

Wenzhao Xiang

ALGORITHM ENGINEER

5-318, Academy of electronic information and electrical engineering, Shanghai Jiao Tong University, Shanghai, 200240, China

☎ (+86) 158-2193-7913 | ✉ wenzhao-xiang@foxmail.com | 🌐 wenzhao-xiang.github.io/Blog/ | 📷 Wenzhao-Xiang



Biography

I am a third-year postgraduate student of the Institute of Image Communication and Networks Engineering in the Department of Electronic Engineering (EE), Shanghai Jiao Tong University (SJTU), advised by Prof. Shibao Zheng. I completed my bachelor degree in Electronic Engineering at SJTU. I was selected into the "Excellent Engineer Training Program" in my sophomore year. And in 2019, I received the postgraduate recommendation from the Department of EE, SJTU. From 2018 to 2019, I was an research intern in Intel Asia Pacific R&D Center. During this period, I finished my graduation project and won the "Excellent Intern" prize of 2019. From March 2020 until now, I have been studying in the TSAIL Group of State Key Lab. of Intelligent Tech. & Sys., Department of Computer Science and Technology, Tsinghua University, as a visiting student, advised by Prof. Jun Zhu/Hang Su.

My research areas include machine learning, deep learning and their applications in computer vision. At present, my main research field is the adversarial robustness of deep learning.

Education

Shanghai Jiao Tong University

B.S. IN INFORMATION ENGINEERING

Shanghai, China

Sep. 2015 - Jun. 2019

Shanghai Jiao Tong University

M.S. IN ELECTRONIC AND COMMUNICATION ENGINEERING

Shanghai, China

Sep. 2019 - Mar. 2022

Academic Achievements

Publications

- Wenzhao Xiang, Chang Liu, and Shibao Zheng. "Improving Visual Quality of Unrestricted Adversarial Examples with Wavelet-VAE." *ICML 2021 Workshop on Adversarial Machine Learning*. 2021.
- Wenzhao Xiang, Hang Su, Chang Liu, Yandong Guo, and Shibao Zheng, "Improving robustness of adversarial attacks using an affine-invariant gra-dient estimator," *arXiv preprint arXiv:2109.05820*, 2021. (TIFS<ccf-a>, Under Review)
- Xiao Yang, Yinpeng Dong, Wenzhao Xiang, Tianyu Pang, Hang Su, Jun Zhu, "Model-Agnostic Meta-Attack: Towards Reliable Evaluation of Adversarial Robustness", 2021. (NeurIPS 2021, Under Review)

Patents

- "Enhancing Transferrable Adversarial Examples With Affine-Invariant Attacks", 2020. (Substantive Examination)
- "Unrestricted Adversarial Attack Method Based on Frequency Domain Transformation", 2021. (Substantive Examination)

Contests

2021	2nd Place , TianChi/CVPR2021 AIC Phase VI Track2: Unrestricted Adversarial Attacks on ImageNet	Beijing, China
2020	9th Place , TianChi/CIKM2020 AIC Phase IV: Adversarial Challenge on Object Detection	Beijing, China
2019	2nd Prize of Global Finals (top3) , Huawei ICT Innovation Competition	Shenzhen, China
2019	Winning Award , Huawei Developer Competition IoT Track	Shenzhen, China
2018	National 1st Prize/Huawei Innovation Award , National IoT Contest	Wuxi, China
2018	H Prize , Mathematical Contest In Modