Hui Wei Curriculum Vitae

+86 189 3765 7603 | weihui0713@whu.edu.cn | GitHub | Homepage | Wuhan, China

A fourth-year CS Ph.D. student in AIM Lab at Wuhan University, under the supervision of Prof. Zheng Wang. My research interests lie in **AI safety**, **adversarial attack**, and **computer vision**, with a particular emphasis on constructing **trustworthy AI** systems.

Education

Wuhan University — Wuhan, China
Ph.D. in Computer Science and Technology. — *Sep. 2021 – Present*

Zhengzhou University — Zhengzhou, China
Master in Software Engineering. — *Sep. 2018 – July 2021*

Henan Agricultural University — Zhengzhou, China
B.S. in Software Engineering. — *Sep. 2014 – July 2018*

Research Experience

AIM Lab (AI&Multimedia Lab) — Wuhan, China
Ph.D. Candidate — *Sep 2021 – Present*

- Currently working with Prof. Zheng Wang on the field "Physical Adversarial Attack" in the AIM Lab (*Lab's Homepage*) at Wuhan University.
- Served as the leader of the Trustworthy AI group in the AIM Lab.

Selected Publications

⋆ Equal Contribution.

- **Physical Adversarial Attack Meets Computer Vision: A Decade Survey**
  Hui Wei, *Hao Tang, Xuemei Jia, Zhixiang Wang, Hanxun Yu, Zhubo Li, Shin'ichi Satoh, Luc Van Gool, Zheng Wang*
  IEEE Transactions on Pattern Analysis and Machine Intelligence (IEEE T-PAMI), 2024
- **Revisiting Adversarial Patches for Designing Camera-Agnostic Attacks against Person Detection**
  Hui Wei, *Zhixiang Wang, Kewei Zhang, Jiaqi Hou, Yuanwei Liu, Hao Tang, Zheng Wang*
  The Thirty-Eighth Annual Conference on Neural Information Processing Systems (NeurIPS), 2024
- **HOTCOLD Block: Fooling Thermal Infrared Detectors with a Novel Wearable Design**
  Hui Wei, *Zhixiang Wang, Xuemei Jia, Yinqiang Zheng, Hao Tang, Shin'ichi Satoh, Zheng Wang*
  The Association for the Advancement of Artificial Intelligence (AAAI), Oral, 2023
- **Moiré Backdoor Attack (MBA): A Novel Trigger for Pedestrian Detectors in the Physical World**
  Hui Wei, *Hanxun Yu, Kewei Zhang, Zhixiang Wang, Jianke Zhu, Zheng Wang*
  Proceedings of the 31nd ACM International Conference on Multimedia (ACM MM), 2023
- **ProjAttacker: A Configurable Physical Adversarial Attack for Face Recognition via Projector**
  Yuanwei Liu⋆, ***Hui Wei⋆***, *Chengyu Jia, Ruqi Xiao, Weijian Ruan, Xingxing Wei, Joey Tianyi Zhou, Zheng Wang*
  The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2025
- **Balancing Privacy and Performance: A Many-in-One Approach for Image Anonymization**
  Xuemei Jia, Jiawei Du, ***Hui Wei****, Ruinian Xue, Zheng Wang, Hongyuan Zhu, Jun Chen*
  The Association for the Advancement of Artificial Intelligence (AAAI), 2025
- **Federated Learning Vulnerabilities: Privacy Attacks with Denoising Diffusion Probabilistic Models**
  Hongyan Gu, Xinyi Zhang, Jiang Li, ***Hui Wei****, Baiqi Li, Xinli Huang*
  Proceedings of the ACM Web Conference (ACM WWW), 2024
- **Scale Matters: A Benchmark for Physical Adversarial Attacks on Person Detection**
  Hui Wei, *Yuanwei Liu, Xuemei Jia, Baraa Al-Hassani, Manhuen Zhang, Joey Tianyi Zhou, Zheng Wang*
  The IEEE/CVF Conference on Computer Vision and Pattern Recognition (ICCV), 2025, Under Review

- **Pose Does Matter: Keypoint-Guided Adversarial Patches for Effective Person Hiding Attacks**
  Kewei Zhang, **Hui Wei***, *Jiaqi Hou, Zheng Wang*
  The IEEE/CVF Conference on Computer Vision and Pattern Recognition (ICCV), 2025, Under Review

Selected Awards

- DiDi Scholarship, Wuhan University, 2024.
- China National Scholarship, Wuhan University, 2023.
- Second Prize of Academic Innovation of Wuhan University, 2023.
- First prize in the 18th China "Challenge Cup" Competition, 2023. [Leader]
- First prize in the "Huawei Cup" Postgraduate Network Security Innovation Competition, 2022. [Technical leader]

Selected Open-Source Projects

Survey for Physical Adversarial Attack

- A repository that is dedicated to tracking the latest advances in the field of Physical-Adversarial-Attack. The maintainer will continue to update it.
- GitHub: https://github.com/weihui1308/PAA. **83 Stars**.
- Accompanying paper published at IEEE T-PAMI 2024.

Human Privacy Protection under Intelligent Thermal Infrared Cameras

- We use anti-fever stickers/heating pads to form an effective solution to protect human privacy under intelligent thermal cameras.
- GitHub: https://github.com/weihui1308/HOTCOLDBlock. **31 Stars**.
- Accompanying paper published at AAAI 2023.