PRATIK VAISHNAVI

pvaishnavi@cs.stonybrook.edu | Stony Brook, NY
pratik18v.github.io | linkedin.com/in/pratik-vaishnavi-aa2585b3

PROFESSIONAL SUMMARY

8+ years of research experience in Machine Learning, Deep Learning, and Computer Vision, covering the following **topics**: adversarial robustness, transfer learning, knowledge distillation, self-supervised learning, domain generalization, and video understanding; and the following **models**: classifiers, detectors, GANs, transformers, and segmentation models.

EDUCATION

PhD, Computer Science, Stony Brook University ***08/2018 – 05/2024 (Expected)***
Thesis: Improving the Usability of Methods for Training and Evaluating Secure ML Models
Topics: Adversarial Machine Learning, Knowledge Transfer, Vision Foundation Models, LLM Pre-training

MS, Computer Science, Stony Brook University ***08/2016 – 05/2018***
Thesis: Generating Temporal Action Proposals in Long Untrimmed Videos
Topics: Video Understanding, Action Detection, Sequential Modelling (LSTMs, GRUs)

BTech, Electronics, Sardar Vallabhbhai National Institute of Technology ***07/2012 – 05/2016***
Thesis: Developing Software for Drone-Based Precision Farming

EXPERIENCE

Sony AI, Security & Privacy Research Intern, Tokyo, Japan ***05/2023 – 09/2023***
Developed an efficient method to train secure object detectors (Faster-RCNN, YOLO, SSD) using dataset distillation. Reduced training time by 50% while preserving performance and robustness, in turn reducing monetary costs and environmental impact associated with GPU usage.

Amazon, Applied Scientist Intern, Seattle, WA ***06/2021 – 09/2021***
Curated a camera obstruction dataset from scratch, containing over 3000 videos collected using 19 unique obstructions. Using this data, developed a video-based camera obstruction detector (3D-CNN) to improve the reliability of Amazon One devices in unrestricted deployment settings. Work was published at Amazon Machine Learning Conference and spawned a dedicated project for a new full-time employee.

Amazon, Applied Scientist Intern, Remote ***05/2020 – 08/2020***
Developed a novel facial spoof image generation method using Generative Adversarial Networks (GANs). Effectively integrated this synthetic data into the training process of the spoof detector, reducing ACER by 14% on average across 13 unseen spoof types. This was the first demonstration of the utility of synthetic data towards spoof detection for facial recognition systems and was published at Amazon Computer Vision Conference.

SKILLS

- **Coding**: Python, Bash, HTML, CSS, JavaScript
- **Python Libraries**: NumPy, Pandas, Scikit-learn, OpenCV, Jupyter, Matplotlib, XGBoost
- **Deep Learning Frameworks**: PyTorch, TensorFlow, Keras
- **Cloud Platforms**: AWS (EC2, S3, SageMaker), GCP
- **Documentation**: LaTeX, Markdown
- **Miscellaneous**: Linux, MATLAB, Git, Docker, Slurm

SELECTED PUBLICATIONS

- Accelerating Certified Robustness Training via Knowledge Transfer
  NeurIPS 2022 | *P. Vaishnavi*, K. Eykholt, and A. Rahmati
- On the Feasibility of Compressing Certifiably Robust Neural Networks
  TSRML Workshop @ NeurIPS 2022 | *P. Vaishnavi*, V. Krish, F. Ahmed, K. Eykholt, and A. Rahmati
- Transferring Adversarial Robustness Through Robust Representation Matching
  USENIX Security Symposium 2022 | *P. Vaishnavi*, K. Eykholt, and A. Rahmati
- Ares: A System-Oriented Wargame Framework for Adversarial ML
  IEEE Security and Privacy Workshops 2022 | F. Ahmed, *P. Vaishnavi*, K. Eykholt, and A. Rahmati
- Can Attention Masks Improve Adversarial Robustness?
  EDSMLS Workshop @ AAAI 2020 | *P. Vaishnavi*, T. Cong, K. Eykholt, A. Prakash, and A. Rahmati
- Complete List on Google Scholar

OTHER PROJECTS

- **Rethinking Threat Modeling for Adversarial Evasion Attacks** *(ongoing)*
  Developed a generalizable framework for breaking down a range of attacks (white-box, black-box, and adaptive) into their fundamental components. This framework defines the space of attack strategies, with different permutations of components representing unique attacks. Proposed a comprehensive way of defining threat models in terms of space of attack strategies a defense is supposed to withstand.
- **Leveraging Vision Foundation Models for Secure ML** *(Fall 2023 and Spring 2024)*
  Under review at TMLR 2023. Investigated the potential of vision foundation models and transfer learning to alleviate the high sample complexity of robust learning. Utilized a variety of pre-trained models (supervised, simCLR, BYOL, CLIP, etc.) and 12 downstream tasks to highlight the conditions under which transfer learning from foundation models enhances adversarial robustness.
- **Accelerating LLM Pre-training Using Knowledge Transfer** *(Spring 2023 and Fall 2023)*
  Developed a method to accelerate pre-training of LLMs (T5, BERT, GPT-3) by reusing weights from smaller-sized pre-trained models belonging to the same LLM family. Our knowledge transfer based pre-training can be performed 2 times faster than traditional pre-training, and the resultant models achieve comparable performance on the GLUE evaluation benchmark.
- **Multi-layer Neural Composer for Personalized Product Descriptions** *(Fall 2017 and Spring 2018)*
  Investigated attention-based sequence-to-sequence language generation methods as a scalable approach for delivering personalized e-commerce product descriptions. Specifically, developed a multimodal learning method to refine product embeddings by collectively using image and text data.
- **Large-scale Video Understanding Using Deep Ensemble Networks** *(Spring 2017)*
  Developed a classifier to assign video content labels for the YouTube-8M dataset containing 8 million videos (multi-label classification). Used a combination of pre-trained feature encoders and a Mixture of Experts classifier to improve the Average Precision@k by 7% over the available baseline.

REVIEWER DUTIES

- **Conferences:** CVPR, ICCV, ECCV, ACCV, NeurIPS, ICLR, ICML, USENIX Security, IEEE S&P
- **Journals:** IEEE Transactions on Image Proc., IEEE Transactions on Info. Forensics & Security
- **Workshops:** TSRML @ NeurIPS 2022, EDSMLS @ AAAI 2020

TEACHING ASSISTANTSHIPS (STONY BROOK UNIVERSITY)

- CSE 508: Network Security *(Fall 2019 & Spring 2021)*
- CSE 527: Introduction to Computer Vision *(Spring 2019)*
- CSE 512: Machine Learning *(Fall 2018)*

AWARDS AND EXTRACURICULARS

- Best Poster Award Recipient, Graduate Research Day, *2023*
- Organizer, Adversarial Machine Learning Reading Group, *2022*
- Invited Speaker, IBM Security Group Seminar, *2021*
- Mentor, Women in Science and Engineering Lab Rotations, *2021*
- Organizing Committee, Graduate Research Day, *2021*
- Vice President, Computer Science Graduate Student Organization, *2020-2021*
- Editor, College Newsletter, *2015*
- Winner, National Competition on License Plate Recognition organized by Wipro Inc., *2015*
- Executive Board Member, Literary Affairs Committee, *2013-2015*