Xuyang Zhong

xuyang.zhong@my.cityu.edu.hk | +86 19559740729

Education

2023.01 - Present **City University of Hong Kong**
Ph.D. Student in Computer Science, Supervisor: Chen Liu
Research Area: Trustworthy AI, Optimization in Deep Learning

2020.11 - 2022.11 **Technical University of Munich**
M.Sc. in Electrical Engineering and Information Technology

2016.09 - 2020.07 **Beijing Institute of Technology**
B.Eng. in Automation

Internship

Tencent (Shenzhen) 2025.06 - Present

Research Intern (**Tencent Project Up**)
Optimization on LLMs

Siemens Factory Automation Engineering (Beijing) 2019.05 - 2019.11

Data Analysis Intern (Excellent Intern Certificate)
Face Recognition API Development, Products Quality Prediction

Publications

Conference and Journal

1. **Xuyang Zhong**, Chen Liu. "Sparse-PGD: A Unified Framework for Sparse Adversarial Perturbation Generation". *IEEE Transactions on Pattern Analysis and Machine Intelligence (**TPAMI**), 2025*
2. **Xuyang Zhong**, Haochen Luo, Chen Liu. "DualOptim: Enhancing Efficacy and Stability in Machine Unlearning with Dual Optimizers". *Annual Conference on Neural Information Processing Systems (**NeurIPS**), 2025*
3. **Xuyang Zhong**, Yixiao Huang, Chen Liu. "Understanding and Improving Fast Adversarial Training against l_0 Bounded Perturbations". *Annual Conference on Neural Information Processing Systems (**NeurIPS**), 2025*
4. **Xuyang Zhong**, Chen Liu. "Towards Mitigating Architecture Overfitting on Distilled Datasets". *IEEE Transactions on Neural Networks and Learning Systems (**TNNLS**), 2025*
5. Youssef Mansour*, **Xuyang Zhong***, Serdar Caglar, Reinhard Heckel. "TTT-MIM: Test-Time Training with Masked Image Modeling for Denoising Distribution Shifts". *European Conference on Computer Vision (**ECCV**), 2024*
6. **Xuyang Zhong**, Yixiao Huang, Chen Liu. "Towards Efficient Training and Evaluation of Robust Models against l_0 Bounded Adversarial Perturbations". *International Conference on Machine Learning (**ICML**), 2024*
7. Yuyang You*, **Xuyang Zhong***, Guozheng Liu, Zhihong Yang. "Automatic Sleep Stage Classification: A Light and Efficient Deep Neural Network Model based on Time, Frequency and Fractional Fourier Transform Domain Features". ***Artificial Intelligence in Medicine**, 2022*

*** indicates equal contribution**

Award

Outstanding Student Certificate 2025
Tencent Rhino-Bird Open Source Talent Development Program
Research Tuition Scholarship 2025
City University of Hong Kong
Outstanding Academic Performance Award 2024
City University of Hong Kong
Conference Grant 2024
City University of Hong Kong

Academic Service

Reviewer of ICLR, NeurIPS

Skills

Languages: Chinese (Native speaker), English (Fluent), German (Daily)