

Hossein Souri

CONTACT INFORMATION

Homewood Campus, Johns Hopkins University
Personal Website, GitHub, LinkedIn

Phone: +1-443-808-3141
✉ E-mail: hsouri1@jhu.edu

EDUCATION

Johns Hopkins University (JHU), MD, USA

August 2020 - Present

Ph.D. in Computer Science

Advisor: Dr. Rama Chellappa

Research: Adversarial Attacks, Adversarial Robustness, Data Poisoning, Knowledge Distillation.

University of Maryland, College Park (UMD), MD, USA

August 2018 - August 2020

M.S. in Electrical and Computer Engineering (GPA: **3.86/4**)

Advisor: Dr. Rama Chellappa

Research: Face Recognition Systems, GANs

Paper: **ATFaceGAN: Single Face Image Restoration and Recognition from Atmospheric Turbulence**

University of Tehran (UT), Tehran, Iran

2013 - 2017

B.S. in Electrical and Computer Engineering

GPA: 18.66/20 (**3.95/4**)

Advisor: Dr. Hamid Soltanian-Zadeh

HONORS AND AWARDS

- Clark School Distinguished Graduate Fellowships, University of Maryland, 2018-2019
- Ranked **5th (top 3%)** among 250 students of Electrical and Computer Engineering, University of Tehran, 2013-2017
- Awarded scholarship as an honor student for three consecutive years, University of Tehran, 2015-2017
- Ranked **12th** in the 21st Scientific Olympiad for University Students in Electrical and Computer Engineering and qualified to pursue graduate studies in any Iranian university, 2016
- Semi-finalist in Iranain National Mathematics and Physics Olympiad, 2011

PUBLICATIONS AND ARXIV PREPRINTS **Google Scholar Semantic Scholar**

- **Hossein Souri**, P. Khorramshahi, Chun Pong Lau, Micah Goldblum, and Rama Chellappa. “**Identification of Attack-Specific Signatures in Adversarial Examples**”. arXiv preprint arXiv:2110.06802, 2021. [\[Link\]](#)
- **Hossein Souri**, Liam Fowl, Rama Chellappa, Micah Goldblum, and Tom Goldstein. “**Sleeper agent: Scalable hidden trigger backdoors for neural networks trained from scratch**”. arXiv preprint arXiv:2106.08970, 2021. [\[Link\]](#)
- Liu, Jiang, Chun Pong Lau, **Hossein Souri**, Soheil Feizi, and Rama Chellappa. “**Mutual Adversarial Training: Learning together is better than going alone.**” arXiv preprint arXiv:2112.05005 (2021).[\[Link\]](#)
- Lau, Chun Pong, Jiang Liu, **Hossein Souri**, Wei-An Lin, Soheil Feizi, and Rama Chellappa. “**Interpolated Joint Space Adversarial Training for Robust and Generalizable Defenses.**” arXiv preprint arXiv:2112.06323 (2021).[\[Link\]](#)
- P. Khorramshahi*, **H. Souri***, R. Chellappa, and S. Feizi, “**GANs with variational entropy regularizers: Applications in mitigating the mode-collapse issue,**” *arXiv preprint arXiv:2009.11921*, 2020. [\[Link\]](#)
- P. Dhar, J. Gleason, **H. Souri**, C. D. Castillo, and R. Chellappa, “**Towards Gender-Neutral Face Descriptors for Mitigating Bias in Face Recognition,**” 2020. [\[Link\]](#)
- P. Dhar, J. Gleason, **H. Souri**, C. D. Castillo, and R. Chellappa, “**An adversarial learning algorithm for mitigating gender bias in face recognition,**” 2020. [\[Link\]](#)
- C. P. Lau, **H. Souri**, and R. Chellappa, “**Atfacegan: Single face imagerestoration and recognition from atmospheric turbulence,**” arXiv preprint arXiv:1910.03119, *Accepted as Oral presentation for FG 2020*. [\[Link\]](#)

RESEARCH EXPERIENCE	<ul style="list-style-type: none"> • Research Assistant, Artificial Intelligence for Engineering and Medicine Lab (AIEM), Johns Hopkins University Aug 2020 - Present Research: developing novel adversarial attack and defence models. • Research Assistant, University of Maryland Institute for Advanced Computer Studies (UMIACS), University of Maryland, College Park Aug 2018 - Aug 2020 Research: fairness in face recognition systems, image restoration, improving GANs, understanding deep features. • B. Sc. Thesis Project: Emotional State Recognition From EEG Signal Using Machine Learning Models 2017 Emotional state recognition and classification from EEG signals using wavelet-based and power-spectrum based feature extraction methods and MLP, SVM, and KNN classifiers • Research Assistant, Secure Communication Laboratory 2017 - 2018 Acoustic Scene Detection using matching pursuit algorithm for extracting time-frequency features and classifying using MLP and SVM classifiers and hidden Markov model (HMM) 	
ACADEMIC SERVICES	<ul style="list-style-type: none"> • <i>Conference Reviewer</i>: CVPR • <i>Journal Reviewer</i>: Pattern Recognition Journal 	
WORK EXPERIENCE	<ul style="list-style-type: none"> • Computer Networks Lab, University of Tehran, Iran 2016 Internship, Internet of Things Mentor - Dr. Vahid Shah-Mansouri Design and programming a smart home control and monitor system using Zigbee wireless technology 	
TECHNICAL SKILLS	<ul style="list-style-type: none"> • <i>Programming Languages</i>: Python, C/C++, Java, MATLAB • <i>Technical Tools</i>: PyTorch, TensorFlow, MATLAB, OpenCV, Keras, PySpark, Dask 	
RELEVANT COURSES	<ul style="list-style-type: none"> • Machine Learning • Advanced Numerical Optimization • Algorithms and Data Structures • Parallel Programming 	<ul style="list-style-type: none"> • Advanced Computer Vision • Advanced Computer Graphics • Advanced Object-Oriented Programming • Random Processes
TEACHING ASSISTANT EXPERIENCE	Machine Intelligence, Machine Perception, Computing Systems and Programming, Computer Networks, Signal and Systems, Probability and Statistics, Communication Systems, Digital Signal Processing.	
SELECTED PROJECTS Github	<ul style="list-style-type: none"> • Deep Convolutional Neural Network model for detecting the parameters of a circle presents inside a given image under the presence of noise. Code • Boundary detection and object recognition using classical and deep learning methods. Code • Python end-to-end pipeline to swap faces in videos and images. Code • Python implementation of classical and unsupervised Structure from Motion (SfM). Code • Deep Learning Based Denoiser for Images Rendered by Monte Carlo Sampling. Code • PySpark implementation of k-means clustering. Code 	