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
  - Advisor: *René Vidal*
- **Indraprastha Institute of Information Technology Delhi** — Delhi, India
  B.Tech. in Computer Science and Engineering; **CGPA**: 9.91/10 — July 2014 - May 2018

PUBLICATIONS & REPORTS

- "A Game Theoretic View of Additive Adversarial Attacks and Defenses" [PDF]
  Authors: Ambar Pal, René Vidal
  Full Paper Accepted at Neural Information Processing Systems (**NeurIPS**), 2020
- "On the Regularization Properties of Structured Dropout" [PDF]
  Authors: Ambar Pal, Connor Lane, René Vidal, Benjamin D. Haeffele
  Full Paper Accepted at Computer Vision and Patter Recognition(**CVPR**), 2020
- "Making Deep Network Fooling Practical" [PDF]
  Authors: Ambar Pal, Chetan Arora
  Full Paper Accepted at 25th IEEE International Conference on Image Processing (**ICIP**), 2018
- "An Empirical Evaluation of Visual Question Answering for Novel Objects" [PDF]
  Authors: Santhosh Kumar R, Ambar Pal, Gaurav Sharma, Anurag Mittal
  Full Paper Accepted at Computer Vision and Patter Recognition(**CVPR**), 2017
- "Identifying Physically Realizable Triggers for Backdoored Face Recognition Networks" [PDF]
  Authors: Ankita Raj, Ambar Pal, Chetan Arora
  Full Paper Accepted at International Conference on Image Processing (**ICIP**), 2021
- "On Utilizing Relationships for Transferrable, Few-Shot Object Detection"
  Authors: Ambar Pal, Arnau Ramisa, Amit Kumar K C, René Vidal
- "Principled Attacks to Graph Neural Networks"
  Authors: Ambar Pal, Julio Hurtado, Marcel Nassar, Nesreen K. Ahmed, René Vidal
- "Cells in the Internet of Things" [PDF]
  Authors: Ayush Shah, H. B. Acharya, Ambar Pal
- "The Internet of Things: Perspectives on Security from RFID and WSN" [PDF]
  Authors: Ayush Shah, Ambar Pal, H. B. Acharya

AWARDS & SCHOLARSHIPS

- JHU MINDS Data Science Fellowship 2020
- JHU MINDS Data Science Fellowship 2019
- IUSSTF-Viterbi Scholarship 2017
- AICTE INAE Travel Grant 2017
- IIITD Dean's Award for Research and Development 2017
- IIITD Dean's List for Academic Performance 2017
- IIITD Dean's List for Academic Performance 2016

INTERNSHIPS

- **Amazon, Palo Alto, CA, USA** — June 2021 – Nov 2021
  Applied Scientist Intern (Supervisors: Dr. Arnau Ramisa, Dr. Amit Kumar K C)
- **Univeristy of Southern California, Los Angeles, CA, USA** — May 2017 – Aug 2017
  Research Intern (Supervisor: Dr. Yan Liu)

- **Indian Institute of Technology, Kanpur, India** May 2016 – Aug 2016
  Research Scholar (Supervisor: Dr. Gaurav Sharma)

RESEARCH EXPERIENCE

- **Principled Adversarial Attacks and Defenses** May 2019 – Present
  Johns Hopkins University (Dr. René Vidal, Dr. 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.
- **Few Shot, Transferable Object Detection** June 2021 – Nov 2021
  Amazon (Dr. Arnau Ramisa, Dr. 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.
- **Understanding Variants of Dropout** Sep 2018 – May 2019
  Johns Hopkins University (Dr. 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.
- **Methods for Survival Analysis** May 2017 – Aug 2017
  University of Southern California (Dr. 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** May 2016 – May 2017
  IIT Kanpur (Dr. Gaurav Sharma, Dr. Chetan Arora(IIIT Delhi))
  - 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]
- **Hacking Deep Neural Networks** July 2015 – May 2016
  IIIT Delhi (Dr. 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** Aug 2016 – Dec 2016
  IIIT Delhi (Dr. 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.
- **Planar Support for Hypergraphs** Aug 2017 – Aug 2019
  IIIT Delhi (Dr. Rajiv Raman)
  - Looking at the problem of finding planar supports for hypergraphs where the hyperedges correspond to non-piercing regions on a plane.
  - We have developed methods to construct planar supports for some classes of hypergraphs in polynomial time, a significant improvement over existing exponential time algorithms.
- **Improving the Hough Transform Subspace Segmentation Algorithm** Dec 2014 – Feb 2015
  IIIT Delhi (Dr. 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** Apr 2015 – May 2015
  IIIT Delhi (Dr. H. B. Acharya)
  - Attempted to characterise IoT into well defined hierarchies by proposing the concept of "cells" as units of structure and context. [PDF]
  - Surveyed existing literature on RFID and WSN security, compiling all known attacks and defenses relevant to IoT. [PDF]

ACADEMIC PROJECTS

- **Gesture Detection Glove**[SITE]
  - Created a glove capable of detecting and transforming hand gestures from sign language to english.
  - Used Arduino Uno as the microcontroller and manufactured flex sensors in-house at a cost less than 10% of the Market Price.
- **Digitised Document Fraud Detection**
  - Created a system using core CV techniques achieving 90% accuracy on fake document identification.
  - The work was funded by the Ministry of Electronics and Information Technology, Govt. of India. [LINK]
- **Pocket Git Server**
  - Used Open Source software to build a standalone Git server that can be deployed on a Mobile Phone.

SKILLS

- **Programming Languages** - Python, Lua, C++, C, R
- **Tools and Libraries** - Tensorflow, Torch, Caffe, Nvidia DIGITS, OpenCV

CO CURRICULAR ACTIVITIES

- **Competitive Programming**
  - ACM ICPC - Represented IIIT Delhi thrice in the ACM ICPC South Asian Regionals at the Amritapuri and Chennai Sites.
  - IOITC - Ranked among the 22 Indian students selected 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] - Delivered at Theory Group, IIIT Delhi.
  - Code Obfuscation[PDF] - Delivered at Theory Group, IIIT Delhi.
  - Novel Image Captioning[PDF] - Delivered at the Computer Vision group, IIT Kanpur.
- **Positions of Reponsibility**
  - Theory Group - Coordinator for IIITD's Theory Group 2016 - 2018.
  - Foobar - Coordinator for IIITD's Programming Club, Foobar 2015 - 2018.
  - Esya - Lead organiser for Programming events in IIITD's annual technical fest, Esya.
- **Chess**
  - I am an active member of the Chess Club and frequently play on online Chess websites.
  - Our team won the chess event conducted as a part of the inter-college sports meet, Triquetra 2017.