Ameya Joshi

ameya.joshi@nyu.edu | ameya.j005@gmail.com | ameya005.github.io | Ph: +1-917-679-5996 | +1-515-817-3175

Education

Jan 2020 -May 2023	Doctor of Philosophy (PhD) in Electrical Engineering **New York University** Advisor: Dr. Chinmay Hegde Thesis: Robustness and Control in Deep Networks.
Aug 2018 -Dec 2019	Doctor of Philosophy (PhD) in Electrical Engineering (Transferred to NYU) **Iowa State University** Advisors: Dr. Chinmay Hegde, Dr. Soumik Sarkar
Aug 2010 -May 2014	Bachelor of Engineering (Hons.) in Electrical and Electronics Engineering **BITS Pilani**, India

Research Interests

Robust Algorithms for multimodal models, Adversarial Robustness for Deep Learning, Vision-Text Models, Generative Models for Structured Data, Physics Informed Generative Models, Generative Adversarial Networks, Computer Vision

Work Experience

Jan 2020 -*present*	**Graduate Research Assistant** at **NYU Tandon School of Engineering**, New York City, NY Adversarial Attacks and Defenses for Deep Models, Physics Informed Generative Models, Neural PDE Solvers, Generalization Theory for Neural Networks
May 2022-Aug 2022	**Machine Learning SWE Intern** at **Meta Platforms Inc.**, New York, NY Developed ensemble-based modelling schemes for ranking Reels at the Reels Core Modelling Team at Instagram Reels Ranking. Improved over production models by 0.65% intentional plays.
May 2021 -Aug 2021	**Machine Learning Research Intern** at **Bosch Center for AI**, Pittsburgh, PA Certified Adversarial defenses on video classifiers.
Aug 2018 -Dec 2019	**Graduate Research Assistant** at **Iowa State University**, Ames, Iowa Adversarial Attacks and Defenses for Deep Models, Physics Informed Generative Models, Neural PDE Solvers.
May 2016 -Jul 2018	**Lead Computer Scientist** at **SigTuple Inc.**, Bengaluru, India Worked on building ML informed systems for pathology and ophthalmology. Led a team of 5 data scientists. Two papers published at ISBI'18. One patent granted by Indian PTO.
Feb 2015 -May 2016	**Member of Technical Staff** at **Tonbo Imaging**, Bengaluru, India Developed and deployed robust embedded systems (including linux kernel dev.) for night vision and IR devices for long range surveillance. Contributed to deployment of tracking and detection algorithms for IR imaging.
Jul 2014 -Feb 2015	**Computer Vision Engineer** at **Ducere Technologies**, Hyderabad, India Developed a computer vision system for obstacle detection used for navigation by the visually impaired. Also conceptualised and prototyped an image-to-Braille device for the visually impaired.

Publications

Journal Articles

1. A. Mukherjee, **A. Joshi**, A. Sharma, *et al.*, "Generative semantic domain adaptation for perception in autonomous driving.," *J. Big Data Anal. Transp.*, 2022
2. G. Jagatap, **A. Joshi**, A. B. Chowdhury, S. Garg, and C. Hegde, "Adversarially robust learning via entropic regularization," *Frontiers in Artificial Intelligence*, 2021
3. X. Lee, J. R. Waite, C.-H. Yang, B. Pokuri, **A. Joshi**, A. Balu, C. Hegde, B. Ganapathysubramanian, and S. Sarkar, "Fast inverse design of microstructures via generative invariance networks," *Nature Computational Science*, 2020

Conferences and Workshop Papers

1. M. Cho, **A. Joshi**, S. Garg, B. Reagen, and C. Hegde, "Selective network linearization for efficient private inference," in *ICML*, 2022
2. M. Cho, A. Balu, **A. Joshi**, A. D. Prasad, B. Khara, S. Sarkar, B. Ganapathysubramanian, A. Krishnamurthy, and C. Hegde, "Differentiable spline approximations," in *NeurIPS*, 2021
3. M. Cho, **A. Joshi**, and C. Hegde, "ESPN: Extremely sparse pruned networks," in *IEEE Data Science Learning Workshop*, 2021
4. **A. Joshi**, B. Khara, S. Sarkar, B. Ganapathysubramanian, and C. Hegde, "Solving linear PDEs with generative models," in *Asilomar Conf. on Signals, Systems and Computers*, 2020
5. **A. Joshi**, M. Cho, V. Shah, B. Pokuri, S. Sarkar, B. Ganapathysubramanian, and C. Hegde, "Invnet: Encoding geometric and statistical invariances in deep generative models," in *Asso. of Adv. of Artif. Intell. (AAAI)*, 2020
6. **A. Joshi**, A. Mukherjee, S. Sarkar, and C. Hegde, "Semantic adversarial attacks: Parametric transformations that fool deep classifiers," in *Int. Conf. on Computer Vision (ICCV)*, 2019
7. S. Athar, A. Vahadane, **A. Joshi**, and T. Dastidar, "Weakly supervised fluid filled region localization in retinal oct scans," in *ISBI*, IEEE, 2018

