苏悦

西安电子科技大学 | 智能科学与技术

基本信息

男　19岁　汉族

电话/微信：18062089249　　邮箱：s3702681@gmail.com

个人主页：　selen-suyue.github.io

西安电子科技大学 - 人工智能学院 - 智能科学与技术（2022-2026）

课程情况

- **推免课程均分 88.5，Core GPA 3.8/4**
- **专业排名　【待第六学期更新推免排名】**
- **代表课程**

  高等数学 94　*概率论* 90　*电路分析* 96　*数据结构* 98　*线性代数* 89

科研经历

- **协同智能教育部重点实验室公茂果老师团队**　　*2023.9 至今*

  从大二学年开始跟随团队李豪老师进行视觉对抗攻击研究

- ***基于多任务进化的多方安全研究***　　*2023.9-2023.11*

  在传统的多任务进化算法中考虑隐私安全保护问题，用同态加密和差分隐私技术优化多任务进化的知识迁移过程。

- **Advtype:针对红外检测模型的对抗攻击**　　*2023.9-2024.1*

  论文三作（学生二作），IJCAI-2024 Reject （2WA1WR）

AdvDisplay: Adversarial Display Assembled by Thermoelectric Cooler for Fooling Thermal Infrared Detectors

针对YOLO模型在红外行人检测任务上进行对抗攻击，通过将其建模为优化问题来部署TEC板以达到规避检测的效果

- **Advpull:针对多模态图像匹配任务的对抗攻击**　　*2024.1-2024.5*

  独立提出想法和主持研究，实验基本完成，预计一作投递 AAAI-2025

考虑RGB和红外图像的匹配问题（以ReID任务为场景）往往依赖于边缘特征，我们首次将生成模型引入物理对抗攻击，通过提取图像的边缘特征并通过解码器生成补丁，在对抗性训练中完善补丁，然后装饰补丁以诱导模型误分类

竞赛与项目经历

- **河体堵江识别项目**　　*2023.8-2023.12*

基于语义分割的河体堵江任务识别，在SAR图像拍摄的黄河某河段三年内的堵塞情况图中通过河体关键特征检测以实现对未来河体堵塞情况的预测。

- **数学建模国赛省级一等奖**　　*2023.9*

果商的水果进货和销售价格的动态规划建模任务

- **计算机设计大赛（Advpull投入应用）**　　*2024.4-2024.5*

团队负责人，项目目前已送审国赛，我们针对Advpull所涉及的图像匹配问题设计了两种攻击算法，一种是基于CNN的灰盒对抗攻击，另一种是基于ViT-GAN架构的端到端地黑盒对抗攻击

- **一些大作业项目**　　*2023.11-2023.12*

1.通过蒙特卡洛树搜索的强化学习方法设计智能五子棋算法

2.通过DE差分进化算法解决NP难问题（以TSP为例）

语言与技能

语言：**CET-4：552**　　**CET-6：504**

技能：良好的表达能力（西电校辩论赛冠军） 等