Shehzeen Samarah Hussain

+1 (413) 801 8420
shehzeensh@gmail.com
shehzeen.github.io

Summary

I am a diligent and resourceful engineer with exceptional communication skills and leadership background. My technical interests include machine learning, speech and natural language processing, systems security and deep learning. I am eager to contribute towards developing technology to move societies forward.

Education

2023 **PhD in Computer Engineering**, University Of California San Diego.
Advised by Prof. Farinaz Koushanfar, *GPA 3.9*

2019 **Masters in Computer Engineering**, *University Of California, San Diego*, *GPA 3.9*.

2015 **Bachelor of Science in Electrical Engineering**, *University of Massachusetts, Amherst*.
Summa Cum Laude, GPA 3.9

2014 **Bachelor of Arts in Physics, Minor in Computer Science**, *Mount Holyoke College*.
Cum Laude, GPA 3.6

Experience

Aug 2017 - Present **Graduate Research Assistant**, *Prof. Farinaz Koushanfar*, UCSD.
Member of the Adaptive Computing and Embedded Systems Lab focusing on security in machine learning, natural language processing, and hardware acceleration of deep neural networks.

Jun 2022 - Sept 2022 **Research Intern - Deep Learning**, NVIDIA Corporation, *Santa Clara, CA*.
Designed deep neural networks for voice conversion and text-to-speech synthesis. Developed state-of-the-art zero-shot voice conversion framework with speaker-adaptive pitch and duration controllability.

Jun 2021 - Sept 2021 **Audio R&D Research Intern**, Qualcomm Technologies, Inc., *San Diego, CA*.
Developed self-supervised models for speech and audio processing tasks. Performed transfer learning with wav2vec 2.0 for downstream tasks such as keyword spotting and speaker verification.

Jun 2020 - Sept 2020 **Research Intern**, *Facebook Applied AI Research*, *Menlo Park, CA*.
Developed deep neural network models for multi-speaker and multi-style controllable speech synthesis for Speech team. Designed end-to-end pipeline for joint training of speaker encoder model with text-to-speech synthesis model using PyTorch. Developed voice cloning toolkit for synthesizing speech of unseen speakers from a few reference audio samples.

Jul 2019 - Oct 2019 **Graduate Machine Learning Intern**, Intel Corporation, *Santa Clara, CA*.
Worked on reinforcement learning for memory and SSD application as a part of the Non-Volatile Memory Systems Group. Developed frameworks for training and evaluation of reinforcement learning models.

Jun 2018 - Aug 2018 **Deep Learning R&D Intern**, Qualcomm Technologies, Inc., *San Diego, CA*.
Worked with the research team on applying deep reinforcement learning for optimizing power and performance management on Qualcomm chipsets. Implemented Dynamic Voltage Scaling using Reinforcement Learning and Recurrent Neural Networks. Designed and implemented alignment algorithms for creating the training dataset. Implemented data loader, model, trainers and evaluators using PyTorch.

Jul 2015 - Aug 2017 **Process Engineer**, GLOBALFOUNDRIES, *Malta, NY*.
Applied statistical process control principles and created verification test plans to ensure early detection of process irregularities and minimize excursions for 14nm and 7nm technology node. Designed and implemented sampling algorithm in MATLAB to model advanced wafer level corrections for lithography scanner applications team. Work has led to scientific publication in SPIE Metrology and Process control for Microlithography journal.

Aug 2013 - Dec 2014 **Teaching Assistant for CS Data Structures & ECE Embedded Systems Lab**, University of Massachusetts, Amherst, *Amherst, MA*.

Relevant Projects

Apr 2020 - Present **Deep Neural Networks for Expressive Speech Synthesis**, *https://expressivecloning.github.io/*.
Developed a controllable voice cloning software that allows fine-grained control over various style aspects of synthesized speech for an unseen speaker. This is achieved by explicitly conditioning a deep neural network based speech synthesis model on a speaker encoding, pitch contour and latent style tokens during training. Performed quantitative and qualitative evaluations to demonstrate that framework can be used for expressive voice cloning tasks using only a few transcribed or untranscribed speech samples from a new speaker.

Nov 2018 - 2019 **Acceleration of Audio Synthesis using Deep Neural Networks on FPGA**.
Developed the first accelerator framework for autoregressive convolutional neural networks. Deployed a fast inference model Fast-Wavenet on Xilinx XCVU13P FPGA which achieves 11 times faster generation speed than a high-end GPU and 66 times faster generation speed than a high-end CPU, when performing audio/speech synthesis.

May 2018 - 2019 **Generative Adversarial Network for Audio Reconstruction**.
Developed a framework: Audio-RecGAN for generating raw audio from lossy training dataset, using improved Wasserstein GAN loss (WGAN-GP) to optimize the Audio-RecGAN objective. Designed a generative adversarial training technique to explore different noisy measurement settings tailored for raw audio, and recover the underlying data distribution from a training dataset containing only lossy audio signals. Investigated an optimization objective to project lossy audio signals from natural data space back to the latent space of the trained Audio-RecGAN generator, in order to recover clean audio signals.

Relevant Courses

Neural Networks & Machine Learning, Algorithm Design, Data Structures, Deep Learning for Sequences, Principles of AI: Probabilistic Reasoning, Optimization and Acceleration of Deep Learning on Hardware Platforms, Security of Embedded Systems, Sensing & Estimation in Robotics, Computer Architecture, Probability & Random Processes, Mathematical Methods, Statistical Mechanics.

