WUXINLIN CHENG

GitHub: github.com/chengwuxinlin | wcheng7@stevens.edu

EDUCATION

Stevens Institute of Technology, Hoboken, NJ - Ph.D. in Computer Engineering Jan 2020 – Present

Stevens Institute of Technology, **Hoboken, NJ -** M.Eng. in Computer Engineering Jan 2019 – Dec 2020

Sichuan University, **Chengdu, China -** B. Eng. in Electrical Engineering Sep 2014 – Jun 2018

PROJECTS

SPADE: A Metric for Black-Box Adversarial Robustness Evaluation (ICML 2021)
SPADE measures adversarial robustness of an ML model by examining the bijective distance mappings between the input/output graph-based manifolds. Moreover, SPADE can be further used to reveal robustness of input data, which guides downstream applications such as adversarial training. Compare with the VANILLA PGD training, SPADE can achieve up to 18% better accuracy.

S2D: Sample-to-Decision-Boundary Distance Characterization on the Manifold
S2D leverages output graph-based manifolds to measure robustness of each sample. By dynamically selecting non-robust samples, S2D leads to 1.7× training speedup over the state-of-the-art robustness training without any accuracy decreasing

Computer Vision Model Improvement for Vial Classification
This work exploits data selection, neural network pruning, and data augmentations to accelerate Vial classification while performing a better accuracy, leading to 42% accuracy improvement and 5.8× runtime speedup over the previous model from LEMA (Beijing) Technology Co., Ltd.

PERSONAL EXPERIENCE

- Research assistant at Stevens Institute of Technology June 2020 – Present
- Technical consultant intern at LEMA (Beijing) Technology Co., Ltd. Dec 2021 – May 2022
- Research intern at Shanghai ASES Spaceflight Technology Co. Ltd. Sep 2018 – Jan 2019

TECHNICAL STRENGTHS

Research Areas	Graph Learning, Machine Learning, Computer Vision, Robustness training
Software & Tools	Python, Matlab, C++, RoboDK, Altium Design

AWARDS AND HONORS

- Stevens Institute of Technology scholarship, USA Jan 2020
- National Entrepreneurship (top 1% nationally) at 3rd China International College “Internet Plus” Competition Jan 2018
- Sichuan University scholarship, China Dec 2017
- Honorable Award (top 21% globally) at the Mathematical Contest in Modeling, USA Apr 2017

Publication

Wuxinlin Cheng, Chenhui Deng, Zhiqiang Zhao, Yaohui Cai, Zhiru Zhang, and Zhuo Feng. “SPADE: A Spectral Method for Black-Box Adversarial Robustness Evaluation.” International Conference on Machine Learning (ICML), 2021.

Wuxinlin Cheng, Xu Zhou, Xin He. “Quick Pass Optimization in Airport Security Check,” TianFuShuXue, ISSN: 1006-0324, Vol, 21, 2018