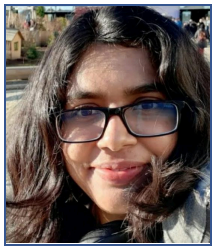
Harshitha Machiraju

+41 78 259 40 25 code-Assasin

harshitha.machiraju@epfl.ch www.linkedin.com/in/harshitha-machiraju



About Me

I am a **Machine Learning Researcher** focused on enhancing the robustness of neural networks by evaluating and addressing challenges posed by **adversarial** perturbations, **image corruptions**, and **background** variations. Recently awarded a **PhD** from EPFL under the supervision of Prof. Pascal Frossard and Prof. Michael Herzog, I have developed various methodologies to uncover **biases** and fortify the **robustness** of deep neural networks to **distribution shifts**.

Education

Sep. 2019 - Apr. 2024	**PhD in Machine Learning** - *EPFL, Switzerland* Advisors : Prof. Pascal Frossard & Prof. Michael Herzog
Jul. 2014 - Aug. 2018	**B.Tech in Electrical Eng.** - *IIT Hyderabad, India* ***Summa cum Laude*** & Minor in Comp. Sci

Experience

Sep. 2019 - Apr. 2024	**Doctoral Assistant** *at EPFL, Switzerland* Conducted research on enhancing the **robustness** of vision models against diverse **out-of-distribution** inputs, including **image corruptions, background** and **adversarial** alterations
Sep. 2018 - Aug. 2019	**Research Assistant** *at IIT Hyderabad, India* Conducted research on designing better **adversarial attacks** to emulate realistic **weather** conditions to assess the **robustness** of **autonomous navigation** systems.
Jul. 2018 - Aug. 2018	**Research Intern** *at UNIST, S. Korea* Conducted research to establish a better relationship between topology of latent representations and model predictions.

Projects

- **Test time Input Processing against Image Corruptions:** Proposed EREN, a novel, **differentiable image processing algorithm** tailored to the **spectral biases of models.** EREN enhances model robustness against **diverse image corruptions** and achieves **superior** performance.
- **Automating Out-of-Distribution Sample Generation by Leveraging Model Biases:** Proposed MUFIA, an innovative algorithm **automating the generation of out-of-distribution samples** by harnessing model **spectral biases**. This work represents a significant advancement in the field, characterized by its utilization of spectral biases for the generation of adversarial image corruptions.
- **Efficient Contrastive Learning Approach for Mitigating Background Bias:** Proposed CLAD, a novel and efficient contrastive learning approach that achieved **State-of-the-Art** on the **Background** challenge dataset. Work published at **BMVC**.
- **Uniform Robustness Evaluation of bio-inspired models:** Developed a novel testbed to evaluate the performance of biologically inspired vision models, specifically to account for the robustness against

out-of-distribution samples. This work helped set the standard in the field to align model quality between researchers. The evaluation pipeline is available on GitHub and was presented at ***CVPR*** NeuroVision 2022.

- **Generation of adversarial foggy images for Robustness Evaluation:** Pioneered **GAN-**based creation of adversarial foggy images, marking the forefront of **adversarial weather attack** exploration within this domain. Work published at **WACV**.
- **Metric design for Robustness Evaluation under varying Weather Conditions:** Pioneered a new metric to gauge the **robustness** of **object detection networks** within navigation systems across diverse weather conditions. **Oral presentation** at **ICIP**.
- **Enhancing Neural Network Robustness via Latent Perturbations:** Proposed a novel **adversarial training** method based on perturbations in the latent space to increase the robustness of neural networks. Work published at **IJCAI**.

Selected Publications

- **HM**, M. Herzog, P. Frossard, "Eren: Enhancing deep learning robustness through image pre-processing," (Under Review), 2024.
- **HM**, M. Herzog, P. Frossard, "Frequency-based vulnerability analysis of deep learning models against image corruptions," (Under Review), 2023.
- **HM,** O. Choung, M. Herzog, P. Frossard, "Empirical advocacy of bio-inspired models for robust image recognition," **CVPR** NeuroVision Workshop, 2022.
- K. Wang, **HM**, O. Choung, M. Herzog, P. Frossard, "CLAD: A contrastive learning based approach for background debiasing," **BMVC**, 2022.
- **HM**, V. Balasubramanian, "A Little Fog for a Large Turn," **WACV**, 2020.
- N. Kumari, M. Singh, A. Sinha, **HM**, B. Krishnamurthy, V. Balasubramanian, "Harnessing the Vulnerability of Latent Layers in Adversarially Trained Models," **IJCAI**, 2019.
- **HM**, S. Channappayya, "An Evaluation Metric for Object Detection Algorithms in Autonomous Navigation Systems and its Application to a Real-time Alerting System," **ICIP**, 2018 (Oral).

*Complete List on Google Scholar

Skills

Programming	Python, C, C++, Java, Matlab
Frameworks	Pytorch, Tensorflow, Seaborn, Matplotlib, Sklearn, Git, Latex, Illustrator
Languages	English (Fluent), French (Basic), Korean (Int.), Hindi (Native), Telugu (Native)

Awards and Recognition

- Qualified for **JICA Scholarship**, 2018.
- **JENESYS Scholarship** 2017.
- **Special Recognition for a Young Team**, IEEE SP CUP, 2016.
- **Top 10 teams of IEEE SP CUP**, 2016.
- **Academic Excellence Award**, IIT Hyderabad, 2014.
- Qualified for **KVPY** 2013.

Community Service

- **Reviewer** for ECML, CVPR, TIP, ICVGIP.
- **TA** for Signal Processing & Deep Learning courses.
- **Supervision** of many Masters students projects.

Personal Interests

- Strength Training, Music, Cooking.