BINGYIN ZHAO

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

ABOUT ME

▷ 7+ years AI researcher and engineer with first-author papers in CVPR, ICCV, AAAI
▷ Proficient coding in Python and PyTorch, familiar with Numpy, Scikit-learn, Pandas, Docker, Git, LaTeX
▷ Experience designing and training neural networks in fast-paced teams
▷ Solid knowledge in Generative AI, Trustworthy AI, Computer Vision and Deep Learning
▷ Research interests in AIGC, AI for Science, Foundation Models, and AI safety

EXPERIENCE

National University of Singapore *Singapore*
Research Fellow Oct. 2024 – Now
- Research on AIGC, LLM, diffusion models and fractal generative 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, forecasting and enhancement.
- Delivered Betterdata's first-generation time series tabular generative model.
- Design and develop the conditional tabular generative model using the auto-regressive transformer.

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.**

Clemson University *Clemson, SC, USA*
Researcher Jan. 2018 – May. 2024
- Research on trustworthy AI, particularly poisoning attacks, backdoor attacks and corresponding countermeasures.
- Published papers at AAAI, WACV, TCAD, DAC, etc.

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) (Selected as highlight = 3%)

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)