Tooba Imtiaz

imtiaz.t@northeastern.edu | in | |

EDUCATION

FALL 2021 -PhD Candidate, ELECTRICAL ENGINEERING. Advisor: Prof. Jennifer Dy **PRESENT** Northeastern University, Boston Masters, ELECTRICAL ENGINEERING, (GPA: 3.87/4.3) | Advisor: Prof. In-So Kweon 2018 - 2020 Korea Advanced Institute of Science and Technology (KAIST), S. Korea 2014 - 2018 Bachelors, ELECTRICAL ENGINEERING, (GPA: 3.93/4.0, Rank: 5th/156) | Advisor: Prof. Faisal Shafait National University of Sciences and Technology (NUST), Pakistan

WORK EXPERIENCE

SEP 2021 -Research Assistant | Machine Learning Lab @ SPIRAL,

PRESENT Northeastern University, Boston

- Developed an optimization-based sparse adversarial attack on images and evaluated its interpretability. (Pre-print under review.)
- Implemented Nerf-based 3D scene reconstruction from phone camera videos to facilitate at-home patient health monitoring.

Teaching Assistant | EECE7397 Advanced Machine Learning, Northeastern University **SPRING 2023**

External Consultant for ML and AI | ENDRESS+HAUSER, SEP 2020 -

AUG 2021 Maulburg, Germany

Proposed ML and CV-based solutions for process automation and optimization. Led two projects, both deployed to production:

- Deep learning for unsupervised 3D classification: used Autoencoders, Capsule architectures, and Implicit Neural Networks.
- · Forecasting on time series: utilized DNNs and Temporal Transformers to predict compound concentrations in liquids using sensors measuring base physical quantities. Achieved $\sim 96\%$ accuracy w.r.t. specialized physical sensors.
- SEP 2018 -Research Assistant | ROBOTICS AND COMPUTER VISION LAB,

AUG 2020 KAIST, South Korea

- · Bosch-RCV Project: Performed camera calibration, data collection, and vehicle trajectory estimation. Designed an occlusionrobust vehicle re-identification method using GANs for seamless tracking across a multi-camera surrounding awareness system.
- Universal Adversarial Perturbations: Developed novel adversarial attack algorithms. Published at CVPR, AAAI, and ACCV '20.
- SEP 2015 -Research Intern | TUKL-NUST R&D CENTRE,

MAY 2018 NUST, Pakistan

- · Proposed table detection and parsing in document images using ML and CV (LSTMs, text classification, clustering algorithms).
- Implemented LSTMs for handwritten address recognition to sort postal mail.

PUBLICATIONS

SAIF: Sparse Adversarial and Interpretable Attack Framework | Under review at ICCV 2023

T. Imtiaz, M. Kohler, J. Miller, Z. Wang, M. Sznaier, O. Camps, J. Dy

Devised a sparse adversarial attack using Frank-Wolfe, achieving SOTA results under tight sparsity and magnitude constraints on ImageNet & CIFAR10.

Volumetric propagation network: Stereo-lidar fusion for long-range depth estimation | IEEE RA-L 2021

J. Choe, K. Joo, T. Imtiaz, I.S. Kweon

Proposed a geometry-aware stereo-LiDAR fusion network for long-range depth estimation. I contributed to the network design and experiments.

Understanding Adversarial Examples from the Mutual Influence of Images and Perturbations | CVPR 2020

C. Zhang*, P. Benz*, T. Imtiaz, I.S. Kweon

Analyzed logits of clean images against additive perturbations and proposed a novel adversarial attack. I developed the loss objective and experiments.

CD-UAP: Class Discriminative Universal Adversarial Perturbation | AAAI 2020

C. Zhang*, P. Benz*, T. Imtiaz, I.S. Kweon

Proposed a novel UAP attack, causing a DNN to misclassify only a select group of classes. I contributed to the sampling strategy and experiments.

Double targeted universal adversarial perturbations | ACCV 2020

P. Benz*, C. Zhang*, T. Imtiaz, I.S. Kweon
Proposed a 'bidirectional' targeted UAP attack, such that classification labels are switched across a pair of classes. I designed the ablative experiments.

SCHOLARSHIPS AND AWARDS

ICML '22 volunteer award 2022

Qualcomm Innovation Fellowship Award, South Korea (among the 20 awardees) 2020

NUST Merit Scholarship (Awarded to top-3 GPA holders of cohort) 2014-2018

Global UGRAD Exchange Program, US Dept of State ($\sim 7.6\%$ selection rate)

SKILLS AND SERVICE

PyTorch, Tensorflow, Keras, Numpy, scikit-learn, Matplotlib

C / C++ / JAVA Object-oriented programming, Data structures, frontend and backend dev

MISC. MATLAB (Image and signal processing, Geometry and ML Toolbox, Simulink), Unix, gcc, Git, LTEX, ROS, AutoCAD

Reviewer for ICCV 2023 SERVICE

Workflow chair at AAAI 2024