# 于瀚勋

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

#### 教育背景

硕士—浙江大学 专业:人工智能

2023/09 - 2026/03

GPA: 4.0 / 4.0

研究方向: 开放词汇二维/三维视觉物体定位 (Open-Vocabulary 2d/3d Visual Grounding)、二维/三维多模态大模型 (2d/3d Multi-modal LLM)

• 蒋震奖学金

本科—武汉大学 专业:计算机科学与技术

2019/09 - 2023/06

GPA: 3.8 / 4.0

研究方向:对抗/后门攻击 (Adversarial/Backdoor Attack)、可信人工智能 (Trustworthty AI)

- 国家奖学金(Top 0.2%) 2022 年
- 加拿大 Mitacs-CSC 国家公派留学研究型实习奖学金 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

#### \*: 共同第一作者

导师:朱建科 教授 机构: 浙江大学计算机软件研究所

• Inst3D-LMM: Instance-Aware 3D Scene Understanding with Multi-modal Instruction Tuning. *Preprint.* Hanxun Yu, Wentong Li, Song Wang, Junbo Chen, Jianke Zhu.

导师:王正 教授 机构: 武汉大学国家多媒体软件工程研究中心

• Moiré Backdoor Attack (MBA): A Novel Trigger for Pedestrian Detectors in the Physical World. ACM Multimedia 2023(CCF A 类会议)

Hui Wei\*, **Hanxun Yu\***, 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**\*, Zhixiang Wang, Shin'ichi Satoh, Hao Tang, Zheng Wang. Download [PDF]

## 实习经历

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

Mentor: Xujie Si 助理教授 [Certificate]

- Utilize language models and graph transformations to detect and fix bugs in programs automatically with learning-based feedback propagation.
- Test our frameworks on real-world datasets, which consist of homework Ocaml codes in CS 302 (one class of McGill University) to demonstrate their superiority compared with existing methods.

#### 韩国科学技术院 (KAIST) remote 研究型实习生

2021/12 - 2022/02

Mentor: Chang D. Yoo 教授 [Certificate]

- Study Bayesian Neural Network and Gaussian Process. Apply GP&BNN for regression and classification on Benchmark Dataset.
- Examine the correspondence between deep Bayesian Neural Network and Gaussian Process.

## 相关技能

• 雅思: 6.5

• 编程语言: Python, C++, JAVA, HTML

• 操作系统: Linux, Windows

#### 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