



KEWEI ZHANG

(+86) 155-2770-6812 | 2022302111077@whu.edu.cn |  zkwsdsg |  github.com/xiwen1

I am a third-year CS undergraduate student in the AIM Lab at Wuhan University, under the supervision of Prof. Zheng Wang. My research interests lie in **Computer Vision**, **Trustworthy AI**, and **Large Vision-Language Models (LVLM)**. Additionally, I am passionate about AI-driven computer applications and have accumulated technical expertise in AI-related software development.

EDUCATION

Wuhan University

Bachelor of Software Engineering

Expected Graduation Date: June 2026

Senior | GPA: 3.91 / 4.0

SELECTED PUBLICATIONS

[1] Hui Wei*, Zhixiang Wang*, **Kewei Zhang* (Co-first Author)**, Jiaqi Hou, Yuanwei Liu, Hao Tang, and Zheng Wang. Revisiting Adversarial Patches for Designing Camera-Agnostic Attacks against Person Detection[C]. *NeurIPS 2024*.

[2] 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*.

SUBMITTED WORKS

[1] Pose Does Matter: Keypoint-Guided Adversarial Patches for Effective Person Hiding Attacks. Submitted to CVPR 2025. Investigating new approach to attack person detector, other than patch-based methods and texture-based methods, in order to achieve a total evasion facing real-world cameras.

[2] Adversarial Watermarking under Diverse Manipulations: Benchmarking and Beyond. Submitted to TIP. Focused on exploring defense method against watermark remove networks.

RESEARCH EXPERIENCE

AIM Lab (AI&Multimedia Lab)

Intern under the supervision of Professor [Zheng Wang](#)

Wuhan, China

March 2023 – Present

- Currently working with [Hui Wei](#) on the field “Adversarial Attack” in the AIM Lab ([Lab’s Homepage](#)) at [Wuhan University](#).
- Also Conducting research on **Controllable Diffusion models** and **Model Diagnosis** with [Zhixiang Wang](#).

SELECTED AWARDS

Lei Jun Computer Scholarship (20 of 1600) | Wuhan University

November 2024

National Scholarship (2 of 522) | Ministry of Education

October 2023

Honorable Mention | COMAP’s 2024 MCM/ICM.

April 2024

National First Award | The 18th China “Challenge Cup” Competition.

September 2023

SELECTED PERSONAL PROJECTS

Enhanced MultiDiffusion (Academic project)

January 2024

- * Inject ControlNet into [MultiDiffusion](#)’s pipeline, implemented with **Pytorch**.
- * Enable user to generate images with both region and sketch control, and to write prompts for every mask, achieving extremely precise control for SD models.

Project Manager: Just Dev (Web Application)

June 2024

- * A novel project manager that establishes a binding between project requirements, tasks, GitHub PR. It introduces a “task dependency graph” mechanism, integrated with **LLM Agent**.
- * Backend implemented in **Rust** with *Axum framework* and y-CRDT. Frontend implemented in Typescript with *Next.js*.

Bias Discovery: Model Diagnosis with LLM (Academic project)

November 2024

- * Automatically discover bias in Glass Segmentation Model by a framework of hypothesis prompt and verify cycle.
- * Implemented with Langchain and GPT-4o.