Tao Wu

Department of Computer Science
Missouri University of Science and Technology
Rolla, MO, USA

Email: wuta@mst.edu
Website: https://mstwutao.github.io/
Google Scholar: /citations?user=KS0Q4oEAAAAJ&hl=en

Education

Missouri University of Science and Technology — Rolla, MO, USA
Ph.D. in Computer Science — Aug. 2018 - May. 2024 (expected)
Focus: Adversarial Attacks and Robustness, — Advisor: Dr. Donald C. Wunsch and Dr. Tie Luo

Huazhong University of Science and Technology — Wuhan, Hubei, China
B.S in Engineering Mechanics — Aug. 2014 - May. 2018

Research Interests

Adversarial Attacks and Robustness

Explainable and Trustworthy AI

Optimization for Generalization

Self-supervised Pretraining and Finetuning

Experience

Teaching Instructor — Aug. 2021 – Present
Missouri University of Science and Technology — *Rolla, MO*

- Teach 200+ total undergraduate students in CS1982 **Matlab Programming Laboratory** across 4 semesters.
- Design summer course CS1970 **Introduction to C++ Programming** as sole instructor, write and present 40+ lectures, to teach how to solve data structure and algorithm problems with C++ programming.
- Troubleshoot and answer computer hardware and programming problems brought by students and host office hours.

Graduate Researcher — Aug. 2018 – Jul. 2021
Missouri University of Science and Technology — *Rolla, MO*

- Publish 5 research papers as the first author and deliver presentations at 2 major machine learning conferences.
- Explore **adversarial vulnerability** of DNNs and leverage adversarial training mechanism to enhance robustness.
- Develop efficient **optimization** algorithms for training CNN/ ViT and validate on large-scale image datasets.
- Design novel **self-supervised training and finetuning** strategy for image retrieval and image clustering tasks.

Summer Research Internship — Aug. 2017 – Oct. 2017
Applied Computational Intelligence Laboratory — *Rolla, MO*

- Analyze training instability and mode collapse problem of Generative Adversarial Networks (GAN) via game theory.
- Implement 10+ network architectures, loss functions, normalizations and regularizations for stable training of GAN.

Selected Projects

Adversarial Vulnerability of DNNs

- Analyze the adversarial vulnerability of modern DNNs from network architecture, loss landscape and optimization.
- Develop novel algorithms by finetuning pretrained models for generating more transferable adversarial examples.
- Our methods offer **7%-35%** improvement on attack success rate over SOTA and paper accepted by **AAAI** 2024.

Curvature Regularized Optimization

- Introduce the concept of **normalized hessian trace** to accurately measure the curvature of DNNs' loss landscape.
- Develop efficient algorithm for optimizing Hessian and implement parallel training for CNNs/ViT on GPU clusters.
- Our methods offer up to **1%** absolute accuracy increase on ImageNet over SGD and paper accepted by **AAAI** 2024.

Technical Skills

Programming: Python, C/C++, MATLAB, SQL, HTML, CSS.
Developer Tools: Linux, Git, NVIDIA Jetson, Bash, Docker, AWS, GCP.
ML Libraries: PyTorch, Huggingface, TensorFlow, Scikit-learn, Numpy, Pandas, Flask.
Professionals: Computer Vision, CNN, Transformers, Clustering, Generative models.

Licenses & certifications

- **AWS Cloud Technical Essentials (Coursera)**
- **AI for Medical Diagnosis (Coursera)**
- **Image and Video Processing (Coursera)**
- **Advanced Computer Vision with TensorFlow (Coursera)**
- **Advanced Learning Algorithms (Coursera)**

Awards and Scholarships

- Outstanding Graduates, HUST, 2018
- National Endeavor Scholarship of China, 2016
- Study Excellence Scholarship, 2016

Teachings

- **Fall 2021. CS1982 Matlab Programming Laboratory**
- **Spring 2022. CS1982 Matlab Programming Laboratory**
- **Summer 2022. CS1970 Introduction to C++ Programming**
- **Fall 2022. CS1982 Matlab Programming Laboratory**
- **Spring 2023. CS1982 Matlab Programming Laboratory**
- **Spring 2024. CS6405 Clustering Algorithms**

Publications

[1] Tao Wu, Tie Luo, and Donald C Wunsch. Feature map rearrangement: A zero-flop method for enhancing adversarial transferability efficiently. *submitted to International Joint Conference on Artificial Intelligence (IJCAI), under review*, 2024.

[2] Tao Wu, Tie Luo, and Donald C Wunsch. Cr-sam: Curvature regularized sharpness-aware minimization. *AAAI Conference on Artificial Intelligence (AAAI)*, 2024.

[3] Tao Wu, Tie Luo, and Donald C Wunsch. Lrs: Enhancing adversarial transferability through lipschitz regularized surrogate. *AAAI Conference on Artificial Intelligence (AAAI)*, 2024.

[4] Tao Wu, Tie Luo, and Donald C Wunsch. Gnp attack: Transferable adversarial examples via gradient norm penalty. In *2023 IEEE International Conference on Image Processing (ICIP)*, pages 3110–3114. IEEE, 2023.

[5] Tao Wu, Tie Luo, and Donald C Wunsch. Black-box attack using adversarial examples: A new method of improving transferability. *World Scientific Annual Review of Artificial Intelligence*, 1:2250005, 2023.

[6] Tao Wu, Tie Luo, and Donald C Wunsch. Learning deep representations via contrastive learning for instance retrieval. In *2022 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1501–1506. IEEE, 2022.