

# 向文钊

算法工程师

5-318, 电子信息与电气工程学院, 上海交通大学, 上海, 200240, 中国

☎ (+86) 158-2193-7913 | ✉ wenzhao-xiang@foxmail.com | 🌐 wenzhao-xiang.github.io/Blog/ | 📷 Wenzhao-Xiang



## 个人简介 Biography

我是上海交通大学电子系图像通信与网络工程研究所的三年级硕士研究生，我的导师是郑世宝教授，而我本科同样就读于上海交通大学电子系。我在大二时入选了“卓越工程师培养计划”，并于2019年保研至电子系图像所。2018-2019年，我在英特尔亚太研发中心实习，在此期间完成了毕设课题并获得了2019年英特尔最佳实习生。2020年03月至今，我作为访问学者在清华大学计算机系智能技术与系统国家重点实验室的朱军/苏航老师的课题组(TSAIL Group)中进行科研工作。

我的研究领域包括机器学习、深度学习以及它们在计算机视觉中的应用。目前，我的主要研究方向是深度学习的对抗鲁棒性问题。

## 教育 Education

上海交通大学

本科，信息工程

上海, 中国

2015年9月 - 2019年6月

上海交通大学

硕士，电子与通信工程

上海, 中国

2019年9月 - 2022年3月

## 学术成果 Academic Achievements

论文

- Wenzhao Xiang, Chang Liu, and Shibao Zheng. "Improving Visual Quality of Unrestricted Adversarial Examples with Wavelet-VAE." *ICML 2021 Workshop on Adversarial Machine Learning*. 2021.
- Wenzhao Xiang, Hang Su, Chang Liu, Yandong Guo, and Shibao Zheng, "Improving robustness of adversarial attacks using an affine-invariant gradient estimator," *arXiv preprint arXiv:2109.05820*, 2021. (TIFS<ccf-a> 投稿中)
- Xiao Yang, Yinpeng Dong, Wenzhao Xiang, Tianyu Pang, Hang Su, Jun Zhu, "Model-Agnostic Meta-Attack: Towards Reliable Evaluation of Adversarial Robustness", 2021. (NeurIPS 2021 审稿中)

专利

- "Enhancing Transferrable Adversarial Examples With Affine-Invariant Attacks", 2020. (实质审查)
- "Unrestricted Adversarial Attack Method Based on Frequency Domain Transformation", 2021. (实质审查)

## 比赛 Contests

- |      |  |        |
|------|--|--------|
| 2021 | 亚军, 阿里云天池竞赛/CVPR2021 安全 AI 挑战者计划第六期赛道二: ImageNet 无限制对抗攻击 | 北京, 中国 |
| 2020 | 第九名, 阿里云天池竞赛/CIKM2020 安全 AI 挑战者计划第四期: 通用目标检测的对抗攻击        | 北京, 中国 |
| 2019 | 二等奖 (前 3), 华为 ICT 创新大赛全球总决赛                              | 深圳, 中国 |
| 2019 | 优胜奖, 华为开发者大赛 IoT 赛道                                      | 深圳, 中国 |
| 2018 | 全国一等奖/华为创新奖, 全国大学生物联网竞赛                                  | 无锡, 中国 |
| 2018 | H 奖, 美国大学生数学建模比赛   | 上海, 中国 |

## 项目 Projects

- |      |  |        |
|------|--|--------|
| 2020 | TSAIL Group, "Adversarial Robustness Evaluation for Safety" (ARES) 平台的开发     | 北京, 中国 |
| 2020 | 上交大图像所, 基于裂隙灯图像的人眼白内障分级诊断  | 上海, 中国 |
| 2019 | Google Summer of Code 2019, 基于 WebAssembly threads 和 SIMD 技术的 OpenCV.js 性能优化 | 上海, 中国 |
| 2019 | 英特尔亚太研发中心, 基于 WebAssembly 的 Web 深度学习推理引擎的实现与优化 (本科毕设)                        | 上海, 中国 |
| 2018 | 教育部-华为产学研合作协同育人项目, 基于 OceanConnect 平台的部分智能家居实现                               | 上海, 中国 |
| 2017 | 卓越工程师计划, 基于 Arduino 与 Android 平台的智能循迹避障遥控小车设计                                | 上海, 中国 |

## 工作经历 Work Experience

---

### 英特尔亚太研发中心

机器学习工程师 (实习)

上海, 中国

2018 年 7 月 - 2019 年 9 月

### 华为诺亚方舟实验室

AI 工程师 (实习)

北京, 中国

2021 年 9 月 - 现在

## 荣誉 & 奖励 Honors & Awards

---

2020 英特尔奖学金

上海, 中国

2020 上海交通大学优秀研究生一等奖学金

上海, 中国

2019 英特尔亚太研发中心最佳实习生

上海, 中国

2018 上海交通大学 C 类奖学金

上海, 中国

2017 国家励志奖学金

上海, 中国

2016 唐仲英德育奖学金

上海, 中国

## 技能 Skills

---

机器学习框架 Pytorch, Tensorflow, OpenCV, Matlab

编程 C/C++, Python, JavaScript(WebAssembly), Node.js, LaTeX

语言 Chinese, English