Avery Ma

Vector Institute
Schwartz Reisman Innovation Campus
108 College St, Suite W1140
Toronto, ON M5G 0C6
averyma.com
ama@cs.toronto.edu
Last update: Feb 2025

Education

Ph.D in Computer Science **Toronto ON**
University of Toronto, Vector Institute *2018 – 2024*

- Thesis: Understanding Adversarial Robustness in Deep Learning
- Supervisors: Amir-massoud Farahmand and Richard Zemel

M.A.Sc. in Systems Design Engineering **Waterloo ON**
University of Waterloo, Vision and Image Processing Lab *2016 – 2018*

- Thesis: "Computational Depth from Defocus via Active Quasi-random Pattern Projections"
- Supervisors: Alexander Wong and David Clausi

B.A.Sc. in Mechatronics Engineering *with Distinction*, Honours, Co-op Program **Waterloo ON**
University of Waterloo *2011 – 2016*

- Capstone project: "All Terrain Personal Transportation Device"

Publications

- **Avery Ma**, Yangchen Pan, Amir-massoud Farahmand (2025). PANDAS: Improving Many-shot Jailbreaking via Positive Affirmation, Negative Demonstration, and Adaptive Sampling. *Under Review.*
- **Avery Ma**, Amir-massoud Farahmand, Yangchen Pan, Philip Torr, Jindong Gu (2024). Improving Adversarial Transferability via Model Alignment. *ECCV'24: European Conference on Computer Vision.*
- Jindong Gu, Xiaojun Jia, Pau de Jorge, Wenqian Yu, Xinwei Liu, **Avery Ma**, Yuan Xun, Anjun Hu, Ashkan Khakzar, Zhijiang Li, Xiaochun Cao, Philip Torr (2023). A Survey on Transferability of Adversarial Examples Across Deep Neural Networks. *TMLR: Transactions on Machine Learning Research.*
- **Avery Ma**, Yangchen Pan, Amir-massoud Farahmand (2023). Understanding the robustness difference between stochastic gradient descent and adaptive gradient methods. *TMLR: Transactions on Machine Learning Research (**Featured Certification (Top 3%)**, ICLR'24 Journal-to-Conference*).
- **Avery Ma**, Nikita Dvornik, Ran Zhang, Leila Pishdad, Konstantinos G. Derpanis, Afsaneh Fazly (2022). SAGE: Saliency-Guided Mixup with Optimal Rearrangements. *BMVC'22: British Machine Vision Conference.*
- **Avery Ma**, Aladin Virmaux, Kevin Scaman, Juwei Lu (2021). Improving Hierarchical Adversarial Robustness of Deep Neural Network. *arXiv preprint arXiv: 2102.09012.*
- **Avery Ma**, Fartash Faghri, Nicolas Papernot, Amir-massoud Farahmand (2020). SOAR: Second-Order Adversarial Regularization. *arXiv preprint arXiv: 2004.01832* .
- Plinio Morita, Adson Rocha, George Shaker, Dave Lee, Jing Wei, Brandon Fong, Anjali Thatte, Amir Karimi, Linlin Xu, **Avery Ma**, Alexander Wong, Jennifer Boger (2020). Comparative Analysis of Gait

Speed Estimation Using Wideband and Narrowband Radars, Thermal Camera, and Motion Tracking Suit Technologies. *Journal of Healthcare Informatics Research.*

