Sara Ghazanfari

github.com/SaraGhazanfari linkedin.com/in/sara-ghazanfari sg7457@nyu.edu

Education

Ph.D. Candidate Jan. 2023 - Present
Electrical and Computer Engineering Department, New York University GPA: 3.945/4.0
Advisor: Siddharth Garg, Farshad Khorrami
Research Area: Deep Learning, Adversarial Machine Learning, Computer Vision

Courses: Probability & Stochastic (A), Deep Learning (A), Algorithmic Machine Learning & Data Science (A^-), Linear Systems (A), Machine Learning for Cybersecurity (A).

Master's of Science Sep 2018- July 2021
Computer Engineering Department, Sharif University of Technology GPA: 4.0/4.0
Bachelor's of Science Sep 2013- Feb 2018
Computer Engineering Department, Sharif University of Technology GPA: 3.6/4.0

Publications

LipSim: A Provably Robust Perceptual Similarity Metric ICLR 2024
R-LPIPS: An Adversarially Robust Perceptual Similarity Metric ICML Workshop 2023

Skills

Programming Languages: Python, C, Java, R, MATLAB.
Machine Learning Tools: Scikit-Learn, Spacy, Pytorch.
Database: PostgreSQL, Redis, Elasticsearch. Software and Tools: Microsoft Office, Jupyter Notebook, Pycharm, Git/GitHub, Unix Shell, Kafka.
Web frameworks: Django, Flask.

Teaching Experiences

Head TA, Machine Learning (Feb. 2021 – Aug. 2021) Sharif University of Technology
Instructor: Prof. Soleymani, Prof. Sharifi-Zarchi.

- Coordinating all course plans with the teaching group.
- Participating in mid-term and final exam design and assessment.
- Cooperating in home-works design.

TA, Modern Information Retrieval (Feb. 2020 – Aug. 2020) Sharif University of Technology
Instructor: Prof. Soleymani.

- Designing the course project.

TA, Machine Learning (Feb. 2019 – Aug. 2019) Sharif University of Technology
Instructor: Prof. Rohban, Prof. Sharifi-Zarchi.

- Designing assignments for the course.

Projects

LipSim: A Provably Robust Perceptual Similarity Metric

In this work, we demonstrate the vulnerability of SOTA perceptual similarity metric which is based on an ensemble of ViT-based feature extractors to adversarial attacks. We then propose a framework to train a robust perceptual similarity metric called LipSim (Lipschitz Similarity Metric) with provable guarantees by leveraging 1-Lipschitz neural networks as backbone and knowledge distillation approach to distill the knowledge of the SOTA models.

R-LPIPS: An Adversarially Robust Perceptual Similarity Metric

In this work, we propose the Robust Learned Perceptual Image Patch Similarity (R-LPIPS) metric, a new metric that leverages adversarially trained deep features. We further employ R-LPIPS as a proxy to bound the perturbation size for adversarial attacks.

FaRS: Fast Randomized Smoothing

In this project, we leverage the Lipschitz bound of the 1-Lipschitz networks as the backbone of our model and add the linear layer for the classification, and therefore we show that the Monte Carlo sampling is only required for the Linear layer and not for whole model including the backbone.

RoDINO: Boosting Empirical Robustness of Representations by Leveraging Modern Attacks

In this project, we propose RoDINO (Robust DINO) which is a method to boost the empirical robustness of downstream tasks by leveraging PGD attack to generate adversary images and adversarially train DINO which is a self-supervised representation learning model with Vision Transformers backbone.

Adversarial Attacks against the FixCaps Model for Skin Cancer Detection

In this project, we tried to reproduce the accuracy of the FixCaps model on the HAM10000 dataset and explore the robustness of FixCaps to three extensively used attacks, FGSM, PGD, and UAP.

Deep Learning Course Mini-project

In this project a Resnet network with at most 5 million parameters is trained.

Experience

Research Assistant Jan. 2023 - Present

Electrical and Computer Engineering Department, New York University

My primary research is focused on trustworthy machine learning with the goal of improving the robustness of vision systems including robust presentations and robust perceptual metrics.

Technical Team Lead Oct. 2021 – Jan. 2023

Narvan Startup Studio, Iran

The technical team leader of a software development team.

Data Engineer & Scientist Aug. 2020 – Oct. 2021

Narvan Startup Studio, Iran

* Designing and implementing data pipelines using Kafka.
* Storing and retrieving data in SQL-like databases such as PostgreSQL and NoSQL databases such as Elasticsearch, InfluxDB, and Redis.
* Designing an NLP pipeline, applied on Persian News.
* Designing and implementing preprocessing components named: Tokenizer, Lemmatize, and Normalizer with Python.
* Implementing and tuning CNN with residual connections for topic modeling (text classification) with Pytorch.

All tasks are done with **Python** programming language.