

HAOKUN CHEN

81549 Munich, Germany ◊ (+49) 15237770369 ◊ chenhaokun24549@gmail.com ◊ haokunchen245.github.io

EDUCATION

University of Munich (Munich, Germany) 11.2021 - Present

Ph.D. (Supervisor: Prof. Dr. Volker Tresp and Dr. Denis Krompaß)

Interests: **Multimodal Learning**: Post-training of LLMs, Vision-Language Foundation Models.

Trustworthy AI: Federated Learning, Machine Unlearning, Adversarial Attacks.

Technical University of Munich (Munich, Germany) 10.2018 - 10.2021

Master of Science (Major: Computer Science) GPA: 1.6/1.0

Tongji University (Shanghai, China) 10.2014 - 10.2018

Bachelor of Science (Major: Mechatronic Engineering) GPA: 4.2/5.0

EXPERIENCE

Research Intern, Siemens AG (Munich, Germany) 01.2021 - Present

- Developed a hyperparameter tuning pipeline for distributed LLM optimization; research published at *AAAI 2025* (Oral, First Author). Integrated the algorithm into an internal RAG-based industrial chatbot using Azure ML.
- Proposed a PEFT-based post-training algorithm for LLMs and Vision-LLMs using Federated Learning with distributed datasets; the manuscript was accepted at *AAAI 2024* (First Author).
- Designed algorithms to address data heterogeneity, deficiency, and system scalability in Federated Learning; methods accepted at *ICCV 2023* and *CVPR 2025* (Both First Author).
- Conducting research on adversarial robustness and red-teaming strategies for Multimodal LLMs.

Research Intern, Intel Corp. (US, Remote) 08.2024 - 11.2024

- Conducted research on Machine Unlearning for responsible LLMs and Multimodal LLMs.
- Contributed to LLM adversarial robustness toolkit (LLMart): <https://github.com/IntelLabs/LLMart>

Research Intern, BMW Autonomous Driving Campus (Munich, Germany) 03.2020 - 11.2020

- Developed a Computer Vision function validation framework in C++.

PUBLICATIONS

Haokun Chen, Hang Li, Jindong Gu, Denis Krompass, Volker Tresp.

FedBiP: Heterogeneous One-Shot Federated Learning with Personalized Latent Diffusion Models

Conference on Computer Vision and Pattern Recognition (CVPR), 2025.

Haokun Chen, Denis Krompass, Jindong Gu, Volker Tresp.

FedPop: Federated Population-based Hyperparameter Tuning

AAAI Conference on Artificial Intelligence (AAAI), 2025, **Oral**.

Haokun Chen, Yao Zhang, Denis Krompass, Jindong Gu, Volker Tresp.

FedDAT: An Approach for Foundation Model Finetuning in Multi-Modal Heterogeneous Federated Learning

AAAI Conference on Artificial Intelligence (AAAI), 2024.

Haokun Chen, Ahmed Frikha, Denis Krompass, Jindong Gu, Volker Tresp.

FRAug: Tackling Federated Learning with Non-IID Features via Representation Augmentation

International Conference on Computer Vision (ICCV), 2023.

Haokun Chen, Sebastian Szyller, Weilin Xu, Nageen Himayat.
Soft Token Attacks Cannot Reliably Audit Unlearning in Large Language Models
Under review, 2025.

Haokun Chen, Jianing Li, Yao Zhang, Denis Krompass, Volker Tresp.
AUVIC: Adversarial Unlearning of Visual Concepts for Multi-Modal Large Language Models
Under review, 2025.

Yao Zhang, **Haokun Chen**, Ahmed Frikha, Yezi Yang, Denis Krompass, Gengyuan Zhang, Jindong Gu, Volker Tresp.
Cl-crossvqa: A continual learning benchmark for cross-domain visual question answering
Winter Conference on Applications of Computer Vision (WACV), 2025.

Jinhe Bi, Yujun Wang, **Haokun Chen**, Xun Xiao, Artur Hecker, Volker Tresp, Yunpu Ma.
LLaVA Steering: Visual Instruction Tuning with 500x Fewer Parameters through Modality Linear Representation-Steering
Under review, 2025.

Yao Zhang, Hwei Gao, **Haokun Chen**, Tong Liu, Yunpu Ma, Volker Tresp.
FedNano: Toward Lightweight Federated Tuning for Pretrained Multimodal Large Language Models
Under review, 2025.

Yao Zhang, Chenyang Lin, **Haokun Chen**, Yunpu Ma, Volker Tresp.
SwarmAgentic: Towards Fully Automated Agentic System Generation via Swarm Intelligence
Under review, 2025.

Ahmed Frikha*, **Haokun Chen***, Denis Krompass, Thomas Runkler, Volker Tresp.
Towards Data-Free Domain Generalization
Asian Conference on Machine Learning (ACML), 2022.

ADDITIONAL INFORMATION

SKILLS *Programming Languages:* Python, C++, Unix, Git.

Frameworks: PyTorch, DeepSpeed, Distributed Training, Langchain, TernsorRT-LLM, RAG, Docker.

Miscellaneous: German Language (C1).

REVIEW *Conferences:* Computer Vision: CVPR 2025, ECCV 2024, ICCV 2025.

Machine Learning: NeurIPS 2024, ICLR 2025, ICML 2025.

Artificial Intelligence: AAI 2024/2025, AISTATS 2025, IJCNN 2025.

Journal: TPAMI, TKDE, TKDD, TCNN