JAECHUL (Harry) ROH

Ph.D. Student in Computer Science, University of Massachusetts Amherst

jroh@umass.edu | https://www.jrohs.com | https://github.com/jcroh0508 | Google Scholar

EDUCATION

University of Massachusetts Amherst — **September 2023 – Present**
Ph.D. in Computer Science, Manning College of Information and Computer Sciences — Amherst, Massachusetts, USA
Advisor: Prof. Amir Houmansadr

Hong Kong University of Science and Technology — **September 2017 – May 2023**
B.Eng. in Computer Engineering, School of Engineering — Clear Water Bay, Hong Kong, HK

RESEARCH INTERESTS

My research interests rely on *adversarial machine learning, federated learning, and trustworthy AI.*

PUBLICATIONS

[1] Robust Smart Home Face Recognition under Starving Federated Data
ROH, Jaechul, Yajun Fang
- **Accepted** by the *IEEE International Conference on Universal Village (IEEE UV2022)* for oral presentation on September 26th, 2022
[paper][code][slides][video]

[2] MSDT: Masked Language Model Scoring Defense in Text Domain
ROH, Jaechul, Minhao Cheng, Yajun Fang
- **Accepted** by the *IEEE International Conference on Universal Village (IEEE UV2022)* for oral presentation on September 26th, 2022
[paper][code][slides][video]

[3] Impact of Adversarial Training on the Robustness of Deep Neural Networks
ROH, Jaechul
- **Accepted** by the *2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE)* on April 15th, 2022
[paper][code]

RESEARCH / WORK EXPERIENCE

BAID: Backdoor Attack for Gradient Inversion Defense — **August 2022 – May 2023**
Final Year Thesis, Supervisor: Prof. Jun Zhang — Clear Water Bay, Hong Kong
- Proposed novel text domain defense method against gradient inversion attack in the context of federated learning.

IEEE International Conference on Universal Village 2022 — **May 2022 – October 2022**
Student Research Program, Supervisor: Dr. Yajun Fang (CSAIL, MIT) — Cambridge, Massachusetts
- Experimented the robustness of federated learning in smart home face recognition system

MSDT: Masked Language Model Scoring Defense in Text Domain — **December 2021 – May 2022**
Independent Work Research, Supervisor: Prof. Minhao CHENG — Clear Water Bay, Hong Kong
- Proposed a novel improved textual defense method against backdoor attack on pre-trained language models.

Personal Research Project — **January 2022 – March 2022**
Topic: "Impact of Adversarial Training on the Robustness of Deep Neural Networks"
- Experimented the effectiveness of various methods of adversarial training on improving the robustness of neural networks against classifying perturbed histopathological images.

Super Chain AI (Conard International) — **June 2021 – August 2021**
NLP Engineer Intern in the Artificial Intelligence Team — Kowloon Bay, Hong Kong

- In charge of topic modeling and semantic analysis based on customer reviews and assigning specific semantics to the topics extracted.
- Competitors' analysis through web-scrapping customer reviews from other drop-shipping websites.

Military Service at Head Quarter of 12th Infantry Division **July 2018 – March 2020**
Sergeant of Republic of Korea Army Injae, Kang Won Do, Republic of Korea

- Officer Administrative Clerk Specialist
- Squad Leader of the Head Quarter

PROJECTS

Histopathological Scan Cancer Detection **December 2021 - January 2022**
2022 Personal Winter Project, Supervisor: Prof. Mark Vogelsberger (MIT)

- Demonstrated a user-friendly application that aids to classify whether a histopathologic scan contains metastatic cancer using modified Convolutional Neural Network and modified Resnet-18.
- In charge of implementing the neural networks for the classification task.

Presentation Project on "Adversarial Attack" **September 2021 – November 2021**
Machine Learning course Final Project, Instructor: Prof. Dit-Yan YEUNG Clear Water Bay, Hong Kong

- 30-minute video presentation on the topic of "Adversarial Attack"
- Papers reviewed: *"Explaining and Harnessing Adversarial Examples" & "Is Bert Really Robust? A Strong Baseline for Natural Language Attack on Text Classification and Entailment"*
  [video]

SKILLS / LANGUAGES

Programing Languages: Python, C++
Languages: Korean (Native), English (Native), Chinese (Fluent)