YUN-YUN (ALICE) TSAI

(+1) 917-498-2709 • yt2781@columbia.edu • https://yunyuntsai.github.io

RESEARCH INTERESTS

My research focuses on **robust machine learning**, **robustness on generative model**, and **self-supervised learning** in computer vision field. I am particularly interested in test-time domain adaptation and defenses against adversarial attacks. My personal goal is to make practical ML algorithms trustworthy and reliable.

EDUCATION

Columbia University in the City of New York
Ph.D. student in Computer Science — *Sept., 2021 – Present*
– Advisor: Prof. Junfeng Yang

National Tsing Hua University
Master of Science in Computer Science — *Sept., 2018 – June, 2020*
– Overall GPA: 3.9/4.0, Advisor: Prof. Tsung-Yi Ho
Bachelor of Science in Computer Science — *Sept., 2014 – June, 2018*
– Last 60 GPA: 3.8/4.0

PUBLICATIONS

Conference and Workshop Papers

[C1] **Yun-Yun Tsai**, Fu-Chen Chen, Albert Y.C. Chen, Junfeng Yang, Che-Chun Su, Min Sun, Cheng-Hao Guo, "GDA: Generalized Diffusion for Robust Test-time Adaptation," in Proceeding of the IEEE / CVF Computer Vision and Pattern Recognition Conference (**CVPR**) 2024.

[C2] **Yun-Yun Tsai**, Chengzhi Mao, Junfeng Yang, "Convolutional Visual Prompt for Robust Visual Perception," 37th Conference on Neural Information Processing Systems (**NeurIPS**) 2023.

[C3] **Yun-Yun Tsai**, Ju-Chin Chao, Albert Wen, Zhaoyuan Yang, Chengzhi Mao, Tapan Shah, Junfeng Yang, "Test-time Detection and Repair of Adversarial Samples via Masked Autoencoder," in Proceeding of the IEEE / CVF Computer Vision and Pattern Recognition Conference (**CVPR**) 2023, AdvML workshop

[C4] Lei Hsiung, **Yun-Yun Tsai**, Pin-Yu Chen, and Tsung-Yi Ho, "Towards Compositional Adversarial Robustness: Generalizing Adversarial Training to Composite Semantic Perturbations," in Proceeding of the IEEE / CVF Computer Vision and Pattern Recognition Conference (**CVPR**) 2023.

[C5] **Yun-Yun Tsai**, Lei Hsiung, Pin-Yu Chen, and Tsung-Yi Ho, "Generalizing Adversarial Training to Composite Semantic Perturbations," in Proceeding of International Conference on Machine Learning (**ICML**) AdvML Workshop, 2021.

[C6] Lei Hsiung, **Yun-Yun Tsai**, Pin-Yu Chen, and Tsung-Yi Ho, "CARBEN: Composite Adversarial Robustness Benchmark," in Proceeding of International Joint Conference on Artificial Intelligence (**IJCAI**), 2022.

[C7] Chao-Han Huck Yang, **Yun-Yun Tsai**, and Pin-Yu Chen "Voice2Series: Reprogramming Acoustic Models for Time Series Classification," in Proceeding of International Conference on Machine Learning (**ICML**), 2021.

[C8] **Yun-Yun Tsai**, Pin-Yu Chen, and Tsung-Yi Ho, "Transfer Learning without Knowing, Reprogramming black box machine learning model with scarce data and limited resources," in Proceeding of International Conference on Machine Learning (**ICML**), 2020.

[C9] **Yun-Yun Tsai**, Pin-Yu Chen, Tsung-Yi Ho, "Adversarial Machine Learning for Social Good: Reprogramming black box machine learning model with scarce data and limited resources," Advances in Neural Information Processing Systems (**NeurIPS**) NewInML Workshop, Poster, 2019.

[C10] Honggang Yu, Kaichen Yang, Teng Zhang, **Yun-Yun Tsai**, Tsung-Yi Ho, Yier Jin, "CloudLeak: Large-Scale Models Extraction Through Adversarial Examples," in Proceeding of Network and Distributed System Security Symposium (**NDSS**), 2020.

[C11] Ta-Wei Huang, **Yun-Yun Tsai**, Chung-Wei Lin, Tsung-Yi Ho, "Vehicle Sequence Reordering with Cooperative Adaptive Cruise Control," in Proceeding of Design, Automation and Test in Europe Conference and Exhibition (**DATE**), 2019.

Patents

[P1] Pin-Yu Chen, **Yun-Yun Tsai**, Sijia Liu, Chia-Yu Chen, I-Hsin Chung, Tsung-Yi Ho. "Transfer Learning With Machine Learning Systems", U.S. Patent Application No: 17/029506, Application Date: September 23, 2020.

Honors, Awards, and Grants

Student Travel Grant, CVPR 2023, Vancouver, Canada.

Ph.D. Dean's Fellowship, Fu Foundation School of Engineering and Applied Sciences, Columbia University, 2021.

Best Presenter, Blackhat Award Forum in CyberSec, Taiwan, 2020.

Research and Working Experience

Applied Scientist Intern — **Amazon Lab126, CoRo Team**, Bellevue, Washington
Mentor: Che-chun Su, Fu-chen Chen — *June, 2023 – present*

- Pr. 1: Improving object detection model robustness on out-of-domain (OOD) data via stable diffusion.

Graduate Research Assistant — **Columbia University**, NY, New York
Advisor: Prof. Junfeng Yang — *Sept, 2021 – present*

- Pr. 1: Improving visual recognition adversarial robustness via self-supervised learning.
- Pr. 2: Test-time model adaptation for out-of-distribution data with convolutional visual prompts.

Graduate Research Assistant — **NTHU**, Hsinchu, Taiwan
Advisor: Prof. Tsung-Yi Ho — *July, 2020 – June, 2021*
Co-Advisor: Dr. Pin-Yu Chen, IBM Research, NY, USA

- Pr. 1.: Generalized Adversarial Training to Composite Semantic Perturbations
- Pr. 2.: Black-box adversarial reprogramming on ML Models for limited data
- Pr. 3.: Reprogram acoustic speech recognition model for time-series classification
- Pr. 4.: Autonomous vehicle sequence optimization for Cooperative Adaptive Cruise Control

Visiting Scholar — **University of Florida**, Gainesville, FL, USA
Advisor: Prof. Yier Jin — *Mar., 2019 – Aug., 2019*

- Pr. 1: Large-scale Model Extraction from machine learning as a services

Research Intern — **Microsoft Cloud + AI Team**, Taipei, Taiwan
Mentor: Cheryl Hsu — *July, 2017 – June, 2018*

- Prototyping IoT solutions to 20+ business partners (e.g., NEC, Nexcom) by leveraging Azure IoT Cloud and Edge computing in a wide range of scenarios including Smart City, Retail, Home and Manufacturing.
  - Designed/Created Azure Machine Learning hands-on materials with Microsoft MVPs and delivered the workshop in coding angel event to 100+ college STEM female students.

Professional Service and Skills

Paper Review	IEEE Access, ICLR 2021, AAAI 2021, ICPAI 2020, CVPR 2022, NeurIPS 2022
Programming Languages	Python, Java, Ruby, C/C++, Verilog
Packages	Tensorflow, Pytorch, Sci-kit Learn, Keras, Caffe
Languages	English (fluent), Chinese (native)
TOEFL iBT	102/120 (Reading 28, Listening 25, Writing 26, Speaking 23)
GRE	Verbal 157/170, Quantitative 166/170, Analytical Writing 3.0/6.0
Certificate	Microsoft Data Science Certificate