Pratik Vaishnavi

pvaishnavi@cs.stonybrook.edu LinkedIn Homepage

Summary

- My research experience lies within computer vision and machine learning/deep learning, covering a wide range of topics such as adversarial robustness, domain generalization, transfer learning, knowledge distillation, and self-supervised learning. I have experience working with a range of ML models including classifiers, detectors, generative AI models, and segmentation models. I excel in rapidly adapting to new challenges and consistently delivering results in unfamiliar domains.

Employment History

- **Security & Privacy Research Intern,** SonyAI, Tokyo, Japan *May 2023 - Sep 2023*
  I was tasked with reducing the financial expenses and environmental impact associated with training adversarially robust object detectors for Sony's commercial applications. I developed a method that significantly reduced GPU hours required for adversarial training by reducing the dataset size at no major cost to robustness. Notably, my work addressed an unexplored gap in the literature.
- **Applied Scientist Intern,** Amazon, Seattle, WA *Jun 2021 - Sep 2021*
  I was tasked with designing a system for detecting degradation in the Amazon One's palm-based biometric device. I developed a 3D-CNN based detection model that comfortably met the initial goals of the project by reliably detecting a wide range of degradations even in presence of significant variations in palm's pose and illumination. My results spawned a new project for a full-time employee.
- **Applied Scientist Intern,** Amazon, Remote *May 2020 - Aug 2020*
  I was tasked with enhancing the security of the Amazon One biometric device against unseen spoofing attacks using very few real spoof images. I designed a novel method for generating synthetic spoof images, using GANs guided by spoof detector's performance. I showed for the first time that synthetic training data is effective at fortifying the device's resilience against unseen attacks.

Education

- **Ph.D., Stony Brook University** *Aug 2018 - Dec 2023*
  Thesis title: *Improving the Usability of Adversarially Robust Training Methods*
- **MS, Stony Brook University** *Aug 2016 - May 2018*
  Thesis title: *Generating Temporal Action Proposals in Long Untrimmed Videos*
- **B.Tech., Sardar Vallabhbhai National Institute of Technology** *Jul 2012 - May 2016*

Research Publications

1. P. Vaishnavi, K. Eykholt, and A. Rahmati, "Accelerating certified robustness training via knowledge transfer," *Advances in Neural Information Processing Systems (NeurIPS)*, 2022.
2. P. Vaishnavi, V. Krish, F. Ahmed, K. Eykholt, and A. Rahmati, "On the feasibility of compressing certifiably robust neural networks," in *NeurIPS Workshop on Trustworthy and Socially Responsible Machine Learning*, 2022.
3. P. Vaishnavi, K. Eykholt, and A. Rahmati, "Transferring adversarial robustness through robust representation matching," in *USENIX Security Symposium*, 2022.
4. F. Ahmed, P. Vaishnavi, K. Eykholt, and A. Rahmati, "Ares: A system-oriented wargame framework for adversarial ML," in *IEEE Security and Privacy Workshops (SPW)*, 2022.

5 P. Vaishnavi, T. Cong, K. Eykholt, A. Prakash, and A. Rahmati, "Can attention masks improve adversarial robustness?" In *AAAI Workshop on Engineering Dependable and Secure Machine Learning Systems*, 2020.

6 P. Vaishnavi, K. Eykholt, A. Prakash, and A. Rahmati, "Towards model-agnostic adversarial defenses using adversarially trained autoencoders," *arXiv preprint arXiv:1909.05921*, 2019.

7 K. Eykholt, S. Gupta, A. Prakash, A. Rahmati, P. Vaishnavi, and H. Zheng, "Robust classification using robust feature augmentation," *arXiv preprint arXiv:1905.10904*, 2019.

8 A. Mohanty, A. Ahmed, T. Goswami, A. Das, P. Vaishnavi, and R. R. Sahay, "Robust pose recognition using deep learning," in *International Conference on Computer Vision and Image Processing*, 2017.

9 A. Mohanty, P. Vaishnavi, P. Jana, *et al.*, "Nrityabodha: Towards understanding indian classical dance using a deep learning approach," *Signal Processing: Image Communication*, 2016.

Academic Services

Reviewer Duties

Conferences	CVPR, ICCV, ECCV, ACCV, NeurIPS, ICLR, ICML, USENIX Security, IEEE S&P
Journals	IEEE Transactions on Image Processing, IEEE Transactions on Information Forensics & Security
Workshops	Trustworthy and Socially Responsible Machine Learning (NeurIPS '22), Engineering Dependable and Secure Machine Learning Systems (AAAI '20)

Teaching Assistantship, Stony Brook University

- CSE 508: Network Security (Fall'19 & Spring'21)
- CSE 527: Introduction to Computer Vision (Spring'19)
- CSE 512: Machine Learning (Fall'18)

Skills

Coding	Python, MatLab, LaTeX, Markdown
Deep Learning	PyTorch, TensorFlow, Keras
Other	Git, AWS

Miscellaneous

Stony Brook University

- Best Poster Award Recipient, Graduate Research Day '23
- Organizer, Adversarial Machine Learning Reading Group (Spring'22)
- Mentor, Women in Science and Engineering Lab Rotations (Spring'21 & Fall'21)
- Vice President, Computer Science Graduate Student Organization (Fall'20 & Spring'21)
- Organizer, Graduate Research Day '21

Sardar Vallabhbhai National Institute of Technology

- Executive Board Member, Literary Affairs Committee
- Editor, College Newsletter