Yiwei Lu

☎ (226)7476966
✉ y485lu@uwaterloo.ca

Education

2020-present **University of Waterloo**, *Ph.D. candidate in Computer Science*.
Waterloo AI Lab and Vector Institute
Supervisor: Prof. Yaoliang Yu and Prof. Sun Sun

2018-2020 **University of Manitoba**, *M.Sc. in Computer Science*.
Computer Vision Lab, Supported by University of Manitoba Graduate Funding
Supervisor: Prof. Yang Wang
Thesis: Anomaly Detection in Surveillance Videos using Deep Learning

2013-2017 **University of Electronic Science and Technology of China**, *B.E. in Electronic Engineering*.
Statistical Machine Intelligence and Learning Lab
Supervisor: Prof. Zenglin Xu and Prof. Zhao Kang
Thesis and patent: Design of a Phase-Reconfigurable Antenna Unit

2016 **University of California, Santa Barbara**, *Electrical Computer Engineering*.
Exchange Program, Funded by China Scholarship Council

Experiences

2022 **Research Internship**, *Huawei Noah's Ark Lab, Montreal*.
Machine Learning Researcher on Neural Network Quantization
Published a paper in NeurIPS 2023.

2021 **Research Internship**, *National Research Council of Canada, Waterloo*.
Machine Learning Researcher on Contrastive Learning
Published a paper in NeurIPS 2021 Workshop and TMLR 2023.

2020-2022 **Teaching Assistant**, *University of Waterloo*.
CS480/680: Introduction to Machine Learning
CS116: Introduction to Computer Science 2
CS245: Logic and Computation

2018-2020 **Teaching Assistant**, *University of Manitoba*.
COMP4190: Advanced Artificial Intelligence
COMP4550: Real-time Systems

Award and Honors

2024	David R. Cheriton Graduate Scholarship
2023	NeurIPS 2023 Top Reviewer
2023	Conference Funding, University of Waterloo
2023	Graduate Student Research Dissemination Award, University of Waterloo
2019-2020	University of Manitoba Graduate Funding (UMGF)
2019	University of Manitoba Graduate Studies Travel Funding
2018-2019	University of Manitoba Graduate Fellowship
2013-2017	People's Scholarship of China
2016	China Scholarship Council Scholarship for Studying Abroad
2016	UESTC Exchange Award

Publications

Journal Papers

[1] **"f-MICL: Understanding and Generalizing InfoNCE-based Contrastive Learning"**, ***Yiwei Lu***, *Guojun Zhang, Sun Sun, Hongyu Guo, Yaoliang Yu*, in *Transactions on Machine Learning Research (TMLR), 2023* (also appeared in *NeurIPS 2021 Workshop on Self-supervised Learning)*.

[2] **"Indiscriminate Data Poisoning Attacks on Neural Networks"**, ***Yiwei Lu***, *Gautam Kamath, Yaoliang Yu*, in *Transactions on Machine Learning Research (TMLR), 2022 (also appeared in* NeurIPS 2022 ML Safety Workshop and Trustworthy and Socially Responsible Machine Learning (TSRML) Workshop*)*.

[3] **"AdaCrowd: Unlabeled Scene Adaptation for Crowd Counting"**, *Mahesh Kumar Krishna Reddy, Mrigank Rochan,* ***Yiwei Lu***, *Yang Wang*, in *IEEE Transactions on Multimedia, Volume 24, Page 1008-1019, 2022*.

[4] **"Structure Learning with Similarity Preserving"**, *Zhao Kang, Xiao Lu,* ***Yiwei Lu***, *Chong Peng, Wenyu Chen, and Zenglin Xu*, in *Neural Networks, 2020, Volume 129, Page 138-148*.

Conference Papers

[5] **"Understanding Neural Network Binarization with Forward and Backward Proximal Quantizers"**, ***Yiwei Lu***, *Yaoliang Yu, Xinlin Li, Vahid Partovi Nia*, in *NeurIPS 2023*.

[6] **"Exploring the Limits of Model-Targeted Indiscriminate Data Poisoning Attacks"**, ***Yiwei Lu***, *Gautam Kamath, Yaoliang Yu*, in *ICML 2023*.

[7] **"Few-shot Scene-Adaptive Anomaly Detection"** **(Spotlight)**, ***Yiwei Lu***, *Frank Yu, Mahesh Kumar K and Yang Wang*, in *ECCV 2020*.

[8] **"Future Frame Prediction Using Convolutional VRNN for Anomaly Detection"**, ***Yiwei Lu***, *Mahesh Kumar K, Seyed shahabeddin Nabavi and Yang Wang.*, in *IEEE AVSS 2019*.

[9] **"Similarity Learning via Kernel Preserving Embedding"**, *Zhao Kang,* ***Yiwei Lu***, *Yuanzhang Su, Changsheng Li, Zenglin Xu*, in *AAAI 2019* .

[10] **"Homoglyph Attack Detection with Unpaired Data"**, ***Yiwei Lu***, *Mahesh Kumar K, Noman Mohammed, Yang Wang*, in *ACM/IEEE Symposium on Edge Computing 2019*.

Workshop Papers

[11] **"CM-GAN: Stabilizing GAN Training with Consistency Models"**, *Haoye Lu,* ***Yiwei Lu***, *Dihong Jiang, Spencer Ryan Szabados, Sun Sun, Yaoliang Yu*, in *ICML 2023 Wrokshop on Structured Probabilistic Inference & Generative Modeling*.

[12] **"Semantic Segmentation in Compressed Videos"**, ***Yiwei Lu***, *Ang Li and Yang Wang*, in *IEEE International Workshop on Multimedia Signal Processing 2019*.

Submitted Papers

[13] **"Indiscriminate Data Poisoning Attacks on Pre-trained Feature Extractors"**, ***Yiwei Lu***, *Matthew Y.R Yang, Gautam Kamath, Yaoliang Yu*, submitted in 2023.

Service

Conference Reviewer, *ICLR 2024, NeurIPS 2023, ICML 2023, TSMLR 2022, NeurIPS 2022, HAET 2022, ICML2022, AAAI 2022, AAAI 2021*.

Journal Reviewer, *Neural Networks, IEEE Transactions on Multimedia, IEEE Transactions on Circuits and Systems for Video Technology*.