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.

AI Agent for Education, Entertainment, and Company in Virtual Reality
Led the Interest Group lab in the development of 3D avatar assistants, establishing an innovative framework integrating Natural Language Processing and 3D model reconstruction. Developed a language emotion recognition system using Bert with 82% accuracy across 27 emotions and pioneered a text-to-speech model based on VIST2, achieving a 4.4 Mean Opinion Score and a 0.014 Real-Time Factor. Collaborated on facial reconstruction, LLM dialogue, and real-time lip-sync technologies.

CirSTAG: Graph Neural Networks Stability Analysis (DAC 2024)
Developed CirSTAG, a spectral framework for analyzing the stability of Graph Neural Networks (GNNs) using probabilistic graphical models. CirSTAG outperforms traditional Netattack in diverse GNNs, achieving 20% higher error rates in adversarial attacks and reducing defense error rates by 50%. Additionally, CirSTAG offers a significant improvement in evaluating and enhancing the large-scale integrated circuit design.

Real-Time Talking Heads from User-Uploaded Avatars (Video Example)
Developed a state-of-the-art system capable of generating real-time talking heads from user-uploaded avatar images, synchronized with any audio input. Pioneered the integration of this technology with chatGPT for live, avatar-based conversations, enhancing user interaction and engagement across various digital platforms. This innovation opens new interactive possibilities in social media, gaming, e-learning, and virtual customer support, by facilitating more natural and engaging digital communication experiences.

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 $5.8\times$ 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.

SAGMAN: Stability Analysis of Graph Neural Networks on the Manifolds (ICML 2024 Under Review)
Introduced SAGMAN, a spectral framework for assessing GNN stability. Developed a graph dimension reduction technique combining spectral graph embedding with probabilistic graphical models. Demonstrated SAGMAN's application in analyzing recommendation systems stability, improving GNN stability, and facilitating adversarial targeted attacks in downstream tasks.

PERSONAL EXPERIENCE

Scientific Advisor/Lead of AI Lab - Interest Group AI — Sep 2023 – Present
Research Assistant - Stevens Institute of Technology — June 2020 – Present
Scientific Advisor - LEMA (Beijing) Technology Co., Ltd. — Dec 2021 – Sep 2023
Research Intern - Shanghai ASES Spaceflight Technology Co. Ltd. — Sep 2018 – Jan 2019

SKILLS

Research Areas	Graph Learning, Machine Learning, CV, AI Stability, NLP, AIGC, LLM, GNN, Model Compression
Software & Tools	Python, C++, Pytorch, Tensorflow, Scikit-learn

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, Ali Aghdaei, Zhiru Zhang, and Zhuo Feng. "SAGMAN: Stability Analysis of Graph Neural Networks on the Manifolds." International Conference on Machine Learning (ICML), 2024 Under Review.

Wuxinlin Cheng, Yihang Yuan, Chenhui Deng, Ali Aghdaei, Zhiru Zhang, and Zhuo Feng. "CirSTAG: Circuit Stability Analysis via Graph Neural Networks." WIP, Design Automation Conference (DAC), 2024

John Anticev, Ali Aghdaei, **Wuxinlin Cheng,** and Zhuo Feng. "SGM-PINN: Sampling Graphical Models for Faster Training of Physics-Informed Neural Networks." Design Automation Conference (DAC), 2024

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