MEHRDAD SABERI

Computer Science Ph.D. Student at University of Maryland

merhdads@gmail.com   msaberi@umd.edu   +1 (240)-960-9546   mehrdads   mehrdadsaberi.github.io

EDUCATION

Ph.D of Computer Science

University of Maryland

Jan 2023 – Ongoing   College Park, MD, USA

Bachelor of Computer Engineering

Sharif University of Technology

October 2018 – June 2022   Tehran, Iran

GPA: 19.28 / 20

International Olympiad in Informatics Preparation Camp

Young Scholars Club

October 2017 – June 2018   Tehran, Iran

High School Diploma

Allameh Helli High School

October 2015 – June 2017   Tehran, Iran

RESEARCH INTERESTS

Diffusion Models · Deepfake Detection · Image Watermarking · Generative Models · Adversarial Robustness · Interpretability · Large Language Models · Vision-Language Models · Algorithms

PUBLICATIONS

Published Papers

- Prime: Prioritizing interpretability in failure mode extraction. (2024). *ICLR 2024*.
- Robustness of ai-image detectors: Fundamental limits and practical attacks. (2024).
- Robust routing made easy: Reinforcing networks against non-benign faults. (2023). *IEEE/ACM Transactions on Networking*.
- Zerograd: Costless conscious remedies for catastrophic overfitting in the fgsm adversarial training. (2023). *Intelligent Systems with Applications*.

Preprints

- *Securing the future of GenAI: Policy and technology*. (2024).
- *Benchmarking text-guided image editing methods*. (2023).

Competitions

RESEARCH EXPERIENCE

Research Intern at Cruise AI

GenAI Team, Cruise

Jun 2024 – Ongoing   Remote

- Fields: **Video Generative Models**
- Projects: Developing video inpainting models for synthetic video generation, used for training of autonomous vehicles.

Research Assistant

Soheil Feizi, UMD

Jan 2023 – Ongoing   College Park, MD, USA

- Fields: **Generative Models, Trustworthy AI, Watermarking**
- Projects: Examination of fundamental constraints and trade-offs associated with AI-generated deepfake image detection and image watermarking; Development of an evaluation framework for text-guided image editing techniques; Introduction of a method for identifying human-understandable failure modes in visual models;

Summer Intern at EPFL

Nicolas Flammarion, EPFL

July 2021 – Sep 2021   Lausanne, Switzerland

- Field: **Adversarial Robustness in Computer Vision**
- Project: Examining the viability of employing non-L_p norms (such as Wasserstein and LPIPS distances) in the creation of adversarial examples, and subsequently leveraging them to enhance the robustness of adversarial training against unanticipated attacks.

Research Assistant

Mohammad Hossein Rohban, Sharif University of Technology

October 2020 – May 2021   Tehran, Iran

- Field: **Adversarial Robustness in Computer Vision**
- Projects: Several deep learning projects, encompassing tasks such as tackling the challenge of catastrophic overfitting in adversarial training (link), evaluating the robustness of Vision Transformer models, and investigating the generalization capabilities of adversarially trained networks.

Summer Intern at MPI

Christoph Lenzen, Max-Planck-Institut für Informatik

June 2020 – September 2020   Remote

- Field: **Distributed Algorithms**

- Erasing the Invisible: A Stress-Test Challenge for Image Watermarks. (2024). Neurips.

JOB EXPERIENCES

Data Scientist

Charkh.io

September 2022 – December 2022 Tehran, Iran

I was one of the lead members of the ML team responsible for conceiving and developing a comprehensive **recommender system** for shopping on Instagram. To the best of my knowledge, this kind of advanced recommender system has not been previously utilized by other Iranian companies.
The project involved the implementation of a diverse array of ML models, including YOLO and DINO for **object detection**, Milvus and ScaNN for **vector similarity search**, and a range of deep-learning-based collaborative, content-based, and hybrid recommender models. Additionally, the project necessitated proficiency across various programming platforms, spanning **databases** like SQL, MongoDB, and Vespa, **application frameworks** such as RapidAPI and Streamlit, as well as other tools like Docker and RabbitMQ.

Programming Language Teacher (C++, Python, Bash)

Iranian National Olympiad in Informatics Summer Camp

August 2019 – September 2019 Tehran, Iran

Algorithm Course Writer

Quera.ir

October 2018 – December 2018 Tehran, Iran

Algorithms, Combinatorics and Graph Theory Teacher

Shahid Beheshti High School

September 2017 – July 2018 Babol, Iran

HONORS AND AWARDS

- Gold medal in ICPC Regional (2019, Tehran)
- Silver medal in International Olympiad in Informatics (2018, Japan)
- Gold medal and ranked first in Iranian National Olympiad in Informatics (2017)
- Silver medal in Iranian National Olympiad in Informatics (2016)
- Silver medal in AITMO Regional (2013)
- Gold medal in Teenagers' Mathematical Olympiad (2012 and 2013, Mobtakeran)

- Project: Designing simple and generic black-box transformations that increase resilience of routing mechanisms against independently distributed node failures (link).

RELATED COURSES

Ph.D. Courses:
- Foundation of Deep Learning (CMSC 720, A+)
- Advanced Numerical Optimization (CMSC 764, A)
- Parallel Algorithms (CMSC 858I, A+)

Graduate Courses:
- Deep Learning (Sharif UT, 19.0 / 20)
- Convolutional Neural Networks for Visual Recognition (Stanford CS231n, Online)
- Numerical Methods for Optimization (Sharif UT EE, 18.0 / 20)
- NLP with Deep Learning (Stanford CS224n, Online)
- Theory of Distributed Systems (MPI, Online)
- Approximation Algorithms (Sharif UT, Online)

Undergraduate Courses:
- Artificial Intelligence (20 / 20)
- Modern Information Retrieval (19.9 / 20)
- Linear Algebra (20 / 20)
- Engineering Probability and Statistics (20 / 20)

Other Courses:
- Machine Learning (Coursera, Andrew Ng)
- Approximation Algorithms (Coursera, Claire Mathieu)

SKILLS

Python (Pytorch, Tensorflow) | Algorithms
Problem Solving | Data Structures
Graph Theory | Combinatorics | LaTeX
C++, Java, Go, Bash, Octave, Web Programming
Docker, SQL, MongoDB, RapidAPI, Streamlit, RabbitMQ

TEACHING ASSISTANT

University of Maryland:
- Discrete Structures (CMSC 250, Spring 2023)

Sharif University of Technology:
- Machine Learning (Spring 2021)
- Artificial Intelligence (Fall 2020)
- Linear Algebra (Spring 2020)
- Design of Algorithm (Spring 2020, Fall 2020, Spring 2020)
- Discrete Structures (Spring 2021, Spring 2020)
- Advanced Programming (Spring 2019, Fall 2019)

LANGUAGES

Persian	Native
English	Advanced (TOEFL score: 112)