

# Tairan Chen

Beijing, China | +86-17614416037 | [terrencechentr@gmail.com](mailto: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

### 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:** Object detection models are vulnerable to adversarial patch attacks, and existing defenses based on static images perform poorly in dynamic environments. We propose an active exploration-based method that leverages environmental information to enhance model robustness.

- Implemented a **differentiable rendering environment based on EG3D** to support consistent multi-view image generation, enabling more accurate 3D representation.
- Built an active detection system with **YOLOv5-based perception** and **Transformer-based policy** modules, operating in a loop for enhanced environmental exploration and robustness.
- Achieved over **60% mAP50-95** against adversarial patch attacks, outperforming methods like 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>

### 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 image generation method** based on FigStep to enhance attack effectiveness for VLMs.
- Integrated the **COCO dataset** with **Stable Diffusion** to improve attack stealth and diversity.
- Increased the **attack success rate (ASR)** by **26.5%** through image optimization 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. 2022

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 ( <b>Top 5%</b> )                                          | 2024                  |
| ➤ Academic Scholarship ( <b>Top 10%</b> )                                                       | 2021, 2022, 2023      |
| ➤ <b>Top 8.38%</b> of CCF Certified Software Professional in C++ in China                       | 2021                  |
| ➤ Provincial <b>Second Prize</b> in the National Undergraduate Mathematical Contest in Modeling | 2022                  |
| ➤ Outstanding Student Leader ( <b>Top 3%</b> )                                                  | 2021, 2022, 2023      |
| ➤ Cultural and Sports Activities Scholarship ( <b>Top 10%</b> )                                 | 2022, 2024            |
| ➤ Social Work Scholarship ( <b>Top 10%</b> )                                                    | 2023                  |
| ➤ <b>President</b> of the Student Union, School of Computer Science and Technology              | Sept. 2022–Sept. 2023 |
| ➤ <b>Monitor</b> 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.