Hossein Souri

CONTACT INFORMATION

Homewood Campus, Johns Hopkins University
Personal Website, **LinkedIn**, **Twitter**, **GitHub** ✉ E-mail: hsouri1@jhu.edu

EDUCATION

Johns Hopkins University (JHU), MD, USA — March 2024 (expected)

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

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

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

EMPLOYMENT

- **Internship, Ping An Technology, Silicon Valley Research Lab**
  Palo Alto, California — May 2023 - November 2023

  Research: Throughout my internship, I actively contributed to a prominent virtual being project. Specifically, I focused on the Talking Head Generation task, where I successfully designed and implemented a range of vision-language-speech models. By utilizing state-of-the-art diffusion models, I integrated videos, speech, and text resulting in highly realistic talking head animations.

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

  Research: My primary research is applied machine learning and computer vision, focusing on improving the robustness, transferability, and performance of image/face/video classifiers, object detection/segmentation, and generative models. Those include adversarial robustness, transfer learning, self-supervised learning, few-shot learning, and diffusion models, as well as, data poisoning and backdoor attacks.

- **Research Assistant, University of Maryland Institute for Advanced Computer Studies (UMIACS)**, University of Maryland, College Park — 2018 - 2020
  Research: Fairness in face recognition systems, image restoration, and GANs.

PUBLICATIONS AND ARXIV PREPRINTS
Google Scholar

- Micah Goldblum*, **Hossein Souri***, et al.
  "**Battle of the Backbones: A Large-Scale Comparison of Pretrained Models across Computer Vision Tasks**". *NeurIPS* 2023. [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**". *TPAMI* (2023). [Link]
- Valeriia Cherepanova, Steven Reich, Samuel Dooley, **Hossein Souri**, Micah Goldblum, Tom Goldstein.
  "**A Deep Dive into Dataset Imbalance and Bias in Face Identification**". *AAAI/ACM Conference on AI, Ethics, and Society (AIES)* (2023). [Link]
- **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]

- 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]

- 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.

- 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]

- **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]

- 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]

Book Chapters

- Chun Pong Lau, Jiang Liu, Wei-An Lin, **Hossein Souri**, Pirazh Khorramshahi, Rama Chellappa
  "**Adversarial attacks and robust defenses in deep learning**". *Elsevier* (2023).

Community Involvement

- *Conference Reviewer*: CVPR, NeurIPS, ICLR, ICML, ECCV, ICCV, WACV
- *Journal Reviewer*: Pattern Recognition

Technical Skills

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

Teaching Experience

- Machine Intelligence
- Machine Learning
- Machine Perception
- Deep Learning