充分利用服务器资源，实现快速向用户提供业务就绪数据；最后，针对不同的人脸伪造识别场景，基础平台集成不同的功能模块，供用户进行灵活的聚合或裁减。

2.与学位论文撰写的相关程度。

拟定的学位论文方向是关于知识图谱的相关内容。知识图谱的主要目的是把复杂的知识领域通过数据挖掘、信息处理、知识计量和图形绘制而显示出来，揭示知识领域的动态发展规律，为学科研究提供切实的、有价值的参考。人脸图像伪造技术研究的课题也涉及研究数据实体的关联规则，并且也需要构建平台统筹数据算法和应用，与学位论文方向有一定的相关性。

3.在校期间主要研究成果【含产品与样机、专利（含申请）、著作、软件著作权、论文、标准、获奖、成果转化等】

成果名称	类别含产品与样机、专利（含申请）、著作、软件著作权、论文、标准、获奖、成果转化等]	发表时间/授权或申请时间等	刊物名称/专利授权 或申请号等	本人排名/总人数	学校排名/总参与单位数

本人承诺

在专业实践训练及考核报告撰写过程中，如实提供材料，严守学术道德、遵循学术规范。

签字：  2022 年 6月 1日

三、考核评价

校外合作导师(或现场导师)评价	**重点对研究生项目研究开展情况、职业素养、行业知识掌握、环境和岗位适应能力、工程实践能力、团队协作能力，以及通过技术应用创新、成果转化、解决工程实际问题等取得的经济和社会效益等方面的评价：** 雷亮同学参与项目研究过程中，学习积极主动，善于思考和解决问题，具有扎实的基础知识和专业的系统设计思维，很好的完成所负责的工作内容，体现了良好的职业素养。 校外合作导师（或现场导师）签字：邵冲强 2022年 6 月 1 日
校内导师评价	**重点对研究生科学素质、基础及专业知识掌握、技术应用创新能力、取得的研究成果、项目研究与学位论文撰写的相关程度等方面的评价：** 雷亮同学能够很好的将专业理论知识应用到实践项目中，并发挥主观能动性，具有良好的创新意识，项目研究中积累的专业知识和经验有利于后续学位论文的研究和撰写。 校内导师签字：[illegible] 2022 年 6 月 1 日

实践单位过程考核意见	**实际实践开始时间：**2021年 08月 01日 **实际实践结束时间：**2022年 03月 31日 **专业实践训练累计天数：** 242天 **其中项目研究天数：**180天 **实践单位过程考核结果：** ☐优秀 ☐良好 ☑合格 ☐不合格 审核签字并盖公章：2022年 06月 07日
最终考核结果审核备案	**考核总成绩（由现场答辩考核成绩 90%+单位过程考核成绩 10%组成）：** **是否重修：** ☐是 ☐否 教学管理部（或相关分院）审核签字（公章）： 年 月 日

四、相关支撑材料

在校期间主要研究成果【含产品与样机、专利（含申请）、著作、软件著作权、论文、标准、获奖、成果转化等】证明材料原件扫描件，具体提交要求如下：

1.产品与样机扫描件包含企业证明材料（含产品与样机功能及创新性介绍、社会经济效益、个人贡献说明及相关照片等）。

2.授权专利扫描件包含专利证书授权页；未授权专利扫描件包含专利受理书扫描件和专利请求书扫描件需加盖事务所公章或发明专利申请页（有二维码）。

3.著作扫描件包含封面、封底和版权页。

4.软件著作权扫描件包含著作权证书和事务所出具著作权人排序证明。

5.论文扫描件包含封面、封底、目录和论文全文（含收录证明）。

6.标准扫描件包含封面、版权页、发布公告、前言和目次。

7.获奖扫描件包含显示单位和个人排名的获奖证书。

8.成果转化扫描件包含企业证明材料（含成果技术说明、社会经济效益、个人贡献说明及相关照片等）。