Jing Wu

Building 72, Clayton, Melbourne, VIC 3800, Australia
jing.wu1@monash.edu | Google Scholar | Homepage | LinkedIn

Research Interest

My work mostly contributes to the fields of trustworthy machine learning and responsible AI. My research mainly focuses on the analysis of the vulnerabilities of deep learning models, and developing algorithms for enhancing safety and reliability by defending against attacks and mitigating inappropriate influence in AI systems. My long-term research objective is to make AI systems safe, reliable, and unbias, as AI increasingly becomes a part of our daily lives, its safety and reliability must be paramount considerations prior to deployment.

Education

Monash University — Melbourne, Australia
Doctor of Philosophy in Electrical and Computer Systems Engineering — *Aug. 2021 – Present*
Advisors: A/Prof. Mehrtash Harandi and Dr. Munawar Hayat. Thesis submitted.

University of Electronic Science and Technology of China — Chengdu, China
Master in Electronics and Communication Engineering GPA: 3.79/4.0 — *Sept. 2017 – June. 2020*

Saitama University — Saitama, Japan
Exchange student funded by Chinese Scholarship Council — *Sept. 2015 – Mar. 2016*

Nanjing University of Information Science and Technology — Nanjing, China
Bachelor in Electronic Information Engineering (rank 1st in major) GPA: 4.12/5.0 — *Sept. 2013 – June. 2017*

Work Experience

Assistant Lecturer — Jan. 2024 – Jan. 2025
Monash University - Fixed-term (PhD Teaching Fellow) employment — *Melbourne, Australia*

Sessional Teaching Associate — July. 2022 – Dec. 2023
Monash University — *Melbourne, Australia*

Research Assistant — Aug. 2020 – July. 2021
University of Electronic Science and Technology of China — *Chengdu, China*

Research Intern — July. 2019 – Mar. 2020
Megvii Technology Co.,Ltd. — *Chengdu, China*

Selected Publications

Jing Wu, Trung Le, Munawar Hayat, Mehrtash Harandi. EraseDiff: Erasing Data Influence in Diffusion Models. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2025. (CORE A^*)

Jing Wu and Mehrtash Harandi. Scissorhands: Scrub Data Influence via Connection Sensitivity in Networks. The 18th European Conference on Computer Vision (ECCV) 2024. (CORE A^*)

Jing Wu, Munawar Hayat, Mingyi Zhou. and Mehrtash Harandi. Concealing Sensitive Samples against Gradient Leakage in Federated Learning. Proceedings of the AAAI Conference on Artificial Intelligence (AAAI). 2024. (CORE A^*)

Mingyi Zhou, Xiang Gao, **Jing Wu**, et al. Investigating White-Box Attacks for On-Device Models. 46th International Conference on Software Engineering (ICSE) 2024. (CORE A^*)

Xianggang Li, **Jing Wu**, et al. Analyzing the pregnancy status of giant pandas with hierarchical behavioral information. Expert Systems with Applications 237, 121462, 2024. (JCR Q1)

Mingyi Zhou*, **Jing Wu***, et al. DaST: Data-free Substitute Training for Adversarial Attacks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020. (*Equal contribution, Oral, CORE A^*)

Teaching

ECE4179/5179/6179 - Neural networks and deep learning: S2 2024, S2 2023, S2 2022 - Design content (problem sets for the workshop and assignments, etc.), deliver the lab content and grade assignments.
ECE4076/5176 - Computer vision: S1 2024, S1 2023 - Design content (problem sets for the workshop and assignments, etc.), deliver the lab content and grade assignments.
ENG5001/6001 - Advanced engineering data analysis: S1 2023 - Design and deliver the lab content.

Grant

Analysis of giant panda's prenatal behavior video Jan. 2021 – Dec. 2022
Chengdu Research Base of Giant Panda Breeding Collaboration *Grant: 200,000 CNY*

My Roles:

- Help construct the definition of hierarchical behaviors and guide students to annotate the collected video.
- Design the pregnancy analysis model.
- Supervise Master students for algorithm implementation.
- Write and revise the paper.

PROFESSIONAL SERVICE ACTIVITIES

Program Committee: AAAI Conference on Artificial Intelligence (AAAI)

Conference Reviewer:

- International Conference on Learning Representations (ICLR)
- Neural Information Processing Systems (NeurIPS)
- International Conference on Machine Learning (ICML)
- Conference on Computer Vision and Pattern Recognition (CVPR)
- International Conference on Computer Vision (ICCV)
- European Conference on Computer Vision (ECCV)
- ACM Multimedia (ACM MM): Outstanding Reviewer for ACM MM 2024
- International Conference on Artificial Intelligence and Statistics (AISTATS)

Journal Reviewer:

- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)
- Transactions on Machine Learning Research (TMLR)
- IEEE Transactions on Emerging Topics in Computational Intelligence

Advising

Setareh Dehghanfard, Undergraduate student at University of Tehran - Identity Unlearning

Ghazal Mousavi, Undergraduate student at University of Tehran - Identity Unlearning

Chern Khing Boey, Undergraduate student at Monash University - Graphic model of human brain connectome

Shiqi Lin, Undergraduate student at Monash University - Image Detection

Shiyu Feng, Master student at UESTC - AI security

Jingjing Hou, Master student at UESTC - AI security

Jinfeng Xu, Master student at UESTC - AI security

Ziruo Hao, Undergraduate student at UESTC - AI security

Skills

Language: Mandarin (native), English (fluent)
Programming languages and frameworks: Python, MATLAB, Pytorch
Typesetting: Latex, Markdown

Prizes and Honors

- CSIRO DATA61 Top-up scholarship (2022)
- IEEEXtrume 12.0 Programming Competition (2018): 312/9500
- First-class Scholarship of School (2018)
- National Scholarships (Highest level scholarship in Chinese Universities, 2016): 30,000 CNY
- Chinese Scholarship Council (2015): around 800,000 JPY
- National Undergraduate Electronics Design Contest of China (Team leader, 2015): First Prize
- Excellent Red Cross Volunteers in School (2013)