Arezoo Rajabi

Ph.D. Candidate in Computer Science
Oregon State University

Email: rajabia@oregonstate.edu
LinkedIn: wwww.Linkedin.com/in/arezoo-rajabi
Homepage: http://rajabia.github.io

A dedicated and passionate ML researcher. Eager to work on newly emerged challenges. Proposed a practical adversarial perturbation scheme for image privacy in image sharing platforms. Introduced simple and efficient approaches for adversarial and out-distribution samples detection. Expertise in a variety of machine learning techniques especially deep learning, experience on distributed and clustered data processing tools (Spark, Hadoop), convex optimization, and statistical data analysis methods.

Education

Ph.D. in Computer Science **2014- 2021**

Oregon State University, Corvallis, Oregon, USA

Thesis: Two Sides a Coin: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations for Robust CNNs

- Developed two adversarial and out-distribution samples detection approaches
- Explored the practicality requirements of perturbation-based approaches for image privacy and proposed a practical adversarial perturbation scheme for preserving image privacy

M.Sc. in Software Engineering **2011-2013**

Sharif University Engineering, Tehran, Tehran, Iran

Thesis: Local Community Detection in Complex Networks

- Developed a local community detection approach for large complex networks whose topology are unknown

B.Sc. in Computer Science **2005-2010**

Sharif University Engineering, Tehran, Tehran, Iran

Thesis: Community Detection Algorithms

- Exploring complex networks' community detection methods

Professional Experience

Graduate Research Assistant **2015-Present**

Oregon State University, Corvallis, Oregon, USA

- Proposed a practical perturbation scheme for image privacy in image sharing platforms
- Improving augmented convolutional neural networks to detect out-distributions samples using a small set of proper out-distribution samples
- Improving standard and dynamic alternative direction method of multipliers mode estimation in power systems for tolerating false data injection attack

Soft Skills:

- Critical Thinking and Problem Solving
- Collaborative and Independent Researcher

Hard Skills:

- Deep learning
- Machine learning
- Image privacy
- Data Science
- Graph theory and complex networks
- Cybersecurity
- Convex optimization

Programming Languages:

- Python, Java, R, MATLAB, C#

Machine & Deep Learning Toolkits:

- Pytorch, Tensorflow, Keras
- Scikit-Learn, SciPy, Panda, Ggplot, Matplot, LIME
- Hadoop, Spark, AWS

Software and Tools:

- CVX, Lindo
- MySQL
- PST
- Git

Languages

- English: Fluent
- Persian (Native)

Graduate Research Assistant **2011-2013**

Digital Media Lab, Sharif University of Technology, Tehran, Iran

- Introducing a local community detection method to find community of a given node without having knowledge of the network topology
- Collaborating with PhD studying on his project on sampling from complex networks with high community structure and unknown
- Supervising an undergrad student on her project of social networks topology inference using diffusion information

Teaching Assistant **2014-Present**

Oregon State University, Corvallis, Oregon, USA

Teaching assistant for several undergrad and grad courses including Network Security, Advance System Security, Operating Systems(I), Analysis of Algorithms, Distributed Systems, Computer Applications

Teaching Assistant **2012-2013**

Sharif University of Technology, Tehran, Iran

Teaching assistant for Multi-Media Networks and Complex Networks courses

---

Volunteer Experience

Student Research Member **August 2020**

Data Anonymization and Synthesis Project proposed by Desjardin and Bank of Canada

Tenth Montreal Industrial Solving Workshop (IPSW), Montreal, Canada

- Reviewing of literature on synthetizing anonymized data
- Implement generative adversarial networks for creating fully synthetic data

---

Publications & Manuscripts

- **A. Rajab**i, R. Bobba, M. Rosulek, C. Wright, W. Feng, “On the (Im)Practicality of Adversarial Perturbation for Image Privacy", Accepted in Privacy Enhancing Technology symposium (a premier venue in privacy technologies), 2021.
- M. Abbasi, **A. Rajabi**, C. Gagné, R. Bobba, "Toward Adversarial Robustness by Diversity in an Ensemble of Specialized Deep Neural Networks", Long paper in Canadian Conference on Artificial Intelligent, 2020.
- M. Abbasi, C. Shui, **A. Rajabi**, C. Gagné, R. Bobba, "Towards Metrics for Differentiating Out-of-Distribution Sets", European Conference on Artificial Intelligent (ECAI), 2020.
- **A. Rajabi**, R. Bobba, "Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs", Dependable and Secure Machine Learning (DSML), 2019.

- M. Abbasi, **A. Rajabi**, C. Gagné, R. Bobba, "Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning", Dependable and Secure Machine Learning (DSML), 2018.
- M. Abbasi, **A. Rajab**i, A.S. Mozafari, R.B. Bobba, C. Gagné, " Controlling Over-generalization and its Effect on Adversarial Examples Generation and Detection", Arxiv Preprint, 2018.
- **A. Rajabi**, R. Bobba, "False Data Detection in Distributed Oscillation Mode Estimation using Hierarchical K-means", IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2019.
- **A. Rajabi,** R. Bobba, "A Resilient Algorithm for Power System Mode Estimation using Synchrophasors", Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS), ACM, 2016.
- M. Salehi, H. R. Rabiee and **A. Rajabi**, "Sampling from Complex Networks with High Community Structures", Chaos: An Interdisciplinary Journal of Nonlinear Science", 2012.

Selected Presentations

- **Paper Presentation at Dependable Machine Learning Workshop,** "Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs"
- **Paper Presentation at 2nd Annual Industrial Control System Security Workshop (ICSS)**, "A Resilient Algorithm for Power System Mode Estimation using Synchrophasors "
- **Poster Presentation at Graduate Research Showcase**, **School of Engineering, Oregon State University**, "Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning"

Honors and Awards

- First Place at Graduate Research Showcase, School of Engineering, 2018
- Cyber Resilient Energy Delivery Consortium (CREDC) Summer School Student Scholarship
- Student Travel Awards from Top Security Conferences (S&P, ACM, ACSAC, GREPSEC)

Selected Certificates

- Spark Fundamentals II, Cognitive Class, (An IBM Initiative)
- Data Science Foundation- Level 2, Cognitive Class, (An IBM Initiative)
- Cyber Resilient Energy Delivery Construction, Summer School Participation