WUXINLIN CHENG

wcheng7@stevens.edu ◇ Web: chengwuxinlin.github.io

EDUCATION

Stevens Institute of Technology Hoboken, NJ - Doctor of Philosophy in Computer Engineering Jan 2021 – Present
Stevens Institute of Technology Hoboken, NJ - Master of Engineering in Computer Engineering Jan 2019 – Dec 2020
Sichuan University Chengdu, China - Bachelor of Engineering in Electrical Engineering Sep 2014 – Jun 2018

PROJECTS

SPADE: A Metric for Black-Box Adversarial Robustness Evaluation (ICML 2021)
Developed SPADE, a novel metric for evaluating adversarial robustness in ML models, employing bijective distance mappings of input/output graph-based manifolds. Enabled downstream applications such as adversarial training by revealing data robustness, resulting in up to 18% enhanced accuracy compared to standard PGD training.

SGM-PINN: Sampling Graphical Models for Faster Training of Physics-Informed Neural Networks
Designed and implemented SGM-PINN, an innovative solution to overcome limitations of existing PINN-based PDE solvers. Introduced a graph-based importance sampling strategy for the adaptive selection of representative data samples, leading to up to 50% faster convergence on computational fluid dynamics (CFD) problems.

Model Accuracy & Runtime Improvement for Vial Classification (Industrial Task)
Improved accuracy and reduced computational load for Vial classification models by leveraging data selection, neural network pruning, and robust training strategies. Achievements include a significant 42% improvement in model accuracy and a 5.8× speedup in runtime over previous industrial models.

Hair Detection Stability Improvement (Industrial Task)
Enhanced stability and performance of hair detection models through robust training and data augmentations applied to a small dataset (200 pictures). Achieved exceptional test accuracy of 99.97% on the LEMA (Beijing) Technology Co., Ltd model. Notably, the model's accuracy remained consistent even under severity 5 corruption, demonstrating robustness to reasonable perturbations such as brightness differences or blur.

PERSONAL EXPERIENCE

Research Assistant - Stevens Institute of Technology June 2020 – Present

Scientific Advisor - LEMA (Beijing) Technology Co., Ltd. Dec 2021 – May 2022

Researcher Intern - Shanghai ASES Spaceflight Technology Co. Ltd. Sep 2018 – Jan 2019

SKILLS

Research Areas	Graph Learning, Machine Learning, Computer Vision, AI Stability, NLP
Software & Tools	Python, ML Frameworks, Matlab, C++, RoboDK, Altium Design, CUDA

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