阮受炜

153-9232-9486 shouweiruan@buaa.edu.cn 北京 海淀

Biography

- I am a Ph.D. candidate in the Institute of *Artificial Intelligence, Beihang University (BUAA)*, and also a visiting scholar in the *Department of Computer Science and Technology*, Tsinghua University. Before that, I received my B.E. degree in Intelligent Science & Technology from School of Artificial Intelligence, Xidian(XDU) University. I received the national scholarship in 2021 at Xidian University. I was a research summer intern in 2021 at Digital Team, Dell Technologies(China) Co, and was a research intern in 2022 at RealAI. For detail, welcome to my homepage: https://heathcliff-saku.github.io/
- 🔥 My research interests are primarily on adversarial robustness and generalization of computer vision. My recent research interests are related to visual-language model (VLMs) and embodied intelligence.

教育经历

清华大学 计算机科学与技术系 985 双一流 2022.04 - 2027.06

人工智能（计算机科学与技术） 访问学者

- TSAIL Group，联培导师：苏航 / 董胤蓬

北京航空航天大学 人工智能研究院 985 双一流 2022.09 - 2027.06

人工智能（计算机科学与技术） 博士

- 数字媒体北京市重点实验室，导师：韦星星

西安电子科技大学 人工智能学院 211 双一流 2019.09 - 2022.06

智能科学与技术 本科

- GPA：3.8/4.0 前6学期综合排名：2/310

学术成果

出版物 (🔥: 代表性工作)

- 🔥 **Omniview-Tuning: Boosting Viewpoint Invariance of Vision-Language Pre-training Models**
  Shouwei Ruan, *Yinpeng Dong, Hanqing Liu, Yao Huang, Hang Su, Xingxing Wei.*
  *European Conference on Computer Vision (ECCV), Milan, Italy, 2024. (**CCF-B**)*
- **DIFFender: Diffusion-Based Adversarial Defense against Patch Attacks in the Physical World**
  *Caixin Kang, Yinpeng Dong, Zhengyi Wang, **Shouwei Ruan**, Hang Su, Xingxing Wei.*
  *European Conference on Computer Vision (ECCV), Milan, Italy, 2024. (**CCF-B**)*
- **Exploring the Robustness of Decision-Level Through Adversarial Attacks on LLM-Based Embodied Models**
  *Shuyuan Liu, Jiawei Chen, **Shouwei Ruan**, Hang Su, Zhaoxia Yin.*
  *ACM Multimedia (ACM MM), Melbourne, Australia, 2024. (**CCF-A**)*
- **Towards Transferable Targeted 3D Adversarial Attack in the Physical World**
  *Yao Huang, Yinpeng Dong, **Shouwei Ruan**, Xiao Yang, Hang Su, Xingxing Wei.*
  *IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, USA. (**CCF-A**)*
- 🔥 **Towards Viewpoint-Invariant Visual Recognition via Adversarial Training** [paper] [code]
  Shouwei Ruan, *Yinpeng Dong, Hang Su, Jianteng Peng, Ning Chen, and Xingxing Wei.*
  *International Conference on Computer Vision (ICCV), Paris, France, 2023. (**CCF-A**)*
- 🔥 **ViewFool: Evaluating the Robustness of Visual Recognition to Adversarial Viewpoints** [paper] [code] [slide]
  *Yinpeng Dong, **Shouwei Ruan**, Hang Su, Caixin Kang, Xingxing Wei, and Jun Zhu.*
  *Advances in Neural Information Processing Systems (NeurIPS), New Orleans, USA, 2022. (**CCF-A**)*
- 🔥 **Improving Viewpoint Robustness for Visual Recognition via Adversarial Training**
  Shouwei Ruan, *Yinpeng Dong, Hang Su, Jianteng Peng, Ning Chen, and Xingxing Wei.*
  *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), **under review**.*
- 🔥 **Distributional Modeling for Location-Aware Adversarial Patches**
  *Xingxing Wei, **Shouwei Ruan**, Yinpeng Dong, Hang Su.*
  *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), **under review**.*

专利与著作权

- 计算机软件著作权：极智安行—人工智能驾驶辅助系统 （登记号：2021SR1316695）

开源项目

- AREFR (Adversarial Robustness Evaluation for Face Recognition) 人脸识别对抗鲁棒性评估平台
  关注人脸识别系统安全性测试，实现4种人脸识别模型、6种对抗攻击算法、评估以及其他工具性的代码接口
  GitHub：*https://github.com/Heathcliff-saku/AREFR.git*

