

Hui Wei

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

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

EDUCATION

Wuhan University

Ph.D. in Computer Science and Technology.

Zhengzhou University

Master in Software Engineering.

Henan Agricultural University

B.S. in Software Engineering; Rank: 9/61

Wuhan, China

Sep. 2021 – Present

Zhengzhou, China

Sep. 2018 – July 2021

Zhengzhou, China

Sep. 2014 – July 2018

RESEARCH EXPERIENCE

AIM Lab (AI&Multimedia Lab)

Ph.D. Candidate

Wuhan, China

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.

School of Computer and Artificial Intelligence

Master Degree Candidate

Zhengzhou, China

Sep 2018 – Jun 2021

- Worked in the Zhengzhou University with Prof. Mingliang Xu on the field about pedestrian trajectory prediction.

SELECTED PUBLICATIONS

- [1] **Hui Wei**, Hao Tang, Xuemei Jia, Zhixiang Wang, Hanxun Yu, Zhubo Li, Shin’ichi Satoh, Luc Van Gool, and Zheng Wang. Physical Adversarial Attack Meets Computer Vision: A Decade Survey[J]. T-PAMI 2024.
- [2] **Hui Wei**, Zhixiang Wang, Xuemei Jia, Yinqiang Zheng, Hao Tang, Shin’ichi Satoh, and Zheng Wang. HOTCOLD Block: Fooling Thermal Infrared Detectors with a Novel Wearable Design[C]. AAAI 2023 (Oral).
- [3] **Hui Wei**, Hanxun Yu, Kewei Zhang, Zhixiang Wang, Jianke Zhu, and Zheng Wang. Moiré Backdoor Attack (MBA): A Novel Trigger for Pedestrian Detectors in the Physical World[C]. ACM MM 2023.
- [4] Hongyan Gu, Xinyi Zhang, Jiang Li, **Hui Wei**, Baiqi Li, and Xinli Huang. Federated Learning Vulnerabilities: Privacy Attacks with Denoising Diffusion Probabilistic Models[C]. WWW 2024.

SELECTED AWARDS

- 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>. **59 Stars**.
- Accompanying paper published at T-PAMI 2024.

Human Privacy Protection under Intelligent Thermal 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>. **29 Stars**.
- Accompanying paper published at AAAI 2023.