Muhammad Huzaifa

✉ muhammad.huzaifa@mbzuai.ac.ae Linkedin Github Website

Education

Master of Science in Machine Learning **Aug 2022 – June 2024**

Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi *GPA - 3.73/4.00*

- Graduate research student supervised by Dr. Fahad Khan and Dr. Salman Khan
- MS Research: ”Robustness of Vision and Language models using Generative AI (Diffusion Models)”
- Major Courses: Trustworthy AI, Natural Language Processing, Probabilistic Machine Learning

Bachelor of Electrical Engineering **Sept 2017 – Aug 2021**

National University of Science and Technology (NUST), Islamabad, Pakistan

- Undergraduate student supervised by Dr. Latif Anjum and Dr. Mansoor Asif
- Final year thesis ”Gesture to speech recognition system for specially-abled people (using raspberry pi)”
- Major courses: Machine Learning, Computer Vision, Embedded Systems, Signal Processing

Research Interests

- Robustness and Generalizability of Vision-Language models (VLMs, LLMs), Test Time Optimization, Trustworthy AI
- Privacy and Security in Medical Data Handling, Zero-Shot Classification, Self-Supervised Learning

Publications

** indicates Equal Contribution*

- Muhammad Huzaifa*, HS Malik*, M Naseer, S Khan, FS Khan, **ObjectCompose: Evaluating Resilience of Vision-Based Models on Object-to-Background Compositional Changes** *under review at ECCV-2024* | *Project*
- R Imam, H Ghani*, Muhammad Huzaifa*, K Nandakumar, **Test-Time Low Rank Adaptation via Confidence Maximization for Zero-Shot Generalization** *under review at ECCV-2024* |
- Muhammad Huzaifa*, R Imam*, MEA Azz, **On enhancing the robustness of Vision Transformers: Defensive Diffusion,** *27th Conference on MIUA 2023, Scotland* | *arXiv*
- R Imam, Muhammad Huzaifa, N Mansour, SB Mirza, F Lamghari, **Domain Adaptable Fine-Tune Distillation Framework For Advancing Farm Surveillance,** | *arXiv*

Experience

Intelligent Visual Analytics Lab (IVAL) **Aug 2022 – present**

Graduate Research Assistant *MBZUAI, Abu Dhabi*

- Main research topics: Multi-modal modals, Generative AI, Robustness of vision-language models
- Working on Generative AI (Diffusion models) for adversarial attacks and robustness (medical and natural images)
- Act as Teaching assistant for Machine Learning (ML701), Deep Learning(AI703), Artificial Intelligence (AI701) courses

Fujairah Research Center **May 2023 – Aug 2023**

Visiting Researcher *Fujairah, UAE*

- Combined the foundational models SAM & GroundingDINO for automated annotation of raw CCTV/video dataset
- Introduced zero-shot fine tune distillation which distills knowledge from large GroundingDINO to lightweight YOLOv8
- Evaluated SOTA object detection algorithms like YOLO models for enhancing physical security in camel farm settings

Techlogix **Mar 2022 – June 2022**

Application Consultant *Lahore, Pakistan*

- Developed Management Information System (MIS) reports per business requirements using SQL
- Established a streamlined issue tracking system by leveraging the capabilities of SQL databases
- Provided specialized assistance for the deployment and maintenance of critical banking applications

ProntoDigital **Nov 2021 – Feb 2022**

Digital Data Analytics Consultant *Lahore, Pakistan*

- Implemented cutting-edge tracking systems through Google Analytics and Google Tag Manager, providing clients with comprehensive visibility into their website performance.
- Leveraged in-depth analysis of website data to generate bespoke reports, enabling clients to optimize strategies and boost sales effectively

Projects

Multi Modal Learning - Hateful Meme Detection | *Git* **Aug – Dec 2022**

- Improved hateful meme classification using a dynamic multi-modal strategy, overcoming diverse content challenges
- Optimizing feature vectors alignment of a pre-trained Contrastive Language-Image Pre-training (CLIP) model, and employing fusion techniques, resulting in a 2% AUROC improvement over the baseline in hate meme classification

