于瀚勋

■ hanxun.yu@zju.edu.cn · • 17519137080 · 个人主页:hanxunyu.github.io

教育经历

浙江大学 硕博连读 人工智能

2023/09 - 2028/06

- 导师: 朱建科教授
- 研究方向: 开放词汇下视觉场景理解/物体定位、多模态大模型、token 压缩及轻量化 MLLM
- GPA: 4.0 / 4.0
- 浙江大学-蒋震奖学金
- 浙江大学-优秀学业奖学金

武汉大学 本科 计算机科学与技术

2019/09 - 2023/06

- GPA: 3.8 / 4.0
- 研究方向: 视觉安全、可信人工智能 (Trustworthty AI)、对抗/后门攻击 (Adversarial/Backdoor Attack)
- 国家奖学金 (Top 2%) 2022 年
- 加拿大 Mitacs-CSC 国家公派实习奖学金 2022 年
- 优秀学生甲等奖学金 (Top 5%) 2020, 2021, 2022 年
- 校级优秀毕业生 2023 年

发表论文

- VisionTrim: Unified Vision Token Compression for Training-Free MLLM Acceleration.
 Hanxun Yu*, Wentong Li*, Xuan Qu*, Song Wang, Junbo Chen, Jianke Zhu.
 在 MLLM 推理过程中高效的视觉 token 压缩方法,已投稿至 ICML2025
- Inst3D-LMM: Instance-Aware 3D Scene Understanding with Multi-modal Instruction Tuning.
 Hanxun Yu*, Wentong Li*, Song Wang, Junbo Chen, Jianke Zhu.
 实例级三维场景理解多模态大模型 Inst3D-LMM, 已投稿至 CVPR2025 (初始得分:5、5、4)
- Moiré Backdoor Attack (MBA): A Novel Trigger for Pedestrian Detectors in the Physical World. ACM MM 2023(CCF A 类会议)

Hui Wei*, **Hanxun Yu***(共同一作), Kewei Zhang, Zhixiang Wang, Jianke Zhu, Zheng Wang. [Paper] [Code]

• Physical Adversarial Attack Meets Computer Vision: A Decade Survey.

IEEE TPAMI 2024 (CCF A 类期刊)

Hui Wei, Hao Tang, Xuemei Jia, Zhixiang Wang, **Hanxun Yu**, Zhubo Li, Shin'ichi Satoh, Luc Van Gool, and Zheng Wang.

[Paper] [Code]

• Aesthetic Yet Customizable Adversarial Patches Towards Physical Attacks.

Preprint, submitted to IEEE TMM (CCF B 类期刊)

Hui Wei*, **Hanxun Yu***(共同一作), Zhixiang Wang, Shin'ichi Satoh, Hao Tang, Zheng Wang.

[Paper]

研究经历

加拿大麦吉尔大学 (McGill University) & MILA 研究所 研究型实习生 2022/06 – 2022/10

Mentor: Xujie Si 助理教授 [Certificate]

- 基于深度学习的反向传播机制, 使用语言模型和图神经网络自动检测和修复程序中的错误;
- 在包含 CS 302 (麦吉尔大学的一门课程) 的真实代码数据集上测试和比较所提出的方法。

韩国科学技术院(KAIST) 研究型实习生

2021/12 - 2022/02

Mentor: Chang D. Yoo 教授 [Certificate]

- 学习贝叶斯神经网络 (BNN) 和高斯过程 (GP), 并应用于基准数据集进行回归和分类;
- 研究贝叶斯神经网络 (BNN) 和高斯过程 (GP) 之间的相关性和对应关系。

比赛获奖

- 中国大学生计算机设计大赛一等奖 2022 年
- "互联网+"创新创业大赛湖北省银奖 2022年
- "挑战杯"大学生创业竞赛湖北省银奖 2022年
- 全国大学生物联网设计竞赛二等奖 2021年

相关技能

- 雅思: 6.5
- 编程语言: Python, C++, JAVA, HTML
- 操作系统: Linux, Windows