Tingxi Li

800 W Campbell Road, Richardson, TX 75080

☎ (213)-795-5275 ✉ tingxi.li@utdallas.edu linkedin homepage

Education

University of Texas at Dallas **Sep. 2024 – Present**
Doctor of Philosophy in Computer Science *Dallas, TX*

Dalian University of Technology **Sep. 2019 – May 2024**
Bachelor of Science in Chemistry *Dalian, China*

Technical University of Munich **Apr. 2022 – Oct. 2022**
Visiting Student: Computer Science *Munich, Germany*

Academic Experience

Adversarial Attack on a Robotic Arm **Jan. 2024 – Present**
UT Dallas | Supervisor: Wei Yang *Dallas, TX*

- Replaced the non-differentiable heightmap renderer with a differentiable one, enabling gradient computation through the entire model. This enhancement facilitates direct optimization of the model using backpropagation algorithms.
- For the object grasping task investigation, experiments conducted within the Bulletarm robotic framework demonstrated that the effect of a given action on the environment is deterministic. Moreover, it was observed that the boundaries between success and failure within the action space are non-robust.

Survey of Efficiency Robustness of Dynamic Deep Learning Systems **Jun. 2024 – Present**
UT Dallas | Supervisor: Wei Yang *Dallas, TX*

- Wrote a section of the survey paper, introducing and categorizing existing efficiency attacks on dynamic deep learning systems, providing a structured analysis to enhance understanding of potential vulnerabilities.

Efficiency Attack on Multi-level Applications **Jun. 2024 – Present**
UT Dallas | Supervisor: Wei Yang *Dallas, TX*

- Applied efficiency attacks on multi-level applications, evaluating their impact on downstream tasks by measuring energy consumption and time delays.
- Proposed and developed defense mechanisms to detect and mitigate these attacks, enhancing system resilience.

Industrial Experience

Sophgo **Jul. 2024 – Sept. 2024**
Intern *Shenzhen, China*

- Developed and implemented API code in C++ for models deployed on RISC-V processors. Authored comprehensive documentation to support efficient deployment and usage.
- Fine-tuned models on private datasets, identified failure cases, and implemented data augmentation strategies.

Projects

Amazon Trusted AI Challenge **Nov. 2024 – Present**
Team Member *Seattle, WA*

- Selected as one of the red teams. Jailbreaking black-box code models to generate malicious code.

Publication

SoK: Efficiency Robustness of Dynamic Deep Learning Systems **Under Submission**
second author

Efficiency Robustness Towards Multi-level Application **Under Submission**
first-author

Adversarial Attack Towards A Robotic Arm System **Under Submission**
first-author

Miscellaneous

Research Interest: AI Security; Software Engineering; AI for Science
Tech Stack: Python; C; C++; Java; PyTorch; LaTex; SQL
Languages: English / Mandarin / Cantonese