8. A. Vahadane, **A. Joshi**, K. Madan, and T. Dastidar, "Detection of diabetic macular edema in optical coherence tomography scans using patch based deep learning," in *ISBI*, IEEE, 2018
9. A. Mahurkar, **A. Joshi**, N. Nallapareddy, P. Reddy, M. Feigin, A. Kadambi, and R. Raskar, "Selective visualization of anomalies in fundus images via sparse and low rank decomposition," in *ACM SIGGRAPH 2014 Posters*, 2014
10. **A. Joshi**, S. Akula, G. Jagatap, and C. Hegde, "A few adversarial tokens can break vision transformers," in *CVPR Workshop Adversarial Machine Learning (AdvML)*, 2023
11. B. Feuer, **A. Joshi**, M. Cho, K. Jani, S. Chiranjeevi, Z. Deng, A. Balu, N. Merchant, A. Singh, S. Sarkar, A. Singh, B. Ganapathysubramanian, and C. Hegde, "Zero-shot insect detection via weak language supervision," in *AAAI Workshop on AI for Agri. and Food Sci. (AIAFS)*, 2023
12. M. Z. Hasan, **A. Joshi**, M. Rahman, A. Venkatachalapathy, A. Sharma, C. Hegde, and S. Sarkar, "Driveclip: Zero-shot transfer for distracted driving activity understanding using clip," in *NeurIPS Workshop on ML for Autonomous Driving (ML4AD)*, 2022
13. B. Feuer, **A. Joshi**, and C. Hegde, "A meta-analysis of distributionally-robust models," in *ICML Workshop on Principles of Distribution Shift*, 2022
14. **A. Joshi**, G. Jagatap, and C. Hegde, "Adversarial token attacks on vision transformers," *CVPR Workshop on Transformers for Vision*, 2022 **(Spotlight talk)**
15. B. Khara, A. Balu, **A. Joshi**, A. Krishnamurthy, S. Sarkar, C. Hegde, and B. Ganapathysubramanian, "Field solutions of parametric pdes.," in *AAAI Symp. on Machine Learning for Physical Sciences (AAAI-MLPS)*, 2021
16. S. Botelho, **A. Joshi**, B. Khara, S. Sarkar, C. Hegde, S. Adavani, and B. Ganapathysubramanian, "Deep generative models that solve PDEs: Distributed computing for training large data-free models," in *Int. Conf. of High Perf. Comput., Netw., Storage and Analy.(SC) Workshop on ML in HPC (MLHPC)*, 2020
17. **A. Joshi**, V. Shah, S. Ghosal, B. Pokuri, S. Sarkar, B. Ganapathysubramanian, and C. Hegde, "Generative models for solving nonlinear partial differential equations," in *NeurIPS Workshop on ML for Physical Sciences (ML4PS)*, 2019

Preprints

1. B. Feuer, **A. Joshi**, and C. Hegde, "Caption supervision enables robust learners," *arXiv preprint arxiv: 2210.07396*, 2022
2. M. Pham, M. Cho, **A. Joshi**, and C. Hegde, "Revisiting self-distillation," *arXiV preprint arxiv:2206.08491*, 2022
3. **A. Joshi**, M. Pham, M. Cho, L. Boytsov, F. Condessa, J. Z. Kolter, and C. Hegde, "Smooth-reduce: Leveraging patches for improved certified robustness," *arXiV preprint arxiv:2205.06154*, 2022
4. B. Khara, A. Balu, **A. Joshi**, S. Sarkar, C. Hegde, A. Krishnamurthy, and B. Ganapathysubramanian, "Neufenet: Neural finite element solutions with theoretical bounds for parametric pdes," *ArXiV preprint arxiv:2110.01601*, 2021

Patents

1. **A. Joshi** *et al.*, "Method and system for detecting disorders in retinal images," Indian Patent 313571, 2018

Programming Languages and Frameworks

Python, C, C++, Shell, TensorFlow, PyTorch, JAX, OpenCV, CUDA, Matlab, MongoDB, NodeJS, ReactJS

Graduate Courses

Statistical Learning Theory, Advanced Machine Learning, Image Processing, Algorithmic Machine Learning and Data Science, ML for Cybersecurity, Reinforcement Learning and Optimal Control, Deep Learning, Optimization for Machine Learning, Random Processes, Special Topics on Stat. Machine Learning

Scholarships and Awards

2018	2nd Place, MRS OpenData Challenge, Material Research Society
2010 - 14	MCN Scholarship, **BITS Pilani**
2007	National Talent Search Scholar (Top 1000 students in India) , **NCERT**, India

Reviewing Responsibilities

1. Neural Information Processing Systems (NeurIPS), 2022, 2023
2. International Conf. on Machine Learning (ICML), 2022, 2023
3. European Conference on Computer Vision (ECCV), 2022
4. Computer Vision and Pattern Recognition (CVPR), 2022, 2023
5. International Conf. on Learning Representations (ICLR), 2021, 2022, 2023
6. Internation Conf. on Computer Vision (ICCV), 2023
7. AAAI Workshop on AI for Design and Manufacturing (ADAM), 2022
8. AAAI Conference on Artificial Intelligence, 2021
9. NeurIPS workshop on ML for Autonomous Driving, 2020, 2021, 2022
10. Plant Phenomics, Science partner journal, 2020
11. Asilomar Conference on Signals, Systems, and Computers, 2020