- **Avery Ma**, Alexander Wong, David Clausi (2018). Deep Learning-driven Depth from Defocus via Active Multispectral Quasi-random Projections with Complex Subpatterns. *CRV'18: Conference on Computer and Robot Vision.*
- **Avery Ma**, Ahmed Gawish, Mark Lamm, Alexander Wong, Paul Fieguth (2018). Real-time Spatial-based Projector Resolution Enhancement. *SID'18: Society for Information Display.*
- **Avery Ma**, Alexander Wong (2018). An Inverse Problem Approach to Computational Active Depth from Defocus. *Journal of Physics: Conference Series.*
- Xiaodan Hu, **Avery Ma**, Ahmed Gawish, Mark Lamm, Paul Fieguth (2017). Motion Detection in High Resolution Enhancement. *CVIS'17: Conference on Vision and Imaging Systems.*
- **Avery Ma**, Alexander Wong, David Clausi (2017). Depth from defocus via active multispectral quasi-random point projections using deep learning. *CVIS'17: Conference on Vision and Imaging Systems.*
- **Avery Ma**, Alexander Wong, David Clausi (2017). Depth from Defocus via Active Quasi-random Point Projections: a Deep Learning Approach. *ICIAR'17: International Conference on Image Analysis and Recognition.*
- **Avery Ma**, Alexander Wong (2017). Enhanced Depth from Defocus via Active Quasi-random Colored Point Projections. *ICIPE'17: International Conference on Inverse Problems in Engineering.*
- **Avery Ma**, Francis Li, Alexander Wong (2016). Depth from Defocus via Active Quasi-random Point Projections. *CVIS'16: Conference on Vision and Imaging Systems.*

Patents

- **Bojie Ma**, Nikita Dvornik, Ran Zhang, Konstantinos Derpanis, Afsaneh Fazly (2023). Saliency-guided mixup with optimal re-arrangements for efficient data augmentation. Patent App.: 18/201,521
- **Bojie Ma**, Ahmed Gawish, Alexander Wong, Paul Fieguth, Mark Lamm (2018). Real-time spatial-based resolution enhancement using shifted superposition. Patent No.: US10009587 B1

Research Experience

Research Intern **Toronto ON**
Huawei - Noah's Ark Lab (Host: Yangchen Pan) *Sept 2022 – Dec 2022*
- Implicit regularization of optimization and its connection to out-of-distribution generalization

Research Intern **Toronto ON**
Samsung - Samsung AI Center (Host: Afsaneh Fazly) *May 2021 – Aug 2022*
- Data augmentation for improving model generalization in the multi-modal learning setting

Research Intern **Toronto ON**
Huawei - Noah's Ark Lab (Host: Juwei Lu) *May – Nov 2020*
- Improving hierarchical adversarial robustness of deep neural networks

Research Intern **Kitchener ON**
Christie Digital - Advanced Technologies Group (Host: Mark Lamm) *May 2016 – Apr 2017*
- Multiple spatial-temporal super-resolution enhancement methods for projectors

Undergraduate Research Assistant **Waterloo ON**
University of Waterloo - Vision and Image Processing Lab (Host: Prof. Alexander Wong) *Jan – Apr 2015*
- Graph contraction algorithms for large scale graph computation

Research Intern **Toronto ON**
University Health Network - Princess Margaret Hospital (Host: Dr. Robert Weersink) *May – Aug 2013*
- Prototyped an integrated 3D imaging and reconstruction system for intra-operative 3D registration

Work Experience

Mechatronics Engineer, Co-op **Cleveland OH**
Bendix Commercial Vehicle Systems - Vehicle Electronics Group *Sept – Dec 2015*

Electrical Engineer, Co-op **Mississauga ON**
Baylis Medical Company - Biomedical Engineering Group *Jan – Apr 2014*

Software Developer, Co-op **Ottawa ON**
JSI Telecom - UX Team *Sept – Dec 2012*

QA Engineer, Co-op **Calgary AB**
TeleCommunication Systems Inc. - QA Team *Jan – Apr 2012*

