Vinu Sankar Sadasivan

III-year PhD Student
Department of Computer Science
The University of Maryland, College Park
Research Interests — AI/ML Security & Privacy, GenAI

vinusankars.github.io
vinu@umd.edu
Google Scholar

Education

The University of Maryland, College Park — *Aug '21 – Apr '26 (Expected)*
Ph.D. & M.S. in CS advised by Prof. Soheil Feizi — GPA - 4.00/4.00

Indian Institute of Technology, Gandhinagar — *Jul '16 – Jul '20*
B. Tech. in CSE [Director's Silver Medalist] — GPA - 9.21/10.00

Research Papers

* equal contribution

Can AI-Generated Text be Reliably Detected?
VS Sadasivan, A Kumar, S Balasubramanian, W Wang, S Feizi
Preprint on arXiv. March, 2023. [PDF]
Media Coverage: Washington Post, Wired, New Scientist, The Register, TechSpot

Exploring Geometry of Blind Spots in Vision Models
S Balasubramanian*, G Sriramanan*, **VS Sadasivan**, S Feizi
Accepted (spotlight) at Neural Information Processing Systems (NeurIPS), 2023. [PDF]

Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks
M Saberi, **VS Sadasivan**, K Rezaei, A Kumar, A Chegini, W Wang, S Feizi
Preprint on arXiv. September, 2023. [PDF]
Media Coverage: Wired, The Verge, MIT Technology Review, Bloomberg, The Register

Provable Robustness for Streaming Models with a Sliding Window
A Kumar, **VS Sadasivan**, S Feizi
Preprint on arXiv. March, 2023. [PDF]

CUDA: Convolution-based Unlearnable Datasets
VS Sadasivan, M Soltanolkotabi, S Feizi
Accepted at Computer Vision and Pattern Recognition Conference (CVPR), 2023. [PDF]

Statistical Measures For Defining Curriculum Scoring Function
VS Sadasivan, A Dasgupta
Accepted (spotlight) at SubSetML Workshop at International Conference on Machine Learning (ICML), 2021. [PDF]

Shallow RNN: Accurate Time-series Classification On Resource Constrained Device
D Dennis, DAE Acar, V Mandikal, **VS Sadasivan**, V Saligrama, HV Simhadri, P Jain
In Advances in Neural Information Processing Systems (NeurIPS), 2019. [PDF]

High Accuracy Patch-Level Classification Of Wireless Capsule Endoscopy Images Using A Convolutional Neural Network
VS Sadasivan, CS Seelamantula
In IEEE 16^{th} International Symposium on Biomedical Imaging (IEEE ISBI), 2019. [PDF]

Invited Talk

Google Research, Bangalore – Hardness of AI text detection — *Nov '23*

Research Experiences

UMD, College Park — *Aug '21 – Present*
Research Assistant in CS — Advisor: Prof. Soheil Feizi

IIT Gandhinagar, India — *Aug '20 – Jul '21*
Junior Research Fellow in CSE — Advisor: Prof. Anirban Dasgupta

California Institute of Technology, Pasadena — *May – Jul '19*
Undergraduate Research Fellow in Astronomy Department — Advisor: Dr. Ashish Mahabal

Microsoft Research India, Bangalore — *Jan – Apr '19*
Research Intern in Machine Learning and Optimization Group — Advisors: Dr. Harsha Simhadri & Dr. Prateek Jain

Indian Institute of Science (IISc), Bangalore — *May – Jul '17, Dec '17, Feb '18, May – Jul '18*
Research Intern at Spectrum Lab for Signal Processing — Advisor: Prof. Chandra Seelamantula

Awards And Honors

Kulkarni Fellowship Awardee at University of Maryland in 2023.

Notable reviewer top $\sim 1\%$ reviewer in ICLR 2023.

Director's Silver Medalist CSE, IIT Gandhinagar in 2020.

Special mention for poster Undergraduate Research Conclave, IIT Gandhinagar in 2019.

Summer Undergraduate Research Fellow Caltech in 2019 ($\sim$ 6350 USD).

Kerala State Topper, Regional Mathematics Olympiad in 2014.

KVPY awardee by Government of India in 2016. Ranked 85 out of $\sim 100,000$.

NTSE scholar awarded by Government of India in 2012.

Services & Teaching

Reviewer for prominent machine learning conferences such as ICML 2021, NeurIPS 2022, ICLR 2023 (Notable reviewer), NeurIPS 2023, ICML Neural Compression Workshop 2023.

Teaching assistant for CMSC 422: Introduction to Machine Learning (Fall 2021) and CMSC 320: Introduction to Data Science (Spring 2022) at UMD.

Peer-assisted learning mentor at IIT Gandhinagar, helping freshmen who found it difficult to cope with their academic workload.

Research Reports

OSSuM: A Gradient-Free Approach For Pruning Neural Networks At Initialization
VS Sadasivan, J Malaviya, and A Dasgupta [PDF]

Improved Generalized Adaptive Exponential Functional Link Network Approximates
VS Sadasivan, SS Bhattacherjee, V Patel, and NV George [PDF]

FPGA-Based Area, Power, and Latency Optimized Approximate Multipliers For Neural Networks
VS Sadasivan, CK Jha, and J Mekie [PDF]