Ambar Pal

ambarpal.cs@gmail.com
cis.jhu.edu/∼ambar

Education

Ph.D. in Computer Science September 2018 - Present
Johns Hopkins University, Baltimore, MD, USA
- Advisors: René Vidal, Jeremias Sulam

MSE in Computer Science May 2023
Johns Hopkins University, Baltimore, MD, USA

B.Tech. (Honors) in Computer Science and Engineering July 2014 - May 2018
Indraprastha Institute of Information Technology, Delhi, India

Research Interests

I develop trustworthy machine learning systems that perform well under anomalous input or unseen categories. I have developed theory for techniques that utilize structure (e.g., low-dimensionality) in natural data to provide better robustness [1, 3, 2, 9], and applied these ideas to computer vision tasks like image classification [10, 6], action recognition, object detection [4], visual question answering [11], image captioning [12] as well as other tasks like graph classification [7]. Additionally, I also develop theory for regularization (dropout, dropblock) [8] and normalization (layernorm, batchnorm) techniques in deep learning.

Awards

CPAL Rising Star Award 2023
- Awarded to 16 individuals worldwide including PhD Students, Postdoctoral Fellows and Assistant Professors "who exemplify outstanding research potential for the Parsimonious Learning community"

Amazon AI2AI PhD Fellowship 2023
- Awarded to 4 students across JHU "based on outstanding publication record, research proposal and mentor support"

JHU MINDS Data Science Fellowship
Awarded for "outstanding work in the foundations of Deep Learning"
- 12 awardees across JHU 2022
  11 awardees across JHU 2021
  8 awardees across JHU 2019

IUSSTF-USC Viterbi Scholarship 2017
- Awarded to 19 students across India by the Indo-US Science and Technology Forum to undertake a research internship at the Viterbi School of Engineering, University of Southern California

AICTE INAE Travel Grant 2017
- Awarded by the All India Council of Technical Education - Indian National Academy of Engineering to present a paper at CVPR 2017.

- IIITD All Round Performance Medal 2018
  Awarded for "best overall performance in the CS Department".

- IIITD Dean's List for Academic Performance 2017, 2016

- IIITD Dean's Award for Research and Development 2017

Publications and Preprints

Provable Robustness

[1] **Pal, Ambar**, Vidal, René, Sulam, Jeremias, "Certified Robustness against Sparse Adversarial Perturbations via Data Localization". In: *arXiv preprint* (2024). LINK.

[2] **Pal, Ambar**, Sulam, Jeremias, "Understanding Noise-Augmented Training for Randomized Smoothing". In: *Transactions on Machine Learning Research* (2023). LINK.

[3] **Pal, Ambar**, Sulam, Jeremias, Vidal, René, "Adversarial Examples might be Avoidable: The Role of Data Concentration in Adversarial Robustness". In: *Advances in Neural Information Processing Systems* (2023). LINK.

[5] **Pal, Ambar**, Vidal, René, "Certified Defenses Against Near-Subspace Unrestricted Adversarial Attacks". In: *European Conference in Computer Vision Workshops* (2022). LINK.

[9] **Pal, Ambar**, Vidal, Rene, "A Game Theoretic Analysis of Additive Adversarial Attacks and Defenses". In: *Advances in Neural Information Processing Systems* (2020). LINK.

Theory of Deep Learning

[8] **Pal, Ambar**, Lane, Connor, Vidal, René, Haeffele, Benjamin D, "On the regularization properties of structured dropout". In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2020. LINK.

Empirical Robustness

[6] Raj, Ankita, **Pal, Ambar**, Arora, Chetan, "Identifying Physically Realizable Triggers for Backdoored Face Recognition Networks". In: *IEEE International Conference on Image Processing (ICIP)* (2021). LINK.

[7] **Pal, Ambar**, Hurtado, Julio, Nassar, Marcel, Ahmed, Nesreen K. Vidal, René, "Principled Attacks to Graph Neural Networks". In: (2020).

[10] **Pal, Ambar**, Arora, Chetan, "Making Deep Neural Network Fooling Practical". In: *IEEE International Conference on Image Processing (ICIP)*. 2018. LINK.

Object Detection, Visual Question Answering, and Others

[4] **Pal, Ambar**, Ramisa, Arnau, KC, Kumar Amit, Vidal, René, "On Utilizing Relationships for Transferable Few-Shot Fine-Grained Object Detection". In: *Amazon Computer Vision Conference* (2022). LINK.

