Hashmat Shadab Malik

Profile · hashmat.malik@mbzuai.ac.ae · Google Scholar · GitHub ·

Education

2023 - Present | **PhD.** in Computer Vision
Mohamed bin Zayed University of Artificial Intelligence (MBZUAI)
Gpa: **3.90/4.0**, *First Class Honours.*

2021 - 2022 | **Master** of Science in Computer Vision
Mohamed bin Zayed University of Artificial Intelligence (MBZUAI)
Thesis: "Adversarial Pixel Restoration as a Pretext Task for Transferable Perturbations."
Gpa: **4.0/4.0**, *First Class Honours.*

2014 - 2018 | **Bachelor** of Technology in Electronics and Communication Engineering
National Institute of Technology, Srinagar (NIT)
Thesis: "Channel Estimation for Wireless Communication systems, using least-square method."
Gpa: **8.48/10.0**, *First Class Honours.*

Work Experience

Jan.2021 - Present | *Graduate Research Assistant* **Intelligent Visual Analytics Lab (IVAL), MBZUAI, Abu Dhabi**, UAE
Working on evaluating robustness of uni-modal and multi-modal vision-based models.

Mar.2019 - Jun.2019 | *Research Intern* **Robotics Research Center - IIIT Hyderabad**, India
Worked on Motion segmentation and estimating depth from multiple views for autonomous navigation of cars using deep network based framework.

Jul.2018 - Mar.2019 | *Computer Vision Engineer* **Cingularity TEC India Pvt. Ltd.**, Bangalore, India
Built Computer Vision Systems involving License Plate Recognition, Vehicle Recognition and Counting vehicles in malls and parking lots.

Jul.2018 - Mar. 2019 | *Project Assistant* **Computational Intelligence Lab- IISc**, India
Developing frameworks using deep convolutional neural networks for classification/detection of diseases in Sugarcane. Implementing models to detect different type of damages in vehicles.

Research Interests

Intrigued by the vulnerability of deep neural networks, my research focuses on the Safety and Reliability of AI, with a particular emphasis on understanding, evaluating, and enhancing the robustness of vision-based models.

Selected Publications

Google Scholar

FaceGuardian: Protecting Facial Biometrics from Malicious Generative Editing via Latent Optimization **(Under Review)**.

Robust-LLaVA: On the Effectiveness of Large-Scale Robust Image Encoders for Multi-modal Large Language Models **(Under Review)**. [Paper] [Code]

Hierarchical Self-Supervised Adversarial Training for Robust Vision Models in Histopathology. Accepted at International Conference on Medical Image Computing and Computer Assisted Intervention **(MICCAI 2025)**. [Paper] [Code]

Towards Evaluating the Robustness of Visual State Space Models. Accepted in Workshop of Adversarial Machine Learning on Computer Vision: Foundation Models + X at **CVPR 2025**. [Paper] [Code]

ObjectCompose: Evaluating Resilience of Vision-Based Models on Object-to-Background Compositional Changes. Accepted at Asian Conference on Computer Vision **(ACCV 2024-Oral)**. [Paper] [Code]

On Evaluating Adversarial Robustness of Volumetric Medical Segmentation Models. Accepted at The British Machine Vision Conference **(BMVC 2024)**. [Paper] [Code]

Adversarial Pixel Restoration as a Pretext Task for Transferable Perturbations. Accepted at The British Machine Vision Conference **(BMVC 2022–Oral)**. [Paper] [Code]

Academic Service

Reviewer ECCV, BMVC, WACV, CVPR, MICCAI

Honors and Awards

Dec. 2024 Secured Best Student Paper Honorable Mention Award at ACCV 2024.

Jan. 2023 **PhD** Awarded Research Scholarship by Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) for the period of four years.

Jan. 2021 **MSc.** Awarded Postgraduate Research Scholarship by Mohamed bin Zayed University of Artificial Intelligence (MBZUAI) for the period of two years.

Jun. 2018 Qualified National Level Graduate Aptitude Test in Engineering(GATE).

Jun. 2018 Among top 15 percentile of the class of Bachelors in Electronics and Communication.

Jun. 2014 Qualified National Level Joint Engineering Entrance(JEE) for admission into NITs.

Jun. 2013 15th Position in the State Level Board Exam of grade XII.

Computational Skills

Python Expert Knowledge- I am extensively using python to build novel machine learning algorithms for the last few years.

Pytorch Pytorch is usually my default choice due to its dynamic nature and object-oriented graph design approach.

Keras I have used Keras with Tensorflow before and have gained decent familarity with it.

Matlab Most of my Bachelor projects have been done using Matlab.

C I scored A grades in the language in my B.Tech course.

References

Dr. Salman Khan (Primary Supervisor)
Associate Professor at the Mohamed bin Zayed University of Artificial Intelligence (MBZUAI),
✉ salman.khan@mbzuai.ac.ae, Personal Web

Dr. Fahad Shahbaz Khan (Secondary Supervisor)
Professor at the Mohamed bin Zayed University of Artificial Intelligence (MBZUAI),
✉ fahad.khan@mbzuai.ac.ae, Personal Web

Dr. Muzammal Naseer
Assistant Professor at Khalifa University,
✉ muhammadmuzammal.naseer@ku.ac.ae, Personal Web