Hossein Souri

CONTACT INFORMATION

Personal Website, **LinkedIn**, **Twitter**, **GitHub**   ⊠ E-mail: hsouri1@jhu.edu

EMPLOYMENT

- **Research Assistant, Artificial Intelligence for Engineering and Medicine Lab (AIEM)**, Johns Hopkins University   Aug 2020 - Present

  Research: adversarial robustness, poisoning and backdoor attacks, self-supervised and transfer learning, segmentation, object tracking/detection, generative models, few-shot learning, federated learning, and fairness in face recognition.

- **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, GANs, deep features analysis.

EDUCATION

Johns Hopkins University (JHU), MD, USA   September 2020 - Present

Ph.D. in Computer Science
Advisors: Prof. Rama Chellappa, Prof. Tom Goldstein

University of Maryland, College Park (UMD), MD, USA   August 2018 - August 2020

M.S. in Electrical and Computer Engineering
Advisor: Prof. Rama Chellappa

University of Tehran (UT), Tehran, Iran   2013 - 2017

B.S. in Electrical and Computer Engineering

PUBLICATIONS AND ARXIV PREPRINTS
Google Scholar
Semantic Scholar

- **Hossein Souri**, Liam Fowl, Rama Chellappa, Micah Goldblum, and Tom Goldstein.
  "**Sleeper agent: Scalable hidden trigger backdoors for neural networks trained from scratch**". *Advances in Neural Information Processing Systems (NeurIPS)* (2022). [Link]

- Ravid Shwartz-Ziv, Micah Goldblum, **Hossein Souri**, Sanyam Kapoor, Chen Zhu, Yann LeCun, Andrew Gordon Wilson.
  "**Pre-Train Your Loss: Easy Bayesian Transfer Learning with Informative Priors**". *Advances in Neural Information Processing Systems (NeurIPS)* (2022). [Link]

- Jiang Liu, Chun Pong Lau, **Hossein Souri**, Soheil Feizi, Rama Chellappa.
  "**Mutual Adversarial Training: Learning together is better than going alone**". *IEEE Transactions on Information Forensics and Security (TIFS)* (2022). [Link]

- Valeriia Cherepanova, Steven Reich, Samuel Dooley, **Hossein Souri**, Micah Goldblum, Tom Goldstein.
  "**A Deep Dive into Dataset Imbalance and Bias in Face Identification**". *Workshop on Trustworthy and Socially Responsible Machine Learning, NeurIPS* (2022). [Link]

- Yuxin Wen, Jonas Geiping, Liam Fowl, **Hossein Souri**, Rama Chellappa, Micah Goldblum, Tom Goldstein.
  "**Thinking Two Moves Ahead: Anticipating Other Users Improves Backdoor Attacks in Federated Learning**". *AdvML Frontiers workshop at 39th International Conference on Machine Learning (ICML)* (2022). [Link]

- Renkun Ni, Manli Shu, **Hossein Souri**, Micah Goldblum, Tom Goldstein
  "**The Close Relationship Between Contrastive Learning and Meta-Learning**". *International Conference on Learning Representations (ICLR)*. (2021). [Link]

- **Hossein Souri**, Pirazh Khorramshahi, Chun Pong Lau, Micah Goldblum, and Rama Chellappa.
  "**Identification of Attack-Specific Signatures in Adversarial Examples**". *arXiv preprint arXiv:2110.06802* (2021). [Link]

- Chun Pong Lau, Jiang Liu, **Hossein Souri**, Wei-An Lin, Soheil Feizi, Rama Chellappa.
  "**Interpolated Joint Space Adversarial Training for Robust and Generalizable Defenses**". *arXiv preprint arXiv:2112.06323* (2021). [Link]

- Pirazh Khorramshahi*, **Hossein Souri***, Rama Chellappa, Soheil Feizi.
  "**GANs with variational entropy regularizers: Applications in mitigating the mode-collapse issue**". *arXiv preprint arXiv:2009.11921* (2020). [Link]

- Prithviraj Dhar, Joshua Gleason, **Hossein Souri**, Carlos D. Castillo, Rama Chellappa.
  "**Towards Gender-Neutral Face Descriptors for Mitigating Bias in Face Recognition**". *arXiv preprint arXiv:2006.07845* (2020). [Link]

- Prithviraj Dhar, Joshua Gleason, **Hossein Souri**, Carlos D. Castillo, Rama Chellappa.
  "**An adversarial learning algorithm for mitigating gender bias in face recognition**". (2020). [Link]

- Chun Pong Lau, **Hossein Souri**, Rama Chellappa.
  "**Atfacegan: Single face imagerestoration and recognition from atmospheric turbulence**". *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020).* IEEE, 2020. [Link]
  Accepted as Oral presentation for FG 2020. Best Paper (Honorable Mention) Award.

COMMUNITY INVOLVEMENT
- *Conference Reviewer*: CVPR, NeurIPS, ECCV, WACV
- *Journal Reviewer*: Pattern Recognition

TECHNICAL SKILLS
- *Programming Languages*: Python, C/C++, Java, MATLAB
- *Technical Tools*: PyTorch, TensorFlow, OpenCV, Keras, PySpark, Dask

RELEVANT COURSES
- Machine Learning
- Advanced Numerical Optimization
- Algorithms and Data Structures
- Parallel Programming
- 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
- 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**