Zheng Zhou — Curriculum Vitae

github.com/zhouzhengqd zhouzhengqd.github.io
zhengzhou@buaa.edu.cn (+86) 15610035199

RESEARCH INTEREST

My research focuses on exploring the latent properties of neural networks and their connections to brain mechanisms, with the goal of enhancing the reliability and efficiency of machine learning. I aim to investigate these properties from the perspective of robustness and efficiency through two key areas:

. AI Security & Privacy

. Data-efficient Machine Learning

EDUCATION

Beihang University **Beijing, China**
Ph.D. in Electronic Engineering *September 2023 - Now*
Advisor: Prof. Qi Zhao & Prof. Wenquan Feng

Shandong University **Qingdao, China**
M.Eng. in Electronic Engineering *September 2020 - June 2023*
Advisor: Prof. Ju Liu

Technical University of Ilmenau **Thuerigen, Germany**
Visiting Student in Electronic Engineering *September 2016 - October 2018*

Qingdao University of Science and Technology **Qingdao, China**
B.Eng. in Mechanical Engineering and Automation *September 2012 - June 2016*

AWARDS & HONORS

Top Reviewer *NeurIPS, 2024*

Silver Award *ASCEND Competition for Re-ID, 2023*

Oral *The Thirteenth International Conference on Swarm Intelligence (ICSI), 2022*

Academic Service

. **Conference Reviewer**
NeurIPS 2025/2024, *ICLR* 2026/2025, *ICML* 2025, *AAAI* 2026, *AISTATS* 2026/2025

. **Journal Reviewer**
IEEE Transactions on Information Forensics & Security (TIFS), *Transactions on Machine Learning Research (TMLR)*

WORK EXPERIENCE

Haier Group Corporation *2018 - 2023*
Open Innovation Platform & GE Appliance Development Devision
Embedded Software Engineer

. **Project Leadership:** Led multiple AI-driven home appliance projects, including sweeping and mopping robots, and water heaters.

. **Algorithm Development:** Developed and optimized Edge AI applications involving food detection, speech recognition, and defect detection using machine learning techniques.

. **Team Collaboration:** Collaborated with cross-functional teams through daily planning and code reviews to ensure high-quality software delivery.

. **Model Tuning:** Applied algorithm design and model tuning to enhance AI system performance in real-world embedded environments.

CONFERENCE PAPERS

C1. **ROME is Forged in Adversity: Robust Distilled Datasets via Information Bottleneck**
Zhou, Zheng, and Feng, Wenquan and Zhang, Qiaosheng and Lyu, Shuchang and Zhao, Qi and Cheng, Guangliang
International Conference on Machine Learning (ICML), 2025.

C2. **Adversarial Examples Are Closely Relevant to Neural Network Models - A Preliminary Experiment Explore**
Zhou, Zheng and Liu, Ju and Han, Yanyang
Advances in Swarm Intelligence. International Conference on Swarm Intelligence, ICSI. Lecture Notes in Computer Science, vol 13345. Springer, Cham., 2022.

MANUSCRIPTS

M1. **BEARD: Benchmarking the Adversarial Robustness for Dataset Distillation**
Zhou, Zheng and Feng, Wenquan and Lyu, Shuchang and Cheng, Guangliang and Huang, Xiaowei and Zhao, Qi
arXiv preprint arXiv:2411.09265, 2024.
Submitted to top-tier AI conference - Under double-blind review

M2. **BACON: Bayesian Optimal Condensation Framework for Dataset Distillation**
Zhou, Zheng and Zhao, Hongbo and Cheng, Guangliang and Li, Xiangtai and Lyu, Shuchang and Feng, Wenquan and Zhao, Qi
arXiv preprint arXiv:2406.01112, 2024.
Submitted to top-tier AI conference - Under double-blind review

M3. **MVPatch: More Vivid Patch for Adversarial Camouflaged Attacks on Object Detectors in the Physical World**
Zhou, Zheng and Zhao, Hongbo and Liu, Ju and Zhang, Qiaosheng and Geng, Liwei and Lyu, Shuchang and Feng, Wenquan
arXiv preprint arXiv:2312.17431, 2023.
Submitted to EAAI - Under review