

BINGYIN ZHAO

(+65)944-746-31 bingyiz89@gmail.com [Homepage](#) [Google Scholar](#)

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

Pixocial

Applied Scientist

[Singapore](#)

Jun. 2025 – Now

- Product development and research on image/video generation/editing.

National University of Singapore

Research Fellow

[Singapore](#)

Oct. 2024 – Jun. 2025

- Research on AIGC, LLM, diffusion models and fractal generative models.
- Supervise Ph.D. students for research on the privacy and security of generative models.
- Design and implement the first generation conditional time-series tabular generative model for Betterdata.

NVIDIA

Deep Learning Software and Research Intern (AV Perception)

[Santa Clara, CA, USA](#)

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 an ICCV paper and filed one US patent.
- Received a full-time offer as a Senior Systems Software Engineer but could not return to the US due to an unexpected visa issue.

Clemson University

Research Assistant

[Clemson, SC, USA](#)

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

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](#)

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)

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

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

PATENT

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

US Patent App. 18/542,423