VASU SINGLA

vasusingla.github.io
+1-240-470-9952 ⋄ vsingla@cs.umd.edu

RESEARCH STATEMENT

My research interests have been focused on generative models, security, and attribution of machine learning systems.

EDUCATION

University of Maryland, College Park *August 2021 - Present*
Ph.D. in Computer Science
Advisor: Dr. Tom Goldstein, Dr. David Jacobs

University of Maryland, College Park *August 2019 - Present*
M.S in Computer Science GPA: 4.0/4.0

Punjab Engineering College, Chandigarh *July 2014 - June 2018*
B.Tech. + Minors GPA: 8.2/10

PUBLICATIONS

* denotes equal contribution

- **A Simple and Efficient Baseline for Data Attribution on Images**
  Vasu Singla, Pedro Sandoval-Segura, Micah Goldblum, Jonas Geiping, Tom Goldstein
  Under Review
  NeurIPS 2023 ATTRIB Workshop (Short-Version)
- **Why Diffusion Models Memorize and How to Mitigate Copying**
  Gowthami Somepalli, **Vasu Singla**, Micah Goldblum, Jonas Geiping, Tom Goldstein
  NeurIPS 2023
- **What Can We Learn from Unlearnable Datasets?**
  Pedro Sandoval-Segura, **Vasu Singla**, Jonas Geiping, Micah Goldblum, Tom Goldstein
  NeurIPS 2023
- **Learning with noisy labels using low-dimensional model trajectory**
  Vasu Singla, Toshiaki Koike-Akino, Matthew Brand, Kieran Parsons, Shuchin Aeron, Ye Wang
  NeurIPS 2022, DistShift Workshop (Short-version)
- **Diffusion Art or Digital Forgery? Investigating Data Replication in Diffusion Models**
  Gowthami Somepalli, **Vasu Singla**, Micah Goldblum, Jonas Geiping, Tom Goldstein
  CVPR 2023
- **Autoregressive Perturbations for Data Poisoning**
  Pedro Sandoval-Segura*, **Vasu Singla***, Jonas Geiping, Micah Goldblum, Tom Goldstein, David Jacobs
  NeurIPS 2022
- **Poisons that are learned faster are more effective**
  Pedro Sandoval-Segura, **Vasu Singla**, Liam Fowl, Jonas Geiping, Micah Goldblum, David Jacobs, Tom Goldstein
  CVPR 2022 The Art of Robustness Workshop

- **Shift Invariance Can Reduce Adversarial Robustness**
  Vasu Singla*, Songwei Ge*, Ronen Basri, David Jacobs
  NeurIPS 2021
  ICLR 2021, Safety and Security in Machine Learning Systems (Short-version)
- **Low Curvature Activations Reduce Overfitting in Adversarial Training**
  Vasu Singla, Sahil Singla, Soheil Feizi, David Jacobs
  ICCV 2021
  ICLR 2021, Safety and Security in Machine Learning Systems (Short-version)
- **ASAP NMS - Accelerating Non-Maximum Suppression Using Spatially Aware Priors**
  Rohun Tripathi*, **Vasu Singla*** , Bharat Singh, Mahyar Najibi, Abhishek Sharma, Larry Davis.
  Tech Report

RESEARCH EXPERIENCE

Cruise - Research Intern *Jan 2023 - May 2023*

- Working on developing novel applications of diffusion models for Autonomous Vehicle systems.

Mitsubishi Electric Research Labs - Research Intern *June 2022 - Aug 2022*

- Proposed new optimization algorithms to improve accuracy on datasets with noisy labels. Explored the role of data quality and labels on the robustness of ML systems.

Apple - Research Intern *June 2021 - Aug 2021*

- Among the **top-8 out of 100s of interns** selected to present work to the Senior VP of AI/ML Organization at Apple.
- Proposed new data augmentation techniques to boost performance on low-resource accents for Automatic Speech Recognition models.

University of Maryland - Research Assistant *January 2019 - Present*

- Worked with Prof. David Jacobs and Prof. Tom Goldstein on adversarial examples, data poisoning, and data attribution.

Indian Institute of Technology (IIT), Bombay - Research Staff *January 2019 - July 2019*

- Developed a novel system for automated symbol detection, text detection and object association in documents for structured parsing, analysis and information retrieval.

AWARDS

UMD Dean's Fellowship, ICLR 2021 Travel Award, NeurIPS 2023 Travel Award

ACADEMIC SERVICE

Reviewer Conferences - CVPR 2022, ECCV 2022, CVPR 2023, ICCV 2023, NeurIPS 2023, ICLR 2024
Reviewer Journals - CVIU, Pattern Recognition Letters
Volunteer Services - ICML 2021, NeurIPS 2023, Peer Mentoring Service @ UMD