荣誉奖项

- 2022~2023年度 北京航空航天大学校级三好学生 2023.11
- 西安电子科技大学 优秀毕业生 2022.06
- 2020~2021年度 国家奖学金 校优秀学生标兵 2021.10
- 2021~2022年度 西电创新楷模 2021.11
- 2020~2021 校优秀共青团干部 2021.05
- 第七届“互联网+”创新创业大赛 全国金奖 总决赛六强 2021.07
- 美国大学生数学建模竞赛(MCM/ICM) Meritorious Winner（国际一等奖) 2021.04
- 2021年全国大学生节能减排社会实践与科技竞赛 全国三等奖 2021.06
- 第十三届“挑战杯”全国大学生课外学术科技作品竞赛 省级一等奖 2021.05
- 2021年中国大学生计算机设计大赛 西北赛区一等奖 2021.06
- 2020年全国大学生数学建模竞赛 省级二等奖 2020.10

科研经历

雏鹰计划重点科研项目 — 《基于深度学习与顺序学习的面部年龄估计技术研究》 项目负责人 2019.07 - 2021.04

西安电子科技大学 海棠7号书院实验室

- 担任项目负责人，进行小样本、轻量级的人脸年龄估计算法的研究。
- 我在项目中负责统筹安排项目进度，复现经典年龄预测算法、撰写研究型综述，受到人脑对于年龄关系认知的启发，设计基于比较学习的年龄估计算法。
- 该项目被评为【雏鹰计划重点项目】，并获得优秀结题证明。依托该项目所开发的《极智安行—基于年龄分层的危险驾驶行为检测系统》获得【中国大学生计算机设计大赛】西北赛区一等奖

挑战杯项目 —《灵眸视觉—基于反射放大的无线低功耗智能监控系统》 项目核心成员 2021.02 - 2021.05

西安电子科技大学 创新创业学院

- 该项目是基于反射放大电路的无线低功耗数据传输监控系统，运用目标检测领域的深度学习算法，进行了多场景应用的开发。
- 我在该项目负责前后端的智能算法设计，利用YOLOv5对大型活动场景下危险物品携带者的排查模块。
- 该项目已成功获得第十七届【**挑战杯**】陕西省赛区一等奖，我作为团队核心成员参与决赛答辩

国家级大创 — 《基于高灵敏度微米级叉指电极的相关研究》 项目核心成员 2018.09 - 2021.05

西安电子科技大学 材化创新坊

- 该项目主要进行微型叉指电极的制备与特性研究，实现其在物质扩散系数测定的应用。
- 我在项目中跟进微电极光刻到测试的全部流程。对微电极表面的镀膜技术进行研究，并测定了氢离子扩散系数。
- 该项目成功申报【**国家级大学生创新创业计划**】并结题，我在项目中负责微米电极的版图设计和实验数据分析。

工作与实习经历

戴尔(中国)有限公司 2021.07 - 2021.08

机器学习工程师实习生 数字化团队 福建 厦门

- 主要工作内容为机器学习/深度学习算法开发，进行戴尔EMC服务器的生产线测试模块的自动化算法开发。
- 负责制作并标注了工业LED检测灯数据集，基于YOLOv5模型设计了工业LED检测灯的识别与分类算法框架，并辅助开发系统在硬件方面（如工业摄像机）的调用程序。
- 项目入选戴尔制造2025计划，目前相关算法已成功应用于生产线，在最终的项目汇报中评为亚太地区实习生团队第三名

学生工作和社会实践

西安电子科技大学 材料院学生会 副主席 2020.09 - 2021.06

- 统筹管理学生会工作，主要负责文艺部和礼仪队的活动安排与策划。
- 期间担任材料院2020迎新晚会总策划、宣传视频《你要在西电跳舞吗》《西电disco》导演，全网累积播放量超3万

西安电子科技大学 材料院学生会 文艺部部长 2019.09 - 2020.06

- 负责材料院各项文艺活动，如校舞蹈大赛、运动会方阵、晚会的策划、组织、排练。
- 我担任2019年材料院迎新晚会总导演，获学院领导高度认可。期间策划并主演宣传片《西电抖肩舞》全网获50万播放量。

西电volume up音乐社 主席 2019.09 - 2020.06

- 作为社团负责人，负责对接校团委、进行活动策划、社团成员声乐练习，期间组织举办了“5.20”专场演唱会。

专业技能

- **编程**：**Python**：熟练掌握pytorch (深度学习框架) 和sklearn (机器学习库)
  MATLAB：掌握矩阵运算、数字信号仿真测试、数字滤波器设计、图像处理算法等
  JavaScript：掌握Highcharts、Echarts等前端数据可视化工具
- **外语能力**： **CET-4**：534分 **CET-6**：471分