周 正 | 个人简历

github.com/zhouzhengqd zhouzhengqd.github.io

zhengzhou@buaa.edu.cn (+86) 15610035199

研究兴趣

我的研究旨在探索神经网络的潜在属性及其与大脑机制的联系，目标是在提高机器学习可靠性的同时提升训练效率。研究兴趣集中于以下两个方向：

. 人工智能安全与隐私保护

. 数据高效的机器学习方法

教育经历

北京航空航天大学 **中国，北京**

电子信息 博士 *2023 年 9 月 - 至今*

导师：赵琦教授，冯文全教授

山东大学 **中国，青岛**

电子信息 硕士 *2020 年 9 月 - 2023 年 6 月*

导师：刘琚教授

伊尔梅瑙工业大学 **德国，图林根**

电子信息 访问学生 *2016 年 9 月 - 2018 年 10 月*

青岛科技大学 **中国，青岛**

机械工程及其自动化 学士 *2012 年 9 月 - 2016 年 6 月*

奖项 & 荣誉

- **学业二等奖学金**，北京航空航天大学，2025/2024
- **顶级审稿人奖**，国际人工智能会议 *NeurIPS*，2024
- **新生奖学金**，北京航空航天大学，2023
- **华为 Ascend 重识别大赛银奖**，华为, 2023
- **国际会议口头报告**，国际群体智能会议 *ICSI*，2022
- **校级奖学金**，青岛科技大学，2015
- **优秀学生会干部**，青岛科技大学，2014

学术服务

. **会议审稿人**：*NeurIPS* 2025/2024，*ICLR* 2026/2025，*ICML* 2025，*AAAI* 2026，*AISTATS* 2026/2025

. **期刊审稿人**：*IEEE Transactions on Information Forensics & Security (TIFS)*, *Transactions on Machine Learning Research (TMLR)*

工作经历

海尔集团 *2018 - 2023*

开放式创新平台 & 美国 GEA 家电开发部

嵌入式软件工程师

. **项目管理**：主导多个 AI 家电项目，包括扫拖机器人和热水器等。

. **算法开发**：开发并优化边缘 AI 应用，包括食品识别、语音识别与缺陷检测。

. **团队协作**：跨部门合作进行代码评审与每日计划，确保交付质量。

. **模型优化**：在嵌入式环境中调优算法和模型以提高性能。

会议论文

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.

论文投稿

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