

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 , <i>First Class Honours</i> .
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 , <i>First Class Honours</i> .
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 , <i>First Class Honours</i> .

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 in both i.i.d and non-i.i.d settings, I am focused on designing methods and benchmarks to expose their limitations and uncover deeper insights into their weaknesses.

SELECTED PUBLICATIONS

[GOOGLE SCHOLAR](#)

Hierarchical Self-Supervised Adversarial Training for Robust Vision Models in Histopathology (Under Review).

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

Towards Evaluating the Robustness of Visual State Space Models (Under Review). [\[Paper\]](#) [\[Code\]](#)

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). [\[Paper\]](#) [\[Code\]](#)

Object Detection in Aerial Images: What Improves the Accuracy?, Accepted for WIUT-UoW Computing Conference (2022) [\[Paper\]](#)

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 familiarity 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,
✉ muhhammadmuzammal.naseer@ku.ac.ae, 🌐 [Personal Web](#)