On Adversarial Robustness of Vision Transformers in Medical Imaging **Jan – April 2023**

- Developed specialized defense mechanisms against adversarial attacks, customized to the unique characteristics of medical image datasets, ensuring robustness in critical healthcare scenarios.
- Conducted a thorough examination of vision transformers' performance across various medical image datasets, benchmarking their robustness against diverse attack methods and providing valuable insights for enhancing the safety

Segmentation Models (DeepLabV3+ and SegFormer) robustness analysis| *Git* **Aug – Dec 2022**

- Compared Segformer and DeeplabV3+ for semantic segmentation, emphasizing Segformer's robustness to perturbations
- Utilized ADE20k dataset, with a focus on person class segmentation to alleviates pre-training bias.
- Highlighted controlled noise levels as crucial for optimal performance in both models.

Gesture To Speech Recognition System for Specially-abled People| *Git* **July 2020 – May 2021**

- Designed and developed a smart glove incorporating flex and gyro sensors, programmed on a Raspberry Pi microcontroller. This innovation enables the translation of sign language gestures into speech.
- Addressed the global challenge of hearing loss, which affects approximately 5% of the population, by creating a technological solution that empowers individuals with special abilities to interact effectively.

Skills

Languagees: Python, C/C++, MATLAB, Assembly and embedded C, SQL, JavaScript, HTML/CSS
Programming: PyTorch, Keras, Tensorflow, Latex, Diffusers, Scikit-learn
Tools: Linux, PyCharm, VS code, Git, GitHub, AutoCAD, Draw.io, Roboflow, Jira
Soft Skills: Teamwork, Problem-solving, Leadership, Research, Critical Thinking, Management
Languages: English (IELTs Band 7), Hindi, Urdu

Honours & Awards

- Defensive Diffusion nominated for the best Paper award, under Abstract Category, at 27th Conference on MIUA **2023**
- Secured **Fully Funded Scholarship** for Graduate School at MBZUAI for MS program in Machine Learning **2022**
- Achieved 2nd Prize for Best Undergraduate Thesis in Electrical Engineering Department at NUST, Pakistan. **2021**
- Finalist of Crossroads Emerging Leadership Program, organized By Harvard University **2021**

MOOCS, Certifications & Events

Machine Learning, Stanford University
AI For Everyone, DeepLearning.AI
Data Science Methodology, IBM
Computer Vision with TensorFlow, DeepLearning.AI
Improving Deep Neural Networks, DeepLearning.AI
Entrepreneurship in Emerging Economies, edX
Supply Chain Basics for Everyone, LinkedIn
Introduction to Data Studio, Google Analytics
Neural Networks and Deep Learning, DeepLearning.AI
What is Data Science, IBM
Tools for Data Science, IBM
Python for Data Science, AI & Development, IBM
Introduction to Computer Vision and Image Processing, IBM
AI for Medical Diagnosis, DeepLearning.AI
Python Bootcamp Build Applications and Games, Udemy
Google Tag Manager, Google Analytics

Positions & Services

- Selected as a **Mentor**, provided guidance and evaluated student projects at MBZUAI. **2023 – 2024**
- **Participated** in Human Phenotype Project Hackathon, UAE **2023 – 2023**
- Physically **attended** the EMNLP conference in Abu Dhabi. **2022 – 2022**
- University **Campus Ambassador** at WALEE (a marketing company) **2021 – 2021**
- Served As **Science Educator** at Science Fuse Society **2021 – 2022**
- Export **Sales Intern** at Pak Elektron Limited, Pakistan **2021 – 2021**
- **Attended** IEEE Honet (Conference) on Smart Cities **2018 – 2018**

Other Interests

- Reading, Interesting topic discussions, Swimming, Gym, Table Tennis, Football, Nature photography, Traveling

References

1. ✉ Fahad Khan (MBZUAI, Linkoping university) 2. ✉ Salman Khan (MBZUAI, Australian National University)
3. ✉ Muhammad Haris Khan, (MBZUAI) 4. ✉ Muzammal Naseer, (MBZUAI)