

Tairan Chen

Beijing, China | +86-17614416037 | terrencechentr@gmail.com

Homepage: <https://thechentr.github.io/>

EDUCATION

Jilin University

Bachelor in Computer Science and Technology

Jilin, China

Sept. 2020 - Jun. 2024

Overall GPA : 86.01 / 100

Related Coursework: C Programming (95), Compiler Principles (94), Computer Organization (90), Digital Logic Circuits (90), Microcomputer Systems (89), Discrete Mathematics (89), Data Structures (87), Operating System(86)

Tsinghua University

Research Assistant, [Tsinghua SAIL Group](#)

Beijing, China

Dec. 2023 - Present

Team leaders: [Prof. Jun Zhu](#) and [Associate Prof. Hang Su](#)

Research Focus: Computer Vision, Natural Language Processing , Adversarial Machine Learning

RESEARCH EXPERIENCE

Active Perception Defense Against 3D Adversarial Patches

Tsinghua University

Research Assistant

Apr. 2024 - Present

Advisor: Associate Prof. [Hang Su](#) in the Department of Computer Science and Technology at Tsinghua University

Background: Visual Models in critical applications like identity verification and autonomous driving are highly vulnerable to adversarial attacks in 3D environments. Traditional passive defenses struggle to adapt to dynamic conditions. We propose a active defense framework that enhances robustness through adaptive exploration and interaction in 3D adversarial settings.

- Implemented a **differentiable rendering environment based on EG3D** to support consistent multi-view image generation, enabling more accurate 3D representation.
- Developed an active perception defense system that integrates an **RL-based policy module** and a **perception module** in a feedback loop, enhancing environmental exploration and robustness.
- Achieved up to a **95% reduction** in attack success rate (ASR) against various adversarial attacks, surpassing passive defenses and demonstrating effectiveness in real-world settings.

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

Red Teaming Multimodal Large Language Model Security Challenge

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: Visual Language Models (VLMs) are vulnerable to jailbreak attacks caused by crafted inputs. Existing attack methods lack generalization and diversity. We proposed an adversarial sample generation method that significantly improves success rates in black-box scenarios.

- Developed an **adversarial samples generation method** initiated from the visual modality to enhance attack effectiveness on VLMs.
- Integrated the **COCO dataset** with **Stable Diffusion** to improve attack stealth and diversity.
- Achieved a **26.5% increase** in attack success rate (ASR) through optimized image generation and prompt tuning.

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

PROJECT EXPERIENCE

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 is crucial in compiler construction, but building efficient parsers is complex and time-consuming. To address this, we developed an automated C++ code generator for syntax analysis that converts grammar rules into highly optimized, executable code.

- Built an **automated C++ code generator for syntax analysis**, greatly reducing manual coding effort.
- Added support for **recursive descent parsing** and **LL(1) parsing**, improving code reusability and efficiency.
- Developed an **automatic prediction set calculation module**, easing integration with various grammar 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 game with simple rules but a vast and complex search space, where traditional evaluation algorithms often fail. This project aims to propose a new, accurate, and efficient evaluation algorithm for Hex, improving long-term strategic decision-making.

- 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
➤ Top 8.38% of CCF Certified Software Professional in C++ in China	2021
➤ Provincial Second Prize in the National Undergraduate Mathematical Contest in Modeling	2022
➤ Outstanding Student Leader (Top 3%)	2021, 2022, 2023
➤ Cultural and Sports Activities Scholarship (Top 10%)	2022, 2024
➤ Social Work Scholarship (Top 10%)	2023
➤ President of the Student Union, School of Computer Science and Technology	Sept. 2022–Sept. 2023
➤ Monitor of Class 31 of 2020, School of Computer Science and Technology	Sept. 2020–Jul. 2024

TECHNICAL PROFICIENCIES

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

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

Other Tools: Git, Docker, Latex, etc.