Honors and Awards

- DAAD AInet Fellowship for the Postdoc-NeT-AI Program on Safety and Security in AI *Apr 2024*
- Ray Reiter Graduate Award in Computer Science *Feb 2024*
- NeurIPS'23 Top Reviewer *Dec 2023*
- University of Toronto Doctoral Completion Award *Jan 2023 – Apr 2023*
- NSERC Canada Graduate Scholarship - Doctoral (CGS-D) *Sept 2018 – Dec 2022*
- University of Waterloo Alumni Gold Medal (Department Nomination) *Sept 2018*
- Ontario Graduate Scholarship *May 2017 – Apr 2018*
- University of Waterloo President's Graduate Scholarship *May 2017 – Apr 2018*
- University of Waterloo Provost Graduate Scholarship *May 2016 – Apr 2017*
- University of Waterloo President's Scholarship *Sept 2011*

Teaching Assistantships

University of Toronto
- Mathematical Expression and Reasoning for Computer Science *Winter 2020*

University of Waterloo
- Introduction to Pattern Recognition *Winter 2018*
- Digital Computation: Introduction to C++ Programming *Fall 2017*
- Advanced Engineering Math 2: Numerical Methods for ODEs *Spring 2016*

Conference Presentations

- **Avery Ma**, Amir-massoud Farahmand, Yangchen Pan, Philip Torr, Jindong Gu (2024). Improving Adversarial Transferability via Model Alignment. **Poster Presentation** at the *18th European Conference*

on Computer Vision. Milan, Italy

- **Avery Ma**, Yangchen Pan, Amir-massoud Farahmand (2024). Understanding the robustness difference between stochastic gradient descent and adaptive gradient methods. **Poster Presentation** at the *12th International Conference on Learning Representations.* Vienna, Austria
- **Avery Ma**, Simona Meng, Amir-massoud Farahmand (2021). Adversarial Robustness through the Lens of Fourier Analysis. **Poster Presentation** at the *Vector Rsearch Symposium.* Vector Institute, Toronto, Ontario
- **Avery Ma**, Amir-massoud Farahmand (2019). Adversarial Robustness using Taylor Series-based Regularizer. **Poster Presentation** at the *Evolution of Deep Learning Symposium.* Vector Institute, Toronto, Ontario
- **Avery Ma**, Amir-massoud Farahmand (2018). Adversarial Robustness Through Loss regularization. **Poster Presentation** at the *Vector Research Symposium.* Vector Institute, Toronto, Ontario

Talks

- **Ludwig Maximilian University of Munich, Mathematisches Institut** **Nov 2024**
  "Understanding generalization, robustness, and adversarial transferability."
- **Ludwig Maximilian University of Munich, Tresp Lab** **Nov 2024**
  "Understanding generalization, robustness, and adversarial transferability.""
- **University of Toronto, CSC413: Neural Networks and Deep Learning (Guest Lecturer)** **Apr 2024**
  "Is Your Neural Network at Risk? The Pitfall of Adaptive Gradient Optimizers"
- **University of Waterloo, Vision and Image Processing Lab** **Nov 2017**
  "Real-time Spatial-based Resolution Enhancement"
- **University of Waterloo, Systems Design Engineering Graduate Seminar** **Feb 2017**
  "Depth from Defocus via Active Quasi-random Pattern Projection: A Deep Learning Approach"
- **University of Waterloo, Vision and Image Processing Lab** **Oct 2016**
  "Depth from Defocus via Active Pattern Projection"

Student Mentoring

- Simona Meng (Undergraduate – UofT). Topic: Frequency-domain Analysis of Adversarial Robustness of Deep Neural Networks (May 2020 - May 2021)

Professional Activities and Services

- International Conference on Learning Representations (**ICLR**) (2023, 2025)
- Conference on Neural Information Processing Systems (**NeurIPS**) (2023, 2024)
- International Conference on Machine Learning (**ICML**) (2023, 2024, 2025)
- Computer Vision and Image Understanding (**CVIU**) (2022)
- Artificial Intelligence and Statistics (**AISTATS**) (2022, 2025)
- Transactions on Machine Learning Research (**TMLR**)
- Graduate application assistance program for prospective students in groups underrepresented in Computer Science, University of Toronto (2021, 2022, 2023, 2024)
- Graduate admissions committee at the Department of Computer Science, University of Toronto (2020)