Computer Science and Engineering Department
Michigan State University
East Lansing, MI 48823, USA

Mobile: (+1)-352-870-5374
Email: jiajingh@msu.edu
Website:Homepage

RESEARCH FOCUSES

Deep learning: Trustworthy Machine Learning (Machine Unlearning, Adversarial Learning, OOD), Computer Vision (Diffusion-based Generation, image reconstruction/classification), Natural language processing (LLMs, AI4Code, etc), Multi-Modality (Video Understanding, etc)
Optimization: Bi-level optimization, Zeroth-order black-box optimization

EDUCATION

Ph.D. Candidate in Computer Science, Michigan State University Aug. 2021– Present

M.S. in Electrical and Computer Engineering, University of Florida Aug. 2019– May. 2021

B.Eng in Computer Science, Univ. of Science and Technology of China Sep. 2015– July 2019

PUBLICATIONS

Google Scholar

[1] **J. Jia**, J. Liu, et al. "Model sparsity can simplify machine unlearning", *NeurIPS'23 - Spotlight.*

[2] Y. Zhang, Y. Zhang, A. Chen, **J. Jia**, et al. "Selectivity Drives Productivity: Efficient Dataset Pruning for Enhanced Transfer Learning", *NeurIPS'23*

[3] **J. Jia**, S. Srikant, T. Mitrovska, S. Chang, S. Liu, U. O'Reilly, "Having Both: Robust and Accurate Code Models", *SANER'23*

[4] B. Hou, **J. Jia**, Y.Zhang, G.Zhang, S. Liu, S. Chang, "TextGrad: Advancing Robustness Evaluation in NLP by Gradient-Driven Optimization", *ICLR'23*

[5] Y. Zhang, X. Chen, **J Jia**, S Liu, K Ding, Text-Visual Prompting for Efficient 2D Temporal Video Grounding, *CVPR'23*

[6] H Li, **J Jia**, S Liang, Y Yao, S Ravishankar, S Liu, SMUG: Towards robust MRI reconstruction by smoothed unrolling, *ICASSP'23*

[7] **J. Jia**, Y Zhang, D Song, S Liu, A Hero, Robustness-preserving Lifelong Learning via Dataset Condensation, *ICASSP'23*

[8] **J. Jia**, M. Hong, Y. Zhang, M. Akçakaya, S. Liu, On the Robustness of deep learning-based MRI Reconstruction to image transformations, *NeurIPS'22 workshop*

[9] Y. Zhang, Y. Yao, **J. Jia**, J. Yi, M. Hong, S. Chang, S. Liu, "How to Robustify Black-Box ML Models? A Zeroth-Order Optimization Perspective", International Conference on Learning Representation *ICLR'22 - Spotlight*

[10] **J. Jia**, C Zhang, B Yaman, S Moeller, S Liu, M Hong, M Akçakaya, "On Instabilities of Conventional Multi-Coil MRI Reconstruction to Small Adversarial Perturbations", International Society for Magnetic Resonance in Medicine *ISMRM'21 - Oral*

PREPRINT

[1] A. Chen, Y. Zhang, **J. Jia**, et al. "DeepZero: Scaling up Zeroth-order Optimization for Deep Model Training".

[2] **J. Jia**, Y. Zhang, et al. "To Generate or Not? Safety-Driven Unlearned Diffusion Models Are Still Easy To Generate Unsafe Images... For Now".

ACADEMIC ACTIVITIES

- **Contributors to code demos** for NeurIPS'22 tutorial: Foundational Robustness of Foundation Models.
- **Reviewer**: ICASSP'22/23/24, ICML'22, ICLR'22/23/24, NeurIPS'22/23, CVPR, AAAI'24, AISTATS'24
- **TPC** for KDD'22 Workshop 4th Workshop on Adversarial learning Methods for Machine learning and Data Mining
- **Student Chair** for ICML'22 and ICML'23 Workshop AdvML:New Frontiers in Adversarial Machine Learning.

WORK EXPERIENCE

- Applied Science Intern, Amazon, 2023
- Machine Learning Algorithm Engineering Intern, Zoom, 2018

AWARD

- NeurIPS Scholar Award, 2023
- Herbert Wertheim College of Engineering Achievement Award Scholarship, 2019&2020
- USTC Outstanding Student Scholarship, 2018
- USTC Newly Enrolled Students Scholarship, 2015

SKILLS

- **Programming Languages** Python, MATLAB, C++, Java, C
- **Libraries** Pytorch, Huggingface, TensorFlow, Numpy, Matplotlib