Publications

[13] **NetFlick: Adversarial Flickering Attacks on Deep Learning Based Video Compression**,
International Conference on Learning Representations (ICLR) Workshop on ML4IoT 2023,
Jung-Woo Chang, Nojan Sheybani, **Shehzeen Hussain**, Mojan Javaheripi, Seira Hidano, Farinaz Koushanfar.
A physical world LED-based attack on video compression and recognition systems.

[12] **ACE-VC: Adaptive and Controllable Voice Conversion using Explicitly Disentangled Self-supervised Speech Representations**,
IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2023,
Shehzeen Hussain, Paarth Neekhara, Jocelyn Huang, Jason Li, Boris Ginsburg.
A framework for zero-shot voice conversion using a shared self-supervised learning backbone.

[11] **FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs**,
IEEE/ACM International Conference on Computer-Aided Design (ICCAD) 2022,
Shehzeen Hussain, Nojan Sheybani, Paarth Neekhara, Xinqiao Zhang, Javier Duarte, Farinaz Koushanfar.
Accelerating neural networks for embedding hardware signatures into images to establish media authenticity and ownership of digital media.

[10] **Multi-task Voice Activated Framework using Self-supervised Learning**,
IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2022,
Shehzeen Hussain, Van Nguyen, Shuhua Zhang, Erik Visser.
A multi-task learning framework for solving keyword spotting and speaker verification, using a shared wav2vec 2.0 backbone.

[9] **Cross-modal Adversarial Reprogramming**,
IEEE Winter Conference on Applications of Computer Vision (WACV) 2022,
Shehzeen Hussain*, Paarth Neekhara*, Jinglong Du, Shlomo Dubnov, Farinaz Koushanfar, Julian McAuley.
Adversarially repurpose image classification neural networks for NLP and sequence classification tasks.

[8] **Expressive Neural Voice Cloning**,
Asian Conference on Machine Learning (ACML), 2021,
Paarth Neekhara*, **Shehzeen Hussain***, Shlomo Dubnov, Farinaz Koushanfar, Julian McAuley.
A framework for controllable voice cloning that allows fine-grained control over various style aspects of synthesized speech for an unseen speaker.

[7] **WaveGuard: Understanding and Mitigating Audio Adversarial Examples**,
USENIX Security Symposium 2021,
Shehzeen Hussain*, Paarth Neekhara*, Shlomo Dubnov, Julian McAuley, Farinaz Koushanfar.
A framework for defending deep neural network based automatic speech recognition systems against adversarial attacks.

[6] **Exposing Vulnerabilities of Deepfake Detection Systems with Robust Attacks**,
ACM Journal on Digital Threats: Research and Practice (DTRAP) 2021,
Shehzeen Hussain*, Paarth Neekhara*, Brian Dolhansky, Joanna Bitton, Cristian Canton Ferrer, Julian McAuley, Farinaz Koushanfar.
Practical perspective on the robustness of state-of-the-art Deepfake detectors against adversarial inputs.

[5] **Adversarial DeepFakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples**, *IEEE Winter Conference on Applications of Computer Vision (WACV) 2021*,
Shehzeen Hussain*, Paarth Neekhara*, Malhar Jere, Farinaz Koushanfar, Julian McAuley.
Evaluation of the robustness of neural network based fake video detection.

[4] **FastWave: Accelerating Autoregressive Convolutional Neural Networks on FPGA**,
IEEE/ACM International Conference on Computer-Aided Design (ICCAD) 2019,
Shehzeen Hussain, Mojan Javaheripi, Paarth Neekhara, Ryan Kastner, Farinaz Koushanfar.
Accelerating inference of WaveNet based neural networks on FPGA.

[3] **Universal Adversarial Perturbations for Speech Recognition Systems**,
INTERSPEECH, 2019,
Shehzeen Hussain*, Paarth Neekhara*, Prakhar Pandey, Shlomo Dubnov, Julian McAuley, Farinaz Koushanfar.
Evaluation of the robustness and vulnerabilities of deep neural network based automatic speech recognition systems.

[2] **Adversarial Reprogramming of Text Classification Neural Networks**,
Conference on Empirical Methods in Natural Language Processing (EMNLP) 2019,
Paarth Neekhara, **Shehzeen Hussain**, Shlomo Dubnov, Farinaz Koushanfar.
Adversarially repurpose text classification neural networks for alternate tasks.

[1] **Overlay optimization of 1x node technology and beyond via rule based sparse sampling**,
SPIE 9778, Metrology, Inspection, and Process Control for Microlithography XXX, 2016,
Nyan Lynn Aung, Woong Jae Chung, Lokesh Subramany, **Shehzeen Hussain**, Pavan Samudrala, Haiyong Gao, Xueli Hao, Yen-Jen Chen, Juan-Manuel Gomez.
A cost-effective automated rule-based sparse sampling method that can detect the spatial variation of overlay errors during semiconductor chip manufacturing.

Leadership and Awards

- Charles Lee Powell Foundation Fellowship for graduate study at UC San Diego, 2017
- Invited Member of ECE Honors Society Eta Kappa Nu (HKN), 2016
- Vice President for IEEE Student Board at University of Massachusetts, Amherst, 2014 - 2015
- Simon & Satenig Ermonian Memorial Engineering Scholarship – Award for Academic Excellence, 2014
- Invited Member of National Physics Honor Society Sigma Pi Sigma and Society of Physics Students at Mount Holyoke College, 2014
- Howard Hughes Medical Institute (HHMI) Award – A competitive grant awarded from among 300 applicants for summer research in physics, 2012
- Awarded 2nd Place at HackHolyoke Hackathon for Project MyCam, framework that tracks faces in a webcam using automated facial recognition, 2014
- Organized the first student run Embedded Systems Hackathon (HackUMass) at University of Massachusetts, Amherst alongside the IEEE student board, 2014