Jing Wu

Research Fellow, Monash University

✉ wwujing123@gmail.com · ☎ (+61) 431990599 · Google Scholar

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 2021.08 – 2025.02
Doctor of Philosophy in Artificial Intelligence
Supervisors: *A/Prof. Mehrtash Harandi, Dr. Munawar*

University of Electronic Science and Technology of China, Chengdu, China 2017.09 – 2020.06
Master in Electronics and Communication Engineering GPA: 3.79/4.0

Saitama University, Saitama, Japan 2015.09 – 2016.03
Exchange student

Nanjing University of Information Science and Technology, Nanjing, China 2013.09 – 2017.06
Bachelor in Electronic Information Engineering GPA: 4.12/5.0

Work Experience

Monash University, Research Fellow 2025.04 – Present
Department of Data Science & AI, Faculty of Information Technology

Monash University, Assistant Lecturer 2024.01 – 2025.02
Faculty of Engineering

Monash University, Sessional Teaching Associate 2022.07 – 2024.01
Faculty of Engineering

University of Electronic Science and Technology of China, Research Assistant 2020.07 – 2021.08
School of Information and Communication Engineering

Megvii Technology Co.,Ltd., Research Intern 2019.07 – 2020.03
Chengdu, China

Selected Publications

- *DIET: Machine Unlearning on a Data-Diet*
  Nilakshan Kunananthaseelan, **Jing Wu**, Trung Le, Gholamreza Haffari, Mehrtash Harandi.
  Proceedings of the AAAI Conference on Artificial Intelligence. AAAI 2026, Oral, CORE A^*
- *Machine Unlearning via Nash Bargaining*
  Jing Wu, Mehrtash Harandi.
  International Conference on Computer Vision. ICCV 2025, CORE A^*.
- *EraseDiff: Erasing Data Influence in Diffusion Models*
  Jing Wu, Trung Le, Munawar Hayat, Mehrtash Harandi.
  IEEE/CVF Conference on Computer Vision and Pattern Recognition. CVPR 2025, CORE A^*.

- *Scissorhands: Scrub Data Influence via Connection Sensitivity in Networks*
  Jing Wu, Mehrtash Harandi.
  The 18th European Conference on Computer Vision. ECCV 2024, CORE A^*.
- *Concealing Sensitive Samples against Gradient Leakage in Federated Learning*
  Jing Wu, Munawar Hayat, Mingyi Zhou, Mehrtash Harandi.
  Proceedings of the AAAI Conference on Artificial Intelligence. AAAI 2024, CORE A^*.
- *Analyzing the pregnancy status of giant pandas with hierarchical behavioral information.*
  Xianggang Li, **Jing Wu**, Rong Hou, Zhangyu Zhou, Chang Duan, Peng Liu, Mengnan He, Yingjie Zhou, Peng Chen, Ce Zhu.
  Expert Systems with Applications 237, 121462, 2024. JCR Q1.
- *Investigating White-Box Attacks for On-Device Models.*
  Mingyi Zhou, Xiang Gao, **Jing Wu**, Kui Liu, Hailong Sun, Li Li
  International Conference on Software Engineering. ICSE 2024, CORE A^*.
- *ModelObfuscator: Obfuscating Model Information to Protect Deployed ML-based Systems.*
  Mingyi Zhou, Xiang Gao, **Jing Wu**, John Grundy, Chunyang Chen, Xiao Chen, Li Li
  ACM SIGSOFT International Symposium on Software Testing and Analysis. ISSTA 2023, CORE A.
- *A survey on universal adversarial attack.*
  Chaoning Zhang, Philipp Benz, Chenguo Lin, Adil Karjauv, **Jing Wu**, In So Kweon.
  Thirtieth International Joint Conference on Artificial Intelligence. IJCAI 2021, CORE A^*.
- *Data-Free Substitute Training for Adversarial Attacks.*
  Mingyi Zhou*, **Jing Wu***, Yipeng Liu, Shuangcheng Liu, Ce Zhu
  IEEE/CVF Conference on Computer Vision and Pattern Recognition. CVPR 2020, Oral, CORE A^*.

Teaching

ECE4179/5179/6179 - Neural networks and deep learning: S2 2024, S2 2023, S2 2022
ECE4076/5176 - Computer vision: S1 2024, S1 2023
ENG5001/6001 - Advanced engineering data analysis: S1 2023

Advising

- Isaac Ning Lee, Honours student at Monash University - Test-time Adaptation
- Yuanyuan Liu, PhD at Xi'an University of Technology - Video casual reasoning
- Yifan Zhu, Undergraduate student at Beihang University - LLM Unlearning
- Xindi Fan, Undergraduate student at Harbin Institute of Technology - Machine Unlearning
- Chern Khing Boey, Honours student at Monash University - Graphic model of human brain connectome
- Shiqi Lin, Honours student at Monash University - Image Detection

PROFESSIONAL SERVICE ACTIVITIES

Program Committee:

- AAAI Conference on Artificial Intelligence (AAAI)
- European Conference on Artificial Intelligence (ECAI)

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)
- IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)

- International Journal of Computer Vision (IJCV)
- Transactions on Machine Learning Research (TMLR)
- IEEE Transactions on Emerging Topics in Computational Intelligence

☆ Prizes and Honors

- Monash University Travel Grant 2025
- Monash University Travel Grant 2024
- Top Reviewer for NeurIPS 2024
- Outstanding Reviewer for ACM MM 2024
- CSIRO DATA61 Top-up scholarship (2022)
- National Scholarships (Highest level scholarship in Chinese Universities, 2016)
- Chinese Scholarship Council Scholarships (2015)