[11] Ramakrishnan, Santhosh K, **Pal, Ambar**, Sharma, Gaurav, Mittal, Anurag, "An empirical evaluation of visual question answering for novel objects". In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2017. LINK.

[12] **Pal, Ambar**, Sharma, Gaurav, Arora, Chetan, "Exploiting independent visual and textual data sources to improve multi-modal methods for description and querying of visual data". In: *IIITD Bachelors Thesis Repository* (2016). LINK.

[13] Shah, Ayush, **Pal, Ambar**, Acharya, HB, "The Internet of Things: Perspectives on Security from RFID and WSN". In: *arXiv preprint* (2016). LINK.

[14] Wadhwa, Mohit, **Pal, Ambar**, Shah, Ayush, Mittal, Paritosh, "Rules in Play: On the Complexity of Routing Tables and Firewalls". In: *arXiv preprint* (2015). LINK.

Employment

Research Intern May 2022 - Aug 2022
Meta, Bellevue, WA, USA
- Theoretically studied the problem of training a large scale ML model under noisy gradients.
- Developed an optimization algorithm whose performance remains stable under malicious gradients.

Applied Scientist Intern June 2021 - Nov 2021
Amazon, Palo Alto, CA, USA
- Studied object detection in the low and corrupted training data regime.
- Proposed a probabilistic model for object detection based on external relationship knowledge.
- Improved performance on standard metrics while using a low amount of training data.

Research Intern May 2017 - Aug 2017
University of Southern California, CA, USA
- Surveyed the area of Survival Analysis with censored data.
- Proposed a smooth differentiable approximation of a commonly used evaluation metric.
- Analysed Deep Learning approaches to cancer prediction in a small data domain.

Research Scholar May 2016 - May 2017
IIT Kanpur, Kanpur, India
- Studied a setting of Image Captioning where the test images contain objects unseen during training.
- Proposed a dual LSTM based approach to incorporate information about the Novel classes.

Invited Talks

- The Role of Parsimonious Structures in Data for Trustworthy Machine Learning — January 2024
  Rising Star Talk at Conference on Parsimony and Learning, Hong Kong
- The Role of Structure in Data for Certified Robustness — October 2023
  Vision Lab Retreat, University of Pennsylvania
- The Role of Structure in Data for Trustworthy Machine Learning — October 2023
  Seminautonomous Seminar, University of California Berkeley
- Adversarial Robustness for Small-Norm and Large-Norm Attacks — July 2022
  Meta AI, Seattle
- A Game Theoretic Analysis of Adversarial Attacks and Defenses — July 2022
  Meta AI Research
- A Game Theoretic Analysis of Adversarial Attacks and Defenses — March 2022
  MINDS Retreat, Johns Hopkins University, Baltimore
- On the Regularization Properties of Structured Dropout — June 2020
  Pontificia Universidad Católica De Chile
- On the Regularization Properties of Structured Dropout — June 2020
  MINDS Seminar, Johns Hopkins University
- On the Regularization Properties of Structured Dropout — December 2019
  Computer Science Seminar, IIT Delhi, India

Teaching and Service

Teaching

- Teaching Assistant, Unsupervised Learning, JHU - Course taken by 20 graduate students
- Course Assistant, Machine Learning, JHU
- Teaching Assistant, Discrete Mathematics, IIIT Delhi - Course taken by 60 undergraduate students
- Teaching Assistant, Deep Learning, IIIT Delhi - Course taken by 20 students
- Instructor, INOI Workshop, IIIT Delhi - Taken by 100 students in preparation for the Indian National Olympiad in Informatics.

Professional Service

- Reviewing - Have been a reviewer for DeepMath 2023, 2020. NeurIPS 2023, 2022, 2021, 2020. JSP 2022. CVPR 2021. CDC 2020. ICLR 2020. JMIV 2018. ICVGIP 2019
- Mentoring - Have mentored (visiting) PhD student Julio Hurtado, (visiting) Masters Student Johannes Von Stetten, and several undergraduate students

Positions of Reponsibility

- Coordinator, Theory Group at IIITD. (2016 - 2018)
- Coordinator, Foobar, Programming Club at IIITD. (2015 - 2018)
- Lead Organizer, Progamming, Esya at IIITD. (2017, 2018)

Other Activities

Competitive Programming

- ACM ICPC - Represented IIIT Delhi thrice in the ACM ICPC South Asian Regionals at the Amritapuri and Chennai Sites.
- IOITC - Selected among 22 students across India for International Olympiad of Informatics Training and Team Selection camp for IOI, 2013. The IOI is the most prominent global programming contest at the high-school level.