Muzammal Naseer

Masdar City
Abu Dhabi, UAE
☎ *+971 509886713*
✉ *muz.pak@gmail.com*
muzammal-naseer.netlify.app

Google Scholar | Homepage | Linkden | Twitter | GitHub

Citations: 900, H-index: 8 ☆ 300

Education and Degrees

2018–2022 **Doctor of Philosophy in Engineering & Computer Science**, *Australian National University (ANU).*

- Ph.D. Advisors: Dr. Salman Khan, and Prof. Fatih Porikli.
- I defended my thesis titled *Novel Concepts and Designs for Adversarial Attacks and Defenses.*
- My research was focused on understanding and improving out-of-distribution generalization of machine learning and deep learning based models. I developed new algorithms for adversarial attack and defense methods for computer vision applications including segmentation, object recognition and detection.
- Multiple chapters of my Ph.D. thesis are also peer-reviewed and published at top machine learning and computer vision venues including NeurIPS, CVPR, ICCV, TNNLS, and TPAMI.

2011–2013 **Master of Science in Electrical Engineering**, *King Fahd University of Petroleum & Minerals (KFUPM)*, average GPA 3.75/4.0.

- I graduated with *first class honors* and defended my thesis titled *The Design of Finite Impulse Response (FIR) Wavefield Extrapolation Filters.*
- Research was conducted with the collaboration of *Saudi Aramco* and the resulting software of my thesis was tested on the active oil well exploration sites. Multiple chapters of my thesis are also peer-reviewed and published at the Society of Exploration Geophysicists.
- I took in-depth courses on mathematics, signal processing, systems identification, and control theory.

2006–2010 **Bachelor of Science in Electrical Engineering**, *University of the Punjab (PU)*, average GPA 3.9/4.0, Gold Medalist.

- I graduated by defending my thesis titled *Spectrum Monitoring & Analysis of Interference in EGSM Networks.* This project was funded by Pakistan Frequency Allocation Board (FAB) and telecommunication network operator company, ZONG.

Academic and Research Experience

Sept. 2020–present **Postdoctoral Researcher**, *Computer Vision Laboratory, MBZUAI UAE*

- Currently, my research is focused on video understanding, adversarial learning, and developing insights by analyzing and visualizing the internal workings of deep neural networks.
- I am supervising Master and Ph.D. students as well as research assistants.
- I am actively participating in teaching including lab supervisions and guest lectures at MBZUAI.

Sept. 2018 – Mar. 2020 **Research Associate**, *Inception Institute of Artificial Intelligence - IIAI, UAE*

- Developed cross-domain adversarial attack and task-generalizable neural purification defense.

2018 **Research Associate**, *Data61, CSIRO, Canberra, Australia*

- Developed task-generalizable transferable adversarial attack for neural networks vision systems.

Sept. 2014 – June. 2017 **Lecturer (Full-Time)**, *University of Hafr Al Batin - subcampus of KFUPM, KSA*

- I joined subcampus of KFUPM, now known as University of Hafr Al-Batin as a full-time lecturer to teach variety of *Electrical Engineering* courses including circuit analysis, analog and digital systems, and programming (C/C^{++}/Assembly). I also mentored student's final year graduate projects.

2013 **Teaching Assistant**, *Department of Electrical Engineering, KFUPM, KSA*

- Assisted in Control Theory and Signal Processing courses.

2009 **Research Assistant**, *Frequency Allocation Board (FAB), Pakistan*

- Worked with FAB team to develop the direction finding system for Radio Frequency Interferers.

Honors and Awards

2019 Student travel award for Vancouver, Canada at *Neural Information Processing Systems* (NeurIPS).

2017 Postgraduate research scholarship by *ANU, Australia* for the period of three years.

2017 Fee remission merit scholarship by *ANU, Australia* for the period of four years.

2011 Master of science scholarship by the *Ministry of Higher Education*, KSA for the period of two years.

2011 Gold Medal by the *University of the Punjab* (PU) for outstanding performance in B.Sc. degree.

2007-09 University merit scholarship by the *University of the Punjab* (PU) consistently for three years.

Research Funding

2022 **MBZUAI-WIS Program for Collaborative Research in AI**, *UAE*

- **Title**: Biomimetic visual-recognition at low resolution with continuous learning.
- **Amount**: 2.7 Million Dollar.
- **Role**: Work Package Leader

Selected Publications

Note that in terms of impactful scientific research ideas and quality of the publications, the Computer Vision and Machine Learning conferences including CVPR, ICCV, ICLR, and NeurIPS are among the top-tier venues across all Engineering and Computer Science disciplines. ICLR and CVPR are ranked 1st among Artificial Intelligence and Pattern Recognition categories, respectively.

CVPR **Oral**, top 5.0%
Self-Supervised Video Transformer.
Kanchana Ranasinghe, **Muzammal Naseer**, Salman Khan, Fahad Shahbaz Khan, Michael Ryoo
IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2022.

ICLR **Spotlight**, top 5.0%
On Improving Adversarial Transferability of Vision Transformers.
Muzammal Naseer, Kanchana Ranasinghe, Salman Khan, Fahad Shahbaz Khan, Fatih Porikli
International Conference on Learning Representations (ICLR), 2022.

NeurIPS **Spotlight**, top 3.0%
Intriguing Properties of Vision Transformers.
Muzammal Naseer, Kanchana Ranasinghe, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Ming-Hsuan Yang
Advances in Neural Information Processing Systems ((NeurIPS), 2021.

ICCV
On Generating Target Transferable Perturbations.
Muzammal Naseer, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Fatih Porikli
International Conference on Computer Vision (ICCV), 2021.

