BINGYIN ZHAO

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

ABOUT ME

▷ AI researcher and engineer with first-author papers in CVPR, ICCV, AAAI
▷ Proficient coding in Python and PyTorch
▷ Experience designing and training neural networks at fast-paced teams
▷ Research interests in Generative AI, Computer Vision and Trustworthy AI

EXPERIENCE

National University of Singapore *Singapore*
Research Fellow Oct. 2024 – Now

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

Betterdata *Singapore*
Research Scientist Oct. 2024 – Now

- 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).
- Design and develop tabular foundation models.

NVIDIA *Santa Clara, CA, USA*
Deep Learning Software and Research Intern (AV Perception) May. 2022 – Feb. 2023

- Conduct research on zero-shot robustness of ViT-based neural networks against natural corruptions such as weather conditions and natural adversarial examples.
- Published one ICCV paper and filed one U.S patent.
- **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.**

EDUCATION

CLEMSON UNIVERSITY *Clemson, SC, USA*
Ph.D. in Electrical and Computer Engineering GPA: 4.0

ROCHESTER INSTITUTE OF TECHNOLOGY *Rochester, NY, USA*
Master of Science in Electrical Engineering

EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY *Shanghai, China*
Bachelor of Science in Electrical Engineering

SELECTED 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)

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