Susim Mukul Roy

Email : susimmuk@buffalo.edu
Number : +918777717647

Linkedin — Github — Wesbite

Education

University at Buffalo, NY, USA
Incoming Masters of Science in Computer Science and Engineering — *Expected: August 2024*

Indian Institute of Technology Jodhpur, India — **CGPA - 8.48/10**
Bachelors of Technology in Artificial Intelligence and Data Engineering — *December 2020 - May 2024*

Research Experience

- **Indian Institute of Technology, Jodhpur, India**
  Undergraduate Student Researcher - IAB Lab, ***Advisors:*** *Prof. Richa Singh & Prof. Mayank Vatsa* *[Aug 2022 - May 2024]*
  - Established a comprehensive study for the impact of White/Black-Box Adversarial Attacks on different SOTA CNNs and Transformers (ViT & Swin) upon various Vision Benchmarks (MNIST, CiFAR10 & ImageNet200).
  - Designed a self-supervised two-stage pipeline for detecting an intentionally-created attack against a natural unintentional noise (JPEG Compression & Gaussian Blur) on EuroSAT Dataset via the MMD loss function.
  - Investigated the role of foundation models like DDPM, SDE etc. in purification of adversarial perturbations like evasion, poisoning attacks for the development of novel transferable attack utilizing diffusion techniques.
  - A comprehensive analysis of the areas of focus of each network backbone(in addition to the traditional metrics) in presence of l-norm attacks on classification tasks via GradCAM and saliency maps for distinguishable visualization.
  - Technologies Used: **PyTorch, ART, HuggingFace, RobustBench, CleverHans**

- **University of Alberta, Edmonton, Canada**
  MITACS Visiting Researcher - Vision and Learning Lab, ***Advisors:*** *Prof. Li Cheng* *[May 2023 - August 2023]*
  - Worked at the main office of *Super GeoAI* in *University of Saskatchewan* and coordinated with Dr.Weiping Zeng for data collection, annotation, and analysis to create a extensive and varied plant dataset for the company.
  - Improving existing object detection models like *EfficientDet* through self-attention mechanism and selective feature propagation to the Bi-FPN for accurate wheat-head growth stage detection by analysis of it's physical properties and finetuning *Yolov8* by large number of experiments for high-precision canola flower count.
  - Spearheaded the deployment of the trained models through AWS for demo on their website for real-time usage.
  - Technologies Used: **AWS, Pytorch, Javascript, XML, Ultralytics, SCVAT**

- **Indian Institute of Technology, Guwahati, India**
  Research Intern - Vision Intelligence Lab, ***Advisor:*** *Dr. Santosh Kumar Vipparthi* *[May 2022 - Jan 2023]*
  - Creating an extensive literature survey on work done in MOS like analyzing SOTA models like Referformer, MTTR etc. and determining the computational effectiveness of their usage for high fps videos.
  - Proposed an inter-frame movement detector (IFCD) module, which extracts the movement information between the consecutive frames and helps integrate temporal information with spatial visual features
  - Developed a novel CNN-based architecture using an encoder-decoder module, DeepLab-V3 model and text encoders like BERT thereby facilitating late feature fusion and reducing the space and time complexity from previous works.
  - Technologies Used: **PyTorch, OpenCV, Pycocotools**

- **University of Seigen, Seigen, Germany**
  Research Intern - Learning2Sense, ***Advisor:*** *Prof. Michael Moeller* *[August 2023 - Jan 2024]*
  - Did a theoretical analysis on non-uniform noise modelling for the *sinogram* generated from forward propagation algorithm for CT Images via the Beer-Lambert law and researched on existing methods to model the same.
  - Worked on suitable reconstruction technique for the noisy images(*Poisson/Gaussian*) like *FPB* for ULDCT with a constrained loss function and a parameterized version of the pixel intensities for a smoother convergence.
  - Technologies Used: **PyTorch, ASTRA Toolbox, Matplotlib**

Publications

- ***RefMOS: A Robust Referred Moving Object Segmentation framework based on text query*** (Accepted — paper, code)
  Saxena, PP., **Roy, S.**, Tyagi, DK., ,Vipparthi, SK., Balasubramanian, R., Murala, S.
  2024. 25th IEEE International Conference on Advanced Video and Signal-Based Surveillance(AVSS' 24).