ICCV
Orthogonal Projection Loss
Kanchana Ranasinghe, **Muzammal Naseer**, Munawar Hayat, Salman Khan, Fahad Shahbaz Khan
International Conference on Computer Vision (ICCV), 2021.

CVPR **Oral**, top 5.7%
A Self-supervised Approach for Adversarial Robustness
Muzammal Naseer, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Fatih Porikli
IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2020

NeurIPS
Cross-Domain Transferability of Adversarial Perturbations.
Muzammal Naseer, Salman Khan, Harris Khan, Fahad Shahbaz Khan, Fatih Porikli
Advances in Neural Information Processing Systems ((NeurIPS), 2019.

Selected Journal Publications

TPAMI
Stylized Adversarial Defense
Muzammal Naseer, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Fatih Porikli
IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2022. [Impact factor: 24.31]

TNNLS
Guidance Through Surrogate: Towards a Generic Diagnostic Attack
Muzammal Naseer, Salman Khan, Fatih Porikli, Fahad Shahbaz Khan
IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2022 [Impact factor: 14.25]

Selected Other Conference Publications

BMVC
Rich Semantics Improve Few-shot Learning
Mohamed Afham, Salman Khan, Haris Khan, **Muzammal Naseer**, Fahad Khan
The British Machine Vision Conference (BMVC), 2021

WACV **Local Gradients Smoothing: Defense Against Localized Adversarial Attacks**
Muzammal Naseer, Salman Khan, Fatih Porikli
Winter Conference on Applications of Computer Vision (WACV), 2019

Computational Skills

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

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

Tensorflow I have used Tensorflow to build different projects including a defense algorithm against unconstrained adversarial attacks.

C/C^{++} I scored A^{+} grades in these languages in my B.Sc courses. [Transcript]

Teaching

2020-2022 **Machine Learning (ML701)**, *MBZUAI*, labs, exams, and projects
Conducted 14 labs along with short lectures on **Naive Bayes Classification**, **Linear Vs. Logistic Regression**, **Support Vector Machines**, **Cross-validation, Overfitting and Underfitting**, **AdaBoost Classification**, **Clustering**, **Principal Component Analysis**, **Kernel Density Estimation**, **Expectation Maximization Algorithm**, **Neural Networks**, **Reinforcement Learning**, and **Graphical Models**. I also corrected final exams and projects.

2021 **Deep Learning (AI702)**, *MBZUAI*, labs, exams, and projects
Conducted 13 labs along with short lectures on **Backpropagation**, **Optimizers (AdaGrad, RMSprop, Adam, NAdam, AdamW)**, **Regularization**, **Long Short-Term Memory (LSTM)**, **Graph Neural Networks**, **Generative Adversarial Networks**, **Variational Auto-encoder**, **Transfer Learning**, and **Object Detection**. I also corrected final exams and projects.

Research Supervision

2020-2021 Kanchana Ranasinghe, Research associate at MBZ University of AI (MBZUAI, UAE)
He graduated from the University of Moratuwa and was a Lead Machine Learning Engineer before joining as an intern. He explored the effect of inter-class feature orthogonality on the generalization of neural networks under my supervision. He presented this project at ICCV as the main conference paper. He went on to join the University of Stony Brook, New York, as a Ph.D. Student.

2020-2021 Mohamed Afham, Research associate at MBZ University of AI (MBZUAI, UAE)
He was a final year undergrad at the University of Moratuwa before joining as an intern. He worked on improving few-shot learning methods by incorporating textual semantic information under my supervision. He presented this project at BMVC as the main conference paper. He went on to join the Meta AI residency program.

Professional Services

As a Member of Program Committee

2022 **VTTA**, Vision Transformers: Theory and applications, ACCV 2022

2021 **AROW**, Adversarial Robustness In the Real World, ICCV 2021
Reviewed 2 papers on topics including **a)** 3D Adversarial Attack (1 paper), and **b)** Adversarial Training for large Perceptual Bounds (1 paper)

2020 **AROW**, Adversarial Robustness In the Real World, ECCV 2020
Reviewed 2 papers on topics including **a)** Out-of-Distribution Detection (1 paper), and **b)** Transparent Patch Attack (1 paper)

As a Reviewer

From 2022 **Conferences: CVPR, NeurIPS, ACCV**

- Reviewed 7 papers in 2022 on topics including **a)** Adversarial Training (3 papers), **b)** Certifiable Defense against Patch Attack (1 paper), **c)** Robustness analysis against Patch Attack (1 paper), **d)** Transferable Attack (1 paper), and **e)** Defense based on Randomization (1 paper)

From 2020 **Journals: TPAMI, TIP, and TNNLS**

- Reviewed 2 papers in 2020 on Transferable Adversarial Attacks.
- Reviewed 4 papers in 2021 on topics of **a)** Image Decomposition (1 paper), **b)** Adversarial Training (1 paper), **c)** Explainability of Adversarial Vulnerability (1 paper), **d)** Query based Attack (1 paper)
- Reviewed 3 papers in 2022 on topics of **a)** Saliency Object Detection using Transformers (1 paper), **b)** Transferable Attacks on Image/Video Transformers (1 paper), and **c)** Attack on Interpretable Deep Learning (1 paper)

Others

2022 Australian Permanent Residency through Global Talent Independent Program.

References

Dr. Salman Khan, Associate Professor at MBZ University of AI (MBZUAI, UAE)
✉ salman.khan@mbzuai.ac.ae

Dr. Munawar Hayat, Senior Lecturer at Monash University
✉ munawar.hayat@monash.edu.au

Dr. Fahad Shahbaz Khan, Associate Professor at MBZ University of AI (MBZUAI, UAE)
✉ fahad.khan@mbzuai.ac.ae,

Prof. Fatih Porikli, Chief Scientist at Qualcomm, United States
✉ fatih.porikli@gmail.com