

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 sustainability, 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

Ph.D. in Electronic Engineering

Advisor: Prof. Hongbo Zhao & Prof. Wenquan Feng

Beijing, China

September 2023 - Now

Shandong University

M.Eng. in Electronic Engineering

Advisor: Prof. Ju Liu

Qingdao, China

September 2020 - June 2023

Technical University of Ilmenau

Visiting Student in Electronic Engineering

Thuerigen, Germany

September 2016 - October 2018

Qingdao University of Science and Technology

B.Eng. in Mechanical Engineering and Automation

Qingdao, China

September 2012 - June 2016

AWARDS & HONORS

Oral

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

Silver Award

ASCEND Competition for Re-ID, 2023

Service

Conference Reviewer

* *NeurIPS 2024*

* *ICLR 2025*

Journal Reviewer

* *Knowledge-Based Systems (KBS)*

* *IEEE Transactions on Geoscience and Remote Sensing (IEEE TGRS)*

WORK EXPERIENCE

Haier Group Corporation

2018 - 2023

– Open Innovation Platform & GE Appliance Development Division

– Embedded Software Engineer

- As a technical leader, organized and completed multiple projects in the home appliance sector, including sweeping robots, mopping robots, and water heaters.
- Took responsibility for Edge AI applications in the home appliance industry, such as food detection, speech recognition, and defect detection.
- Conducted daily planning sessions and code reviews with team members.

CONFERENCE PAPERS

C1 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 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 IEEE Transactions - Under 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

TO DO LIST

TDL1 BEARD: Benchmarking the Adversarial Robustness in Dataset Distillation

Zhou, Zheng, and co-authors TBD

Unpublished, 2024.

In preparation for submission to ICLR 2025

TDL2 ROME is Forged in Adversity: Robust Distilled Datasets via Information Bottleneck

Zhou, Zheng, and co-authors TBD

Unpublished, 2024.

In preparation for submission to ICLR 2025