Varunkumar Hiregoudar

8217621750 | varunkumarsh369@gmail.com | github | linkedin

Education

KLE Technological University — Hubli, Karnataka
BE CS CGPA (as of 6th Semester) - 9.14 — *Nov. 2022 – May 2026*

Vidyaniketan PU Science College — Hubli, Karnataka
12th Percentage - 96.6 — *June. 2020 – May 2022*

JSS Shri Manjunatheshwara Central School — Dharwad, Karnataka
10th Percentage - 89.8 — *Aug. 2016 – March 2020*

Technical Skills

Languages: Python, C/C++, JavaScript, Bash
Libraries: NumPy, Pandas, Matplotlib, PyTorch, OpenCV, NLTK, Torchvision, Sklearn, Transformers
Frameworks & Databases: Express.js, Node.js, React, MySQL, MongoDB
Development and Tools: HTML, CSS, JavaScript, GIT, Docker

Projects

Improving Robustness of Deep Neural Networks against Adversarial Attacks — Sep. 2024 – Jan. 2025

- Effectively combined Label smoothing, RAILS and per-layer Jacobian Regularization to improve adversarial robustness of DNNs.
- Tested on multiple white-box adversarial attacks on MNIST dataset.
- Evaluated the effectiveness of the defense regarding the tradeoff between clean and adversarial accuracies.

Student Classroom Allocation for In-Semester Examination — Nov. 2024 – Dec. 2024

- Built the logic to dynamically allocate students to available classrooms and determine appropriate question paper count.
- Developed a web-based system for student classroom allocation during in-semester exams.
- Built the backend using Node.js and Express, integrating MySQL for data management.
- Designed a dynamic frontend with React to display real-time seat arrangements.

Text-Based 3D Object Retrieval — Sep. 2024 – Present

- Developed a contrastive learning solution for efficient retrieval of 3D objects through view-based approach.
- Constructed 3 feature extractors for different modalities. Text : CLIP encoder. Ringview images : Blender, EfficientNetv2, Transformer encoder. 3D Object : PointNet
- Implemented a common shared vector space for the feature vectors of all the modalities to determine similarity
- Optimized similarity calculation to handle 3 separate modalities and determine the similarity through training.
- Evaluating on an only animal dataset ANIMAR, trying to achieving competitive results against state-of-the-art models.

Publications

Improving Robustness of DNNs Against Adversarial Attacks using RAILS, Jacobian Regularization, and Label Smoothing

- Proposed a defense mechanism to improve robustness of DNNs against adversarial attacks.
- Developed the defense mechanism by including RAILS together with per-layer Jacobian Regularization on smoothened labels.
- Demonstrated resilience against FGSM and PGD attacks, effectively managing the clean data and adversarial accuracy tradeoff.
- Published in Springer Lecture Notes in Networks and Systems. Presented at CRM2025, SR University, Warangal (Feb 01-02, 2025)