Zexin Li

Email: zli536@ucr.edu
Portfolio: zexinli.com
Mobile: +1-945-217-4139
Github: github.com/zexinli0w0

Education

- **University of California, Riverside** — Riverside, California, USA
  Ph.D. student of Electronic Engineering GPA: 4.00/4.00 — *Aug 2022 - Now*
- **University of Texas at Dallas** — Richardson, Texas, USA
  Ph.D. student of Computer Science; GPA: 3.83/4.00 — *Aug 2020 - Aug 2022*
- **Southern University of Science and Technology** — Shenzhen, China
  Bachelor of Computer Science and Technology; GPA: 3.57/4.00 — *July 2016 - July 2020*

Industrial Experience

- **Tencent** — Shanghai, China
  Research Internship — *May 2021 - Dec 2021*
  - **Responsibility**: Worked at Tencent Youtu Lab which focuses on advanced research on face recognition robustness.
  - **Research**: Research on transferable adversarial attack on face recognition systems.
- **Kwai** — Shenzhen, China
  Research & Development Internship — *Nov 2019 - Jul 2020*
  - **Responsibility**: Worked at Peer Content Delivery Network (PCDN) team which aims to develop and maintain PCDN system, involving technical stack: C++, C and Docker.
  - **Research**: Research on Peer Content Delivery Network (PCDN) optimization, including system-level optimization and application-level optimization.
  - **Engineering**: Updated the internal web protocol framework in PCDN backend to boost overall transmission speed of videos and decrease the retransmission ratio. Wrote tests for the backend service and deploy grey testing for over 10,000 third-party edge devices.

Publications

- **MIMONet: Multi-Input Multi-Output On-Device Deep Learning.**: Zexin Li, Xiaoxi He, Yufei Li, Shahab Nikkhoo, Wei Yang, Lothar Thiele, Cong Liu (Submitted to IROS'2023)
- **PIMbot: Policy and Incentive Manipulation for Multi-Robot Reinforcement Learning in Social Dilemmas.**: Shahab Nikkhoo, Zexin Li, Aritra Samanta, Yufei Li, Cong Liu (Submitted to IROS'2023)
- **White-Box Multi-Objective Adversarial Attack on Dialogue Generation.**: Yufei Li, Zexin Li, Yingfan Gao and Cong Liu (ACL'2023)
- **Dynamic Transformers Provide a False Sense of Efficiency.**: Yiming Chen, Simin Chen, Zexin Li, Wei Yang, Cong Liu, Robby Tan and Haizhou Li (ACL'2023)
- **Sibling-Attack: Rethinking Transferable Adversarial Attacks against Face Recognition.**: Zexin Li*, Bangjie Yin*, Taiping Yao, Junfeng Guo, Shouhong Ding, Simin Chen, Cong Liu (CVPR'2023) [PDF]
- **Efficient algorithms for task mapping on heterogeneous CPU/GPU platforms for fast completion time.**: Zexin Li, Yuqun Zhang, Ao Ding, Husheng Zhou, Cong Liu (JSA'2021) [PDF]

Projects

- **Artificial Intelligence**: The core objective of this research is to enhance attacking transferability on face recognition systems. This approach can significantly improve the attacking success rate on several publicly available datasets and fool several state-of-the-art commercial platforms corresponding to face recognition models. This project is partially supported by Tencent Rhino-BirdElite Talent Training Program. (CVPR'2023)
- **Real-time Systems, Software Engineering**: The main focus of this study consists of a performance optimization scheme for heterogeneous computing systems. The core objective is to optimize the performance of heterogeneous computing systems by optimizing the task scheduling policy between different computing devices. Also, a fine-grain mapping framework is designed for exploring a set of critical factors is needed for heterogeneous embedded systems. This project was awarded Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation in 2019. (JSA'21)
- **Artificial Intelligence, Software Engineering, Security**: The core objective of this study is to detect flaws in the deep neural network model-based autonomous driving system by constructing an adversarial attack sample based on the deep neural network model to cause targeted interference to the autonomous driving system. In addition, the research also involves transferring the approach from numerical simulations to real-world scenarios for empirical learning. This project was awarded Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation in 2018.

Academic Supervision and Mentorship

- **Ao Ding**: SUSTech CSE, 2019–2020 (Co-author; Current master student at SUSTech)
- **Zelin Wang**: SUSTech CSE, 2019–2020 (Project; Current master student at USTC)
- **Shuqing Li**: SUSTech CSE, 2019–2020 (Project; Current Ph.D. student at CUHK)
- **Aritra Samanta**: UCR CS, 2022–Current (Co-author[in submission]; Current master student at UCR)
- **Yifan Yu**: UCR CE, 2022–Current (Project; Current master student at UCR)
- **Tao Ren**: UCR EE, 2023–Current (Co-author[in submission]; Incoming Ph.D. student at UCR)

Honors and Awards

- Dean's Distinguished Fellowship, University of California, Riverside - May, 2022
- Tencent Rhino-BirdElite Talent Training Program, Tencent - May, 2021
- Outstanding Student Scholarship, Southern University of Science and Technology - Nov, 2019
- Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation - Mar, 2019
- Special Funds for the Cultivation of Guangdong College Students' Scientific and Technological Innovation - Mar, 2018

Skills

- **Programming Languages:**: C, C++, Python, Rust.
- **Machine Learning Frameworks:**: Pytorch, Tensorflow, Caffe.
- **Robotic Frameworks:**: ROS, ROS 2, Autoware.
- **Embedded Platforms:**: NVIDIA Jetson Toolkit, Raspberry Pi, Google Coral Edge TPU.
- **Adversarial Machine Learning:**: Transferable attack, Energy attack.

Reference

- **Cong Liu**: Associate Professor of Electrical and Computer Engineering, University of California, Riverside (UCR).
- **Yuqun Zhang**: Assistant Professor of Computer Science, Southern University of Science and Technology (SUSTech).
- **Wei Yang**: Associate Professor of Computer Science, University of Texas at Dallas (UTD).
- **Shouhong Ding**: Senior Researcher of Youtu Lab, Tencent.