Tairan Chen

Beijing, China | +86-17614416037 | terrencechentr@gmail.com
Homepage: https://thechentr.github.io/

EDUCATION

Jilin University — ***Jilin, China***
Bachelor in Computer Science and Technology — *Sept. 2020 - Jun. 2024*
Overall GPA : 86.01 / 100

Tsinghua University — ***Beijing, China***
Research Assistant — *Dec. 2023 - Present*
Research Focus: Computer Vision & Adversarial Machine Learning

Related Coursework: Data Structure, Computer Organization, Operating Systems, Computer Networks, Compiler Principle and Implementation, Calculus, Linear Algebra, Probability and Statistics

RESEARCH EXPERIENCE

Robust Object Detection Algorithm Based on Active Perception — Tsinghua University

Research Assistant — *Apr. 2024 - Present*

Advisor: Associate Prof. **Hang Su** in the Department of Computer Science and Technology at Tsinghua University

Background: Despite the substantial advancements of deep learning in computer vision, models remain highly vulnerable to adversarial attacks, particularly in dynamic 3D environments. Current defense strategies often fall short in such settings. This project introduces a novel object detection method grounded in active perception, integrating a cyclical process between perception and tactical strategy to better utilize environmental information when countering adversarial examples in real-world 3D scenarios.

- Combined YOLOv5 and Transformer models to develop an active perception-based object detection system, achieving over **60% mAP50-95** in defending against adversarial patch attacks.
- Implemented a **differentiable rendering environment based on EG3D**, supporting consistent multi-view image generation.
- Compared with multiple defense methods such as JPEG, LGS, SAC, and PZ, demonstrating the **superiority of our method**.

Achievement: The source code is freely available. For more details, please refer to the following link: https://github.com/thechentr/EAD-YOLOv5

Jailbreak attack on Visual Language Model based on FigStep — Tsinghua University

Research Assistant — *Jun. 2024 - Jul. 2024*

Advisor: Associate Prof. **Hang Su** in the Department of Computer Science and Technology at Tsinghua University

Background: While Visual Language Models (VLMs) have demonstrated impressive capabilities in image recognition and natural language processing, they are also subject to significant security risks and potential misuse. Open-source VLMs often lack rigorous security evaluations, making them vulnerable to jailbreak attacks, where carefully crafted inputs can trigger inappropriate model behavior. This research focuses on improving the success rate of such jailbreak attacks, uncovering critical security flaws in multimodal VLMs.

- Developed an **adversarial sample generation method** for VLMs based on FigStep.
- Increased the attack success rate (ASR) by **26.5%** through image optimization and prompt tuning.
- Combined the COCO dataset with the **Stable Diffusion model** to enhance the stealth and diversity of the attacks.

Achievement: Our team secured **the Second Place** in the Red Teaming Multimodal Large Language Model Security Challenge hosted by CCF.

Automated C++ Code Generator for Syntax Analysis — Jilin University

Undergraduate Researcher — *Mar. 2023 - May. 2023*

Advisor: Associate Prof. **Huaxiao Liu** in the Department of Computer Science and Technology at Jilin University

Background: Syntax analysis plays a vital role in compiler construction, where parsers must accurately interpret the grammar of programming languages. However, building efficient and scalable parsers is a complex, time-intensive task that requires deep knowledge of grammar rules and coding strategies. This project aims to simplify and accelerate the parser development process by creating an automated C++ code generator for syntax analysis, capable of converting grammar productions into executable code.

- Developed an **automated C++ code generator for syntax analysis**, significantly reducing manual coding efforts.
- Implemented a feature for generating **recursive descent parsing** and **LL(1) parsing** code, enhancing code reusability and execution efficiency.
- Developed a component for automatic prediction set calculation, facilitating easy integration with various language generation rules.

Achievement: The source code is freely available. For more details, please refer to the following link: https://github.com/thechentr/SNL-compiler

Hex Game Algorithm Based on Queenbee Evaluation — Jilin University

Undergraduate Researcher — *Apr. 2022 - Jun. 2002*

Advisor: Associate Prof. **Yungang Zhu** in the Department of Computer Science and Technology at Jilin University

Background: Hex is a classic strategy game known for its simple rules and high complexity, making it an ideal platform for research in artificial intelligence and game theory. The project aims to design traditional game algorithms to achieve a level that surpasses human capability.

- Developed a **Hex game algorithm based on the Queenbee evaluation**, significantly enhancing the decision-making capabilities of computer players.
- Combined game tree, **minimax algorithm**, and $\alpha - \beta$ **pruning** to facilitate efficient decision-making and increase win rates.

AWARDS, SCHOLARSHIPS & LEADERSHIP

➢ Outstanding Undergraduate Graduate (**Top 5%**)	*2024*
➢ Academic Scholarship (**Top 10%**)	*2021, 2022, 2023*
➢ Outstanding Student Leader (**Top 3%**)	*2021, 2022, 2023*
➢ Cultural and Sports Activities Scholarship (**Top 10%**)	*2022, 2024*
➢ Social Work Scholarship (**Top 10%**)	*2023*
➢ **Top 8.38%** of CCF Certified Software Professional in C++ in China	*2021*
➢ **President** of the Student Union, School of Computer Science and Technology	*Sept. 2022–Sept. 2023*
➢ **President** of the JLU Guitar Association	*Aug. 2022–Aug. 2023*
➢ **Monitor** of Class 31 of 2020, School of Computer Science and Technology	*Sept. 2020–Jul. 2024*

TECHNICAL PROFICIENCIES

Programming Languages: C/C++, Python, R, Java, etc.

Deep learning models: YOLO, EG3D, Stable Diffusion, GPT-3, etc.

Other Tools: Git, Docker, Latex etc.