Sepehr Rezaee

sepehrrezaee2002@gmail.com | github.com/SepehrRezaee | My Scholar | linkedin.com/in/sepehr-rezaee/

sepehrrezaee.github.io

Education

Shahid Beheshti University, BS. in Computer Sciences 2021 – 2025

- **Interests:** Deep Learning, Computer Vision, AI/ML, and AI Safety

Allameh Tabatabaei (Advanced) High School, Math Diploma 2019 – 2021

- GPA: 3.87/4.0

Experience

Research Assistant, Robust and Interpretable Machine Learning Lab – Sharif University of Technology, Tehran 2024 – Present

- Authored and co-authored 3 papers submitted to NeurIPS 2024, focusing on enhancing model reliability and security in machine learning.
- Developed and implemented 3 robust machine learning pipelines, increasing model reliability by adversarial conditions.
- Collaborated with a multidisciplinary team of 10 members to integrate machine learning solutions into 3 real-world applications(Autonomous Driving, Face Detection, Diagnosing Disease), improving operational efficiency.
- Presented research findings at 2 international conferences, elevating the lab's visibility and fostering academic collaborations.

Research Assistant, Artificial Intelligence and Scientific Computing Lab – Shahid Beheshti University, Tehran 2023 – Present

- Co-authored 2 undereview & 1 published research papers, including:
  - *Physics-Informed Lane-Emden Solvers Using Lynx-Net: Implementing Radial Basis Functions in Kolmogorov Representation*
  - *Leveraging Physics-Informed Convolutional Neural Networks (PICNNs) to Solve Linear and Non-linear Fokker-Planck Equations (FPEs)*
  - *Comparison of Pre-training and Classification Models for Early Detection of Alzheimer's Disease Using Magnetic Resonance Imaging*
- Modeled disease progression using differential equations, enhancing the understanding of biological mechanisms.
- Employed Physics-Informed Neural Networks (PINNs), increasing model accuracy through the integration of physical laws.

Deep Learning and Neuroscience Intern Researcher, Institute for Research in Fundamental Sciences (IPM) – Tehran 2023 – 2024

- Conducted comprehensive M/EEG data analysis utilizing advanced deep learning techniques to decode neural signals.
- Developed and optimized neural network architectures for improved signal processing and feature extraction.
- Collaborated with neuroscientists to interpret data results and contribute to the understanding of brain functionalities.
- Assisted in the preparation of research manuscripts and presentations for academic dissemination.

Publications

Scanning Trojaned Models Using Out-of-Distribution Samples Accepted to NeurIPS 2024

Hossein Mirzaei, Ali Ansari, Bahar Dibaei Nia, Mojtaba Nafez, Moein Madadi, **Sepehr Rezaee**, Zeinab Sadat Taghavi, Arad Maleki, Kian Shamsaie, Mahdi Hajialilue, Jafar Habibi, Mohammad Sabokrou, Mohammad Hossein Rohban

A Contrastive teacher-student framework for novelty detection under style shifts Submitted to ICLR 2025

Hossein Mirzaei, Mojtaba Nafez, Moein Madadi, Arad Maleki, Mahdi Hajialilue, Zeinab Sadat Taghavi, **Sepehr Rezaee**, Ali Ansari, Bahar Dibaei Nia, Kian Shamsaie, Mohammadreza Salehi, Jafar Habibi, Mackenzie W Mathis, Mahdieh Soleymani Baghshah, Mohammad Sabokrou, Mohammad Hossein Rohban

Backdooring Out-of-Distribution Detection Methods: A Novel Attack Approach Submitted to ICLR 2025

Hossein Mirzaei, Moein Madadi, Zeinab Sadat Taghavi, **Sepehr Rezaee**, Mohammad Sabokrou

Comparison of pre-training and classification models for early detection of Alzheimer's disease using magnetic resonance imaging Accepted in ICCCCC 2023 2023

AH Karami, **S Rezaee**, E Mirzabeigi, K Parand

Hierarchical Clustering Algorithms,Chapter of Unsupervised Algorithms: Clustering (with Implementation) Aarvan Publications 2022

Kourosh Parand, **Sepehr Rezaee**, et al.

Selected Projects

AI Model Security: Enhancing Robustness Against Backdoors and Trojans 2024

- Developed methods to detect and mitigate backdoors in machine learning models, enhancing AI deployment security.
- Engineered algorithms using statistical analysis and pattern recognition, improving trojan detection rates.
- Contributed to NeurIPS 2024 publications, advancing the field of AI model security.
- **Tools Used:** Python, PyTorch, Scikit-learn, LaTeX

Physics-Informed Neural Networks for Disease Progression Modeling 2023

- Created a Physics-Informed Neural Network integrating differential equations to accurately predict disease progression.
- Utilized clinical datasets and validated models with patient data, achieving higher accuracy than traditional methods.
- Published findings in peer-reviewed journals, contributing to AI-based healthcare innovations.
- **Tools Used:** PyTorch, NumPy, SciPy, Pandas

AI-Driven M/EEG Data Analysis for Neuroscience Research 2022

- Applied deep learning techniques to decode M/EEG signals, uncovering neural mechanisms.
- Streamlined data workflows by automating preprocessing and artifact removal, enhancing analysis efficiency.
- Facilitated insights into brain connectivity, supporting high-impact neuroscience research publications.
- **Tools Used:** MNE-Python, PyTorch, NumPy, Pandas

Selected Courses

Courses: Foundations of Data Science (A^+, 1st), Data Mining (A^+, 1st), Advanced Data Mining (A^+, 1st), Foundation of Numerical Analysis (A^+, 1st), Non-Linear Optimization (A^+, 1st), Partial Differential Equations (A^+, 1st), Electromagnetics (A^+, 1st), Neural Network (A^+, 3rd), Foundation of Logic and Set Theory (A^+, 3rd), Principles of Operating Systems (A^+, 2nd), Foundations of Machine Learning (A^+, 2nd), Elements of Probability (A, 4th), Data Structures & Algorithms (A, 5th)

Skills

Programming Languages: Python, C++, C, MATLAB, C# & Java

Python Frameworks & Libraries: PyTorch, TensorFlow, OpenCV, MNE-Python, NumPy, SciPy, Matplotlib, Scikit-Learn, NiPype, FastAPI, Django, Django REST Framework, Selenium

Other Tools and Technologies: JAX, PostgreSQL, NoSQL, MongoDB, Kotlin, , Git, Docker, Linux, Bootstrap

Interpersonal Skills: Problem Solving, Team Working

Languages: Fluent in Persian (speaking, reading, and writing), English (Professional working proficiency)

Reference Contacts

Prof. Kourosh Parand - k_parand@sbu.ac.ir
Prof. Mohammad Hossein Rohban - rohban@sharif.edu
Prof. Mohammad Sabokrou - sabokro@ipm.ir