

手机/微信: (+86) 15397310001
邮箱: zhaoyuchen20@fudan.edu.cn
地址: 上海市杨浦区邯郸路 220 号

陈兆宇

Google Scholar
Home Page



教育背景

山东大学	计算机科学与技术 (本科)	2016 年 9 月到 2020 年 7 月
荣誉奖项: CET-4, CET-6, 一等奖学金 (前 5%), 山东省优秀毕业生;		GPA: 87.93/100.0 (5/101)
复旦大学	计算机应用技术 (直博生)	2020 年 9 月至今

研究方向: AI 安全、多模态大模型、AIGC、计算机视觉 **GPA: 3.63/4.0 (7/50)**
荣誉奖项: 华泰证券科技奖学金 (前 1%), 一等奖奖学金 (前 5%), 一等优秀博士候选人奖学金 (前 3%)
论文专利: 发表 CCF A 类会议/期刊和 SCI 一区期刊 19 篇, 以一作和共一在 CVPR、ICCV、ECCV、NeurIPS、AAAI、TIFS 等国际顶会和顶刊发表论文 8 篇, 并申请国家发明专利 5 项; 学术服务包括担任 CVPR、ICCV、ECCV、NeurIPS、ICML 和 ICLR 会议的审稿人, TPAMI、TNNLS、NN、TCSVT 和 KBS 期刊的审稿人; 知乎上论文分享, 粉丝过万;

实习经历

深圳市腾讯计算机系统有限公司	CSIG-优图实验室-盘古研究中心	2021 年 4 月到 2024 年 4 月
· 业务: 为活体检测和人脸篡改检测模型提供数字域和物理域的对抗样本, 评估业务模型的对抗鲁棒性;		
· 科研: 为业务提供对抗攻防的技术预研, 调研和总结人脸安全的相关技术, 对物理攻击和黑盒攻击进行落地实践;		
维沃移动通信有限公司 (vivo)	影像算法研究部-质量增强算法中心	2024 年 5 月至今
· 基于多模态大模型, 实现面向摄影场景的 Agent, 使其可以根据用户反馈和拍摄场景给出拍摄参数、模式等建议;		

科研经历

- ### 基于 AIGC 的对抗内容生成
- 提出首个基于扩散模型的无限制对抗样本生成方法和视频数据对抗防御方法, 代表性成果:
 - *Content-based Unrestricted Adversarial Attack* 以**第一作者**发表于 NeurIPS 2023;
 - *VideoPure: Diffusion-based Adversarial Purification for Video Recognition* 以**共同通讯作者**在投于 IEEE TIFS 期刊;
- ### 基于基础视觉模型的鲁棒性研究
- 探究预训练视觉模型是否能提高和传递鲁棒性问题, 并对多模态大模型提出对抗鲁棒性分析方法, 代表性成果:
 - *Towards Practical Certifiable Patch Defense with Vision Transformer* 以**第一作者**发表于 CVPR 2022;
 - *Out of Thin Air: Exploring Data-free Adversarial Robustness Distillation* 以**共同第一作者**发表于 AAAI 2024;
 - *Boosting the Transferability of Adversarial Attacks with GMI* 以**共同第一作者**发表于 ESWA 期刊 (中科院一区);
 - *Improving Adversarial Transferability of VLP Models through Collaborative Multimodal Interaction* 以**共同第一作者**获得 CVPR 2024 Workshop Challenge: Black-box Adversarial Attacks on Vision Foundation Models 的**第一名**;
- ### 面向视频模型的对抗鲁棒性分析
- 针对视频识别和视频目标分割模型的白盒和黑盒脆弱性问题, 提出了对应的鲁棒评估方法, 代表性成果:
 - *Efficient Decision-based Black-box Patch Attacks on Video Recognition* 以**共同第一作者**发表于 ICCV 2023;
 - *Towards Decision-based Sparse Attacks on Video Recognition* 以**共同第一作者**发表于 ACMMM 2023 (**Oral**);
 - *Exploring the Adversarial Robustness of VOS via One-shot Adversarial Attacks* 以**共同通讯作者**发表于 ACMMM 2023;
- ### 面向图块攻击的对抗攻防研究
- 针对白盒图块攻击性差和黑盒图块攻击效率低的问题, 提出了可微形变对抗图块和进化图块攻击, 代表性成果:
 - *Shape Matters: Deformable Patch Attack* 以**第一作者**发表于 ECCV 2022;
 - *Query-Efficient Decision-based Black-Box Patch Attack* 以**第一作者**发表于 IEEE TIFS 期刊 (CCF A, 中科院一区);

项目经历

基于 Django web 框架的山大机电学院毕业设计管理平台研发	后端开发	2018 年 9 月到 2019 年 3 月
· 需求调研, 后端开发, 完成主要算法部分设计, 后期部分维护工作, 已经被学院使用三年, 服务六千余人。		

竞赛经历

CVPR24 Workshop: 视觉基础模型的黑盒攻击**第一名** CVPR21 Workshop: 防御模型的白盒对抗攻击 (9/1681)
CVPR21 Workshop: ImageNet 无限制对抗攻击 (10/1599) 2019 年 ACM ICPC 南昌邀请赛铜牌