Yilun (Alan) Zhou

yzhou851@gatech.edu | https://ylz1992.github.io/personalweb/

Education

Georgia Institute of Technology Atlanta, GA
M.S. in Computer Science, GPA: 3.8/4.0 *Expected Dec 2024*
Relevant Coursework: Advanced Machine Learning, Deep Generative Models, Vision-Language Models, Graduate Algorithms, Computer Vision, Deep Learning, Computer Networks, Software Development Processes

University of Florida Gainesville, FL
M.S. in Geographic Information Systems *Jan 2017*

Beijing Jiaotong University Beijing, China

Technical Skills

Languages: Python, Java, JavaScript, C, C, PHP
Frameworks/Tools: Huggingface, PyTorch, scikit-learn, MongoDB, React, Node.js, Unity, Docker, Git
Certificates: AWS Solutions Architect Associate, Data Science (Renmin University of China)

Research and Professional Experience

Research Assistant Aug 2024 – Present
EIC Lab, Georgia Tech *Advisors: Prof. Celine Lin, Dr. Zhongzhi Yu*

- Investigating the role of attention mechanisms in adversarial attacks on large language models (LLMs), focusing on LLaMA2 and Vicuna models.
- Developing generalized adversarial attacks, including token-based and string-based methods to bypass model defenses.

Unity Developer Intern - Remote Jun 2024 – Aug 2024
Plutonic *Atlanta, GA*

- Contributed to the development of a teletherapy platform by implementing multiplayer features through AWS GameLift, Photon Fusion Kit, and S3.
- Integrated OpenAI's APIs to enhance chatbot capabilities for improved user interaction within the platform.

Research Assistant Jan 2024 – Jun 2024
TReNDS Center, Georgia Tech *Advisor: Dr. Sergey Plis*

- Developed deep learning models for fMRI brain image analysis, focusing on classification and object detection tasks.
- Implemented models such as ResNet50 and U-Net for brain image classification and diagnostic tasks.

R&D Engineer 2017 – 2022
China Architecture Design & Research Group *Beijing, China*

- Led a team of engineers in developing digital simulations and parametric models for major infrastructure projects, including over 10 buildings and the internationally recognized No.17 Bobsleigh Track. Portfolio Highlights
- Contributed to 10+ construction projects and earned 8 structural design awards, including 2 national awards. Authored 8 research articles and co-authored 1 book on structural engineering.

Research Assistant Aug 2015 – Aug 2016
Geo Lab, University of Florida *Advisor: Prof. Michael C. McVay*

- Researched soil behavior under saturated and unsaturated conditions using GIS analysis techniques.

Projects

Conditioned Denoising for Adversarial Defense Aug 2024 – Present
Visual Language Model Special Research *Advisor: Prof. Zsolt Kira*

- Developing techniques for denoising adversarial perturbations in images prior to their input into vision-language models (VLMs).
- Exploring the use of multimodal information for enhancing robustness against adversarial attacks (models: Flamingo, LLaVA).

Evaluating the Robustness of T2I Diffusion Models Against Attacks — Aug 2024 – Present

Advanced Machine Learning Research — *Advisor: Prof. Bo Dai*

- Developing novel distribution-based adversarial objectives to mislead text-to-image (T2I) diffusion models in a black-box setting.

Reinforcement Learning for Stock Market Trading Strategies — Jan 2023 – Jun 2023

ML-based Projects — *Self-directed*

- Developed a reinforcement learning model to optimize trading strategies for the Turkish stock market.
- Designed a supervised learning model for housing price prediction in Georgia, USA. Project Link

Job Offer Comparison Android App — Aug 2023 – Dec 2023

Back-end Development — *Georgia Tech OMSCS Program*

- Developed an Android application to compare job offers based on compensation and benefits packages. GitHub Link

Command Line Utility: Txter — Aug 2023 – Dec 2023

CLI Development — *Self-directed*

- Created a Java-based command-line utility for advanced text processing, including JUnit testing and GitHub version control. GitHub Link

Computer Networks Project — Aug 2023 – Dec 2023

Computer Networks Course Project — *Georgia Tech*

- Configured IP, OSPF, and BGP for routers and hosts within a VPN system to ensure secure communication and robust routing between autonomous systems.