Arezoo Rajabi

PhD Candidate in
Computer Science
Oregon State University

Personal Info

Email:
rajabia@oregonstate.edu

LinkedIn:
www.linkedin.com/in/arezoo-rajabi

Homepage:
http://rajabia.github.io

Skills

Depp Learning (CNN, GAN, AE)

Machine Leaning

Image Privacy

Statistical Data Analysis

Complex Networks Analysis

Cybersecurity in Power Systems

Professional Summary:

Ph.D. Candidate in Computer Science, Research Assistant at Oregon State University, and a previous student research member of Cyber Resilient Energy Delivery Consortium (CREDC). Currently, conducting research on image privacy, robust and dependable deep neural networks, and cybersecurity in power systems. Expertise in learning deep neural networks (face recognition, image classification, GANs, AEs), a variety of machine learning techniques including supervised and unsupervised learning, classification and dimension reduction, experience on distributed and clustered data processing tools (Spark, Hadoop), convex optimization, and statistical data analysis methods (e.g. regression, Bayesian statistics)

Education

2014-Present	**Ph.D. in Computer Science, Oregon State University** *Thesis:* Two Sides a Coin: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations for Robust CNNs
2011-2013	**M.Sc. in Computer Science, Sharif University of Technology** *Thesis:* Local Community Detection in Complex Networks
2005-2010	**B.Sc. in Computer Science, Sharif University of Technology** *Thesis:* Community Detection Algorithms

Publication

1. **A. Rajabi**, R. Bobba, M. Rosulek, C. Wright, W. Feng, “On the (Im)Practicality of Adversarial Perturbation for Image Privacy", Accepted in Privacy Enhancing Technology symposium (PETs), 2021.
2. 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.
3. 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.
4. **A. Rajabi**, R. Bobba, "Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs", Dependable and Secure Machine Learning (DSML), 2019.
5. 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
6. M. Abbasi, **A. Rajabi**, A.S. Mozafari, R.B. Bobba, C. Gagné, " Controlling Over-generalization and its Effect on Adversarial Examples Generation and Detection", Arxiv Preprint, 2018.
7. **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.
8. **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.
9. M. Salehi, H. R. Rabiee and **A. Rajabi**, " Sampling from Complex Networks with High Community Structures", Chaos: An Interdisciplinary Journal of Nonlinear Science", 2012.

Software and Tools

Programming Language:
Python, Java, R, MATLAB, C#

Deep Leaning Tools:
Pytorch, Tensorflow, Keras, MatConvNet

Machine Leaning Tools:
Scikit-Learn, SciPy, Panda, Matplot, ggplot

Data Mining Tools:
Weka, RapidMiner

Optimization Solver Tools:
CVX, Lindo

Distributed Data Processing Tools:
Hadoop, Spark, AWS

Others:
MySQL, OPNET, Latex. PST

Languages

English: Advanced

Persian: Fluent

References

Will be available on request

Work Experience

2015-Present	**Graduate Research Assistant** Oregon State University, Corvallis, OR, USA Description: Conducting research on the following projects: • Dependable and Robust Deep Neural Networks • Image Privacy in Image Sharing Platforms • Cybersecurity in Power Systems
2014-Present	**Teaching Assistant** Oregon State University, Corvallis, OR, USA Description: I have been TA for several undergrad and grad courses including Network Security, Advance System Security, Operating Systems(I), Analysis of Algorithms, Distributed Systems, Computer Applications
2011-2013	**Graduate Research Assistant** Digital Media Lab, Sharif University, Tehran, Iran Description: Conducting research on the following projects: • Local Community Detection in Social Networks • Sampling from Complex Networks with High Community Structure • Social Networks Topology Inference Using Diffusion Information
2012-2013	**Teaching Assistant** Oregon State University, Corvallis, OR, USA Description: I have been TA for Multi-Media Networks, Complex Networks courses

Selected Presentations

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

Honor and Awards

1. First Place at Graduate Research Showcase, School of Engineering, 2018
2. Cyber Resilient Energy Delivery Consortium (CREDC) Summer School Student Scholarship, 2017
3. Student Travel Awards from Top Security Conferences (S&P, ACM, ACSAC, GREPSEC)

Selected Certificates

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