AMBAR PAL

Johns Hopkins University

ambar@jhu.edu
cis.jhu.edu/∼ambar

EDUCATION

- **Johns Hopkins University** — Baltimore, Maryland, USA
  Ph.D. in Computer Science — September 2018 - Present
  - Advisors: *René Vidal*, *Jeremias Sulam*
- **Johns Hopkins University** — Baltimore, Maryland, USA
  MSE in Computer Science — May 2023
- **Indraprastha Institute of Information Technology Delhi** — Delhi, India
  B.Tech. in Computer Science and Engineering — July 2014 - May 2018

PUBLICATIONS & PREPRINTS

- "Adversarial Examples Might be Avoidable: The Role of Data Concentration in Adversarial Robustness" [PDF]
  Ambar Pal, Jeremias Sulam and René Vidal, In Neural Inf. Proc. Systems (**NeurIPS**) 2023 (To Appear)
  Poster in DeepMath 2023 (To Appear)
- "On the Need of Noisy-Training for Randomized Smoothing"
  Ambar Pal and Jeremias Sulam, In Transactions of Machine Learning Research (**TMLR**) 2023
  Poster in DeepMath 2022
- "Certified Defenses Against Near-Subspace Unrestricted Adversarial Attacks"
  Ambar Pal and René Vidal, In AROW Workshop, ECCV 2022
  Poster in Seeking Low Dimensionality in Deep Neural Networks, SLowDNN 2023
- "A Game Theoretic View of Additive Adversarial Attacks and Defenses" [PDF]
  Ambar Pal and René Vidal, In Neural Information Processing Systems (**NeurIPS**) 2020
- "On the Regularization Properties of Structured Dropout" [PDF]
  Ambar Pal, Connor Lane, René Vidal, Benjamin D. Haeffele, In **CVPR** 2020
- "Making Deep Network Fooling Practical" [PDF]
  Authors: Ambar Pal, Chetan Arora, In International Conference on Image Processing (**ICIP**) 2018
- "An Empirical Evaluation of Visual Question Answering for Novel Objects" [PDF]
  Santhosh Kumar R, Ambar Pal, Gaurav Sharma, Anurag Mittal, In **CVPR** 2017
- "Identifying Physically Realizable Triggers for Backdoored Face Recognition Networks" [PDF]
  Ankita Raj, Ambar Pal, Chetan Arora, In **ICIP** 2021
- "On Utilizing Relationships for Transferrable, Few-Shot Object Detection"
  Ambar Pal, Arnau Ramisa, Amit Kumar K C, René Vidal
  Short Paper in Amazon Computer Vision Conference (ACVC) 2022
- "Principled Attacks to Graph Neural Networks"
  Ambar Pal, Julio Hurtado, Marcel Nassar, Nesreen K. Ahmed, René Vidal
- "Cells in the Internet of Things" [PDF]
  Ayush Shah, H. B. Acharya, Ambar Pal
- "The Internet of Things: Perspectives on Security from RFID and WSN" [PDF]
  Ayush Shah, Ambar Pal, H. B. Acharya

AWARDS

- Amazon AI2AI Fellowship 2023
- JHU MINDS Data Science Fellowship 2022
- JHU MINDS Data Science Fellowship 2021
- JHU MINDS Data Science Fellowship 2019
- IUSSTF-USC Viterbi Scholarship 2017
- AICTE INAE Travel Grant 2017

- IIITD All Round Performance Medal 2018
- IIITD Dean's List for Academic Performance 2017
- IIITD Dean's Award for Research and Development 2017
- IIITD Dean's List for Academic Performance 2016

INTERNSHIPS

- **Meta, Bellevue, WA, USA** May 2022 – Aug 2022
  Research Intern (Supervisors: Mike Rabbat, Grey Yang, Xing Wang)
- **Amazon, Palo Alto, CA, USA** June 2021 – Nov 2021
  Applied Scientist Intern (Supervisors: Arnau Ramisa, Amit Kumar K C)
- **University of Southern California, CA, USA** May 2017 – Aug 2017
  Research Intern (Supervisor: Yan Liu)
- **IIT Kanpur, Kanpur, India** May 2016 – May 2017
  Research Scholar (Supervisor: Gaurav Sharma)

RESEARCH PROJECTS

- **Principled Adversarial Attacks and Defenses**
  Johns Hopkins University (René Vidal, Jeremias Sulam)
  - Studied adversarial attacks and defenses for Images, Video and Graph classifiers.
  - Proposed a game-theoretical framework for characterizing optimal attacks and defenses.
  - Proposed practical adversarial defenses for Video classifiers and Graph Neural Networks.
  - Proposed improvements to provable adversarial defenses like Randomized Smoothing.
- **Understanding Variants of Dropout**
  Johns Hopkins University (René Vidal)
  - Studied different variants of Dropout, which is a popular heuristic for training Neural Networks.
  - Understood the optimization and regularization properties of DropBlock.
  - Established an equivalence between DropBlock and DropConnect, and extended this theory to more general cases involving Deep Neural Networks and a wide class of Dropout schemes.
- **Understanding Training Stability for Recommendation Systems**
  Meta Research (Mike Rabbat, Grey Yang, Xing Wang)
  - 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.
- **Few Shot, Transferable Object Detection**
  Amazon (Arnau Ramisa, Amit Kumar K C)
  - 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.
- **Hacking Deep Neural Networks**
  IIIT Delhi (Chetan Arora)
  - Explored the problem of generating Fooling Images for DNNs trained for image classification.
  - Proposed an algorithm that generates Fooling Images with high noise robustness.
- **Automated Differential Attack on SHA-2**
  IIIT Delhi (Somitra Sanadhya)
  - Studied differential attacks on the cryptographic hash function, SHA-2 using searching techniques.
  - Implemented fast attacks, extensively documenting carry graph formation and difference propagation.
- **Methods for Survival Analysis**
  University of Southern California (Yan Liu)

- Explored the area of Survival Analysis with Censored Data, surveying existing work.
- Proposed a smooth differentiable approximation of a commonly used evaluation metric.
- Analysed Deep Learning approaches to cancer prediction in a small data domain.

- **Generating Captions for Novel Objects**
  IIT Kanpur (Gaurav Sharma)
  - 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.
  - Analysed how increase in lexical quality leads to drop in the novel-recall evaluation metric and vice-versa; proposed methods to neutralise the two trends. [PDF]

- **Planar Support for Hypergraphs**
  IIIT Delhi (Rajiv Raman)
  - Studied planar supports for hypergraphs whose hyperedges correspond to non-piercing planar regions.
  - Developed poly-time support constructions for some hypergraph-classes, improving upon existing exp-time algorithms.

- **Improving the Hough Transform Subspace Segmentation Algorithm**
  IIIT Delhi (Chetan Arora)
  - Worked to improve the Hough Transform Algorithm for detecting planes in a set of given points in 3D.
  - Introduced negative voting in the HT Algorithm for modelling points voting against a plane.

- **Structure and Security in the Internet of Things**
  IIIT Delhi (H. B. Acharya)
  - Characterised IoT into hierarchies by proposing "cells" as units of structure and context. [PDF]
  - Surveyed RFID and WSN security literature, compiling attacks and defenses relevant to IoT. [PDF]

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 conducted at the school level.
- **Teaching**
  - Teaching Assistant, Discrete Mathematics - Course taken by 60 second year undergraduates.
  - Teaching Assistant, Deep Learning - Course taken by 20 PhD, M.Tech. and B.Tech. students.
  - INOI Workshop - Taught techniques in Competitive Programming to a group of ∼100 school children to prepare them for the Indian National Olympiad in Informatics.
- **Talks**
  - Zero Knowledge Proofs[PDF] - Theory Group, IIIT Delhi.
  - Code Obfuscation[PDF] - Theory Group, IIIT Delhi.
  - Novel Image Captioning[PDF] - Computer Vision group, IIT Kanpur.
- **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).