Hadi Mohaghegh Dolatabadi

Email: mhgh2hadi@gmail.com
Media: Twitter, Website, Google Scholar

Professional Experience

- **Research Fellow in Machine Learning for Automated Decision Making** — Melbourne, Australia
  The University of Melbourne & ARC Center of Excellence (ADM+S) — *Nov. 2022 - Present*
  - Testing implications of data privacy using unlearnable examples and their vulnerability to diffusion models.
  - Researching the definitions of fairness in generative modeling.
  - Supervision of Ph.D. students on topological data analysis and anomaly detection.
  - Supervision of master students on efficient training of neural networks with coreset selection.

- **Graduate Research Student** — Melbourne, Australia
  The University of Melbourne — *Jun. 2019 - May 2023*
  - Design and implementation of various types of generative models (normalizing flows, generative adversarial networks, and diffusion models) for low and high-dimensional data.
  - Design and implementation of robust and efficient learning frameworks for defending neural networks against backdoor and adversarial attacks.
  - Design and implementation of an incognito black-box adversarial attack exploiting the data distribution.

- **Applied Scientist I** — Melbourne, Australia
  Amazon — *Aug. 2021 - Jan. 2022*
  - Generative modeling for 3D image attribute editing.

Education

- **The University of Melbourne** — Melbourne, Australia
  Ph.D. in Computing and Information Systems — *Jun. 2019 - May 2023*
  - **Supervisors**: Dr. Sarah Erfani, Prof. Christopher Leckie

- **Sharif University of Technology** — Tehran, Iran
  M.Sc. in Electrical Engineering-Communications System. — *Sep. 2015 - Sep. 2017*
  - **GPA**: 18.89/20.0 (4.00/4.00)

- **The University of Tehran** — Tehran, Iran
  B.Sc. in Electrical Engineering-Telecommunications. — *Sep. 2011 - Sep. 2015*
  - **GPA**: 18.33/20.0 (3.92/4.00)

Publications

[Under review] **H. M. Dolatabadi**, S. Erfani, and C. Leckie, "The Devil's Advocate: Shattering the Illusion of Unexploitable Data using Diffusion Models," *arXiv preprint arXiv:2303.08500*, 2023. (Link)

H. M. Dolatabadi, "A Novel Perspective on Robustness in Deep Learning," Doctoral Dissertation, School of Computing and Information Systems, the University of Melbourne, 2023. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie, "Adversarial Coreset Selection for Efficient Robust Training," To appear at the *International Journal of Computer Vision* (**IJCV**) (**IF=19.5**), 2023. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie "Collider: A Robust Training Framework for Backdoor Data," in *Proceedings of the 16th Asian Conference on Computer Vision* (**ACCV**), pp. 3893-3910, 2022. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie "ℓ_∞-Robustness and Beyond: Unleashing Efficient Adversarial Training," in *Proceedings of the 17th European Conference on Computer Vision* (**ECCV**), pp. 467-483, 2022. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie "AdvFlow: Inconspicuous Black-box Adversarial Attacks using Normalizing Flows," in *Proceedings of the 34th Conference on Neural Information Processing Systems* (**NeurIPS**), pp. 15871-15884, 2020. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie "Black-box Adversarial Example Generation with Normalizing Flows," in *the ICML Workshop on Invertible Neural Networks, Normalizing Flows, and Explicit Likelihood Models* (**INNF+**), 2020. (Link)

H. M. Dolatabadi, S. Erfani, and C. Leckie "Invertible Generative Modeling using Linear Rational Splines," in *Proceedings of the 23rd International Conference on Artificial Intelligence and Statistics* (**AISTATS**), pp. 4236-4246, 2020. (Link)

H. M. Dolatabadi and A. Amini, "Deterministic Design of Toeplitz Matrices with Small Coherence Based on Weyl Sums," *IEEE Signal Processing Letters* (**IF=4.6**), vol. 26, no. 10, pp. 1501-1505, 2019. (Link)

H. M. Dolatabadi and A. Amini, "A Sampling Theorem for Convex Shapes with Algebraic Boundaries," in *Proceedings of the International Conference on Sampling Theory and Applications* (**SampTA**), pp. 499-503, 2017. (Link)

Honors and Awards

- Awarded outstanding reviewer award (top 2%) at the *International Conference on Computer Vision* (ICCV 2023).
- Runner-up team at the *ADM+S Hackathon* and awarded 6k AUD in research fundings for the project "Polls and Prejudices: Investigating Bias in LLM-Generated Political Personas."
- Awarded the *DAAD AINet Postdoctoral Fellowship* in Generative Modeling.
- Awarded outstanding reviewer award at the *Asian Conference on Computer Vision* (ACCV 2022).
- Admitted to *Machine Learning Summer School* (MLSS 2020) at the Max Planck Institute for Intelligent Systems, Tübingen, Germany (acceptance rate: 13.84%).
- Awarded a *Melbourne Research Scholarship* to pursue Ph.D. at the University of Melbourne, Australia.
- Ranked 2$^{\text{nd}}$ among 33 Communication Systems students at Electrical Engineering Department, Sharif University of Technology, Tehran, Iran.
- Ranked 15$^{\text{th}}$ (top 0.2%) in the *Iranian Nationwide University Entrance Exam* for postgraduate studies in Communication Engineering.
- Recognized as the *Outstanding Talent* at University of Tehran and awarded admission to the M.Sc. program.
- Ranked 380$^{\text{th}}$ (top 0.15%) among more than 250,000 participants of the *Iranian Nationwide University Entrance Exam* for undergraduate studies.

Teaching Experience

- **Statistical Machine Learning** — The University of Melbourne
  Tutor — *Semester 1 2022*
- **Compressed Sensing** — Sharif University of Technology
  Teaching Assistant — *Spring 2017*
- **Signals and Systems** — Sharif University of Technology
  Teaching Assistant — *Spring 2017*
- **Engineering Mathematics** — Sharif University of Technology
  Teaching Assistant — *Fall 2017*

Skills

Programming	Python (PyTorch, TensorFlow, OpenCV, SciPy, SkLearn), C (familiar), MATLAB
Operating Systems	Linux (Ubuntu), Windows
Cloud Services	AWS (EC2, S3, IAM)
Others	Git, MySQL (familiar)
Languages	English (fluent, PTE Academic score of 90/90), Persian (native), Arabic (basic)

Invited Talks

- **Security and Privacy of Large Language Models** — Security Analytics Subject
  University of Melbourne, Parkville, Australia. — *Oct. 2023*
- **A Novel Perspective on Robustness in Deep Learning** — AINet Postdoctoral Event
  ITWM Fraunhofer, Kaiserslautern, Germany. — *Sep. 2023*
- **A Novel Perspective on Robustness in Deep Learning** — AINet Postdoctoral Event
  Technical University of Kaiserslautern, Germany. — *Sep. 2023*
- **Publishing at AI Venues** — ADM+S HDR Workshop
  RMIT University, Melbourne, Australia. — *Mar. 2023*
- **Shattering the Illusion of Unexploitable Data using Diffusion Models** — ADM+S Machines Meeting
  RMIT University, Melbourne, Australia. — *Mar. 2023*

Service

Invited Reviewer	NeurIPS 2021-23, ICLR 2022-24, ICML 2023, AISTATS 2022-24, ICCV 2023, ACCV 2022, IEEE TPAMI, TMLR.