Projects

Vulnerability of Diffusion Models to Adversarial Attacks
*Bachelor's Dissertation — **Advisors:** Prof. Mayank Vatsa & Prof. Richa Singh* *[Aug 2023 - Feb 2024]*

- Conducted an extensive literature survey of generative models employed for purification of adversarial attacks along with challenges incurred by each technique in terms of vanishing/exploding gradient, memory costs and randomness.
- Developed a novel adversarial attack using the Class-Activation Maps of classifiers and the predicted residual maps from the UNet model of a DDPM which successfully fools the classifiers in terms of ASR, Robust accuracy and FID.
- Carried out thorough experiments on the CelebA-HQ and CIFAR-10 dataset for maximizing the extraction of relevant information from the residual map such that they remain gaussian on testing with the Kolmogrov-Smirnoff test.
- Technologies Used: **PyTorch, HuggingFace, RobustBench**

A Sequential Memory Preserving Approach for Few-Shot Image Classification Project Link
*Adv. ML Course Project, IIT Jodhpur — **Advisor:** Prof. Mayank Vatsa* *[Aug 2023 - Dec 2023]*

- Modelled the meta-training set as the combination of all the individual task specific training sets instead of a multi-task setting such that our network has a large feature space to learn a good embedding model as far as possible.
- We apply the Matching Feature Hierarchy(MFH) module on each output feature map of the layers of our backbone in a hierarchical manner followed by the Memory Wrap Module which helps in discarding the sparse attention weights.
- Achieved a classification accuracy of almost 80% on the 5-shot miniImagenet dataset and 72% on the 1-shot CIFAR-FS dataset which is a bit better than certain 2020 SOTA baselines like MetaOptNet.
- Technologies Used: **PyTorch, Tensorboard**

Detecting Adversarial Perturbations While Determining their Intention [Submitted at ECCVw]
*UG Research Project — **Advisors:** Prof. Mayank Vatsa & Prof. Richa Singh* *[Aug 2022 - Sept 2023]*

- We propose a class-independent detection method, CIAI, using Maximum Mean Discrepancy along with Center-based loss to group together similar images and produces a 3-class output using five types of image variations as input.
- We show how both types of noises affect the classification accuracy for gender prediction on the CelebA dataset and the detection accuracy of intentional vs unintentional often exceeds the previous SOTA methods in different settings.
- Visualized the important features for understanding how the detector differentiates between noises using attention maps from the last multi-head attention layer of the Vision Transformer in the prediction of gender on CelebA.
- Technologies Used: **PyTorch, Pytorch-Lightning, OpenCV**

Autonomous UAV-UGV Navigation(Inter-IIT 2k22) Project Link
Inter-IIT Techfest 2022 *[Jan 2022 - Feb 2022]*

- Designed a shortest time algorithm with the help of KMeans to move an UAV on a mountainous terrain with no texture and thereby made a UGV accurately follow the recorded path to the destination.
- Used top-view depth image to segment between road and terrain following which we binarized the world into two classes and drew a line joining the midpoints of the road which the UAV follows as it moves ahead.
- Used *ROSBags* to record messages from UAV and scaled them down to prius messages for UGV movement.
- Technologies Used: **ROS, OpenCV, Gazebo, Mavros, Ardupilot**

Technical Skills

- **Programming**: Python, C/C++, JAVA, JavaScript, MATLAB, SQL, ROS, LaTeX
- **Machine and Deep Learning Tools**: Scikit-Learn, Numpy, Pandas, Matplotlib, Seaborn, PyTorch, Tensorflow, OpenCV, Hugging Face, ASTRA Toolbox
- **Tools & Softwares**: Docker, Kubernetes, SCVAT, Gazebo, Moveit, RVIZ, NS-3, GIT

Teaching and Volunteering Experience

- **Teaching Assistantship:** Served as a teaching assistant at IIT Jodhpur for 200+ Sophomore & Junior year students, conducting weekly lab and viva sessions, preparing assessments and grading them for the following courses:
  - Pattern Recognition and Machine Learning(Under Dr. Richa Singh and Dr. Pratik Mazumder) [*Jan '23 - May '23*]
  - Deep Learning(Under Dr. Angshuman Paul) [*Jan '24 - May '24*]
- **Volunteering Experience:**
  - **Captain** of *Robotics Society* [*Dec '21 - Feb '23*]
    Overall Management of society by organising sessions on ML, ROS, Mechanics of robots etc. along with leading different teams for inter-collegiate competitions and mentoring society members in club projects.
  - **Subsection Head** of Team IITJ for *ABU-Robocon'22* [*Nov '21 - Apr '22*]
    Integrating AI with ROS for proper detection of disks to perform the necessary path planning of the Lagori Robots.