

BINGYIN ZHAO

(+65)944-746-31 bingyiz@nus.edu.sg [Homepage](#)

EDUCATION

CLEMSON UNIVERSITY

Ph.D. in ELECTRICAL AND COMPUTER ENGINEERING

Clemson, SC, USA

GPA: 4.0

ROCHESTER INSTITUTE OF TECHNOLOGY

Master of Science in ELECTRICAL ENGINEERING

Rochester, NY, USA

EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Bachelor of Science in ELECTRICAL ENGINEERING

Shanghai, China

SKILLS

Knowledge Deep learning, Computer Vision, Adversarial/Robust machine learning, Model compression
Language & Tool Python, Pytorch, TensorFlow/Keras, Numpy, Scikit-learn, Pandas, Vim, Docker, Git, Shell, \LaTeX

WORKING EXPERIENCE

Research Fellow

Oct. 2024 – Present

National University of Singapore, Singapore

- Conduct research on univariate/multivariate and relational time-series tabular data generation.
- Supervise Ph.D. students for research on the privacy and security of generative models.

Research Scientist

Oct. 2024 – Present

Betterdata, Singapore

- Work on research and product development of time series tabular data generation.
- Design and develop a general AI model for all-kinds tabular data generation (e.g., single table, relational table).

Deep Learning Software and Research Intern (AV Perception)

May. 2022 – Feb. 2023

NVIDIA, Santa Clara, CA, USA

- Conduct research on zero-shot robustness of ViT-based neural networks against natural corruptions such as weather conditions and natural adversarial examples.
- Received a full-time offer as a Senior Systems Software Engineer but could not return to the U.S. due to an unexpected visa issue.

SELECTED RESEARCH AND PROJECTS

Design of Robust Vision Transformers (Pytorch/TensorFlow/Python)

May. 2022 – Mar. 2023

- Proposed a novel training paradigm that jointly incorporates self-emerging token labels and image-level labels and significantly enhanced clean accuracy and zero-shot robustness of Fully Attentional Networks on image classification and segmentation tasks.
- Achieved SOTA zero-shot robustness on ImageNet-A, ImageNet-R and Cityscape-C with model size of 77.3M.
- Experience with distributed training and parameter tuning of neural networks on GPU clustering such as NGC and Maglev.

Robust DNNs against Poisoning Attacks (Pytorch/TensorFlow/Python)

Sep. 2018 – May. 2022

- Devised a general and scalable defensive framework against clean-label backdoor attacks towards image classification tasks. Achieved up to 100% detection rate and reduced attack success rate from $\sim 90\%$ to 0% against three widespread attacks.
- Proposed a novel defense against poisoning attacks using gradual magnitude pruning. Analyzed the correlation between pruning and model robustness and improved the post-attack accuracy from 5% to over 50%.

Clean-Label Poisoning Attacks towards DNNs (Keras/Pytorch/Python)

Jun. 2020 – May. 2021

- Designed a generative adversarial net (GAN)-based framework for clean-label poisoned data generation that degrades the overall model accuracy.
- Built the framework using BigGAN architecture and devised a triplet loss function to improve the effectiveness and fidelity of poisoned data.
- Achieved 18% accuracy drop with only 20% poisoning ratio and 55% accuracy drop with full poisoning on modern neural networks such as ResNet, VGG and Inception-V3.

PUBLICATIONS

Y. Han*, B. Zhao*, R. Chu, F. Luo, B. Sikdar and Y. Lao, UIBDiffusion: Universal Imperceptible Backdoor Attack for Diffusion Models

2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (*Acceptance Rate = 22%*)

B. Zhao, Z. Yu, S. Lan, Y. Cheng, A. Anandkumar, Y. Lao and J. Alvarez, Fully Attentional Networks with Self-emerging Token Labeling

2023 IEEE/CVF International Conference on Computer Vision (ICCV)

B. Zhao and Y. Lao, CLPA: Clean-Label Poisoning Availability Attacks Using Generative Adversarial Nets

Thirty-Sixth AAAI Conference on Artificial Intelligence (AAAI) (*Acceptance Rate = 15%*)

B. Zhao, L. Qiu and Y. Lao, Data-Driven Feature Selection Framework for Approximate Circuit Design

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)

A. Wang, B. Zhao and Y. Lao, Neural Network Fault Attacks Detection Using Gradient-Based Test Vector Generation

60th ACM/IEEE Design Automation Conference (DAC)

B. Zhao and Y. Lao, Towards Class-Oriented Poisoning Attacks Against Neural Networks

2022 IEEE Winter Conference on Applications of Computer Vision (WACV)

B. Zhao and Y. Lao, Resilience of Pruned Neural Network Against Poisoning Attack

2018 13th International Conference on Malicious and Unwanted Software (MALWARE)