毛 潇锋

18668411821 hzmaoxiaofeng@163.com github.com/vtddggg
阿里巴巴人工智能治理与可持续发展实验室 计算机硕士 1994-07-26 杭州

我目前在阿里巴巴人工智能治理实验室（AAIG）担任算法工程师。此前在哈尔滨工程大学获得了硕士学位，在东北大学获得了学士学位。有丰富的大规模模型训练经验，以及 TensorRT 算法服务部署经验，我的研究兴趣包括对抗机器学习，计算机视觉和预训练大模型。

过往经历

2019.09 2013.09	**阿里巴巴集团** • 人工智能治理与可持续发展实验室 算法安全 • 算法工程师
2019.06 2016.09	**哈尔滨工程大学** • 计算机科学与技术学院 计算机视觉 • 硕士学位
2016.06 2012.09	**东北大学** • 计算机与通信工程学院 物联网工程 • 学士学位

科研成果

- NeurIPS2022 一作: Enhance the Visual Representation via Discrete Adversarial Training
- CVPR2022 一作: Towards Robust Vision Transformer
- AAAI2021 一作: Composite Adversarial Attacks
- ICASSP2020 一作: Learning to Characterize Adversarial Subspaces
- ICASSP2019 一作: Bilinear Representation for Language-based Image Editing Using Conditional Generative Adversarial Networks
- Neurocomputing 一作: Semantic invariant cross-domain image generation with generative adversarial networks
- CVPR2021 二作: Adversarial Laser Beam: Effective Physical-World Attack to DNNs in a Blink
- TIP 三作: Fine-Grained Fashion Similarity Prediction by Attribute-Specific Embedding Learning
- Neurocomputing 三作: Multi-level Alignment Network for Domain Adaptive Cross-modal Retrieval
- ACM MM2020 四作: Sharp Multiple Instance Learning for DeepFake Video Detection
- ICASSP2019 四作: Self-Supervised Adversarial Training
- ICASSP2021 五作: Adversarial Examples Detection Beyond Image Space
- IJCV 在投: Context-Aware Robust Fine-Tuning
- ICCV2023 在投: COCO-O: A Benchmark for Object Detectors under Natural Distribution Shifts

竞赛成果

- 2022 NICO Hybrid Context Generalization Challenge (ECCV 2022 Workshop) 第一名
- Fashion-Gen: The Generative Fashion Dataset and Challenge (ECCV 2018 Workshop) 第一名

参与项目

- EasyRobust: (29 fork, 216 star) 一款基于 Pytorch 的鲁棒视觉训练框架
- Visual Tracking api: (35 fork, 91 star) 基于 Python 的视觉跟踪工具箱
- 第一、二、四、六、八期安全 AI 挑战者计划赛事的主要技术负责人
- (内部项目) 应用级人脸检测/识别算法服务开发及鲁棒性优化
- (内部项目) 应用级内容风险识别算法服务开发及鲁棒性优化

学术经历

- Track 2 Winner Talks: in ECCV2022 Workshop @ 2nd Causality in Vision
- Invited Talk: in AAAI2022 Workshop @ Adversarial Machine Learning and Beyond
- Keynote Speak: in CIKM2020 Analyticup @ Alibaba-Tsinghua Adversarial Challenge on Object Detection
- Organizer: AAAI2022 Workshop on Adversarial Machine Learning and Beyond
- Organizer: CVPR2021 Workshop on Adversarial Machine Learning in Real-World Computer Vision Systems and Online Challenges (AML-CV)
- Organizer: IJCAI2019 1th Workshop on Artificial Intelligence for Business Security
- Reviewer: AAAI2021, ACMMM2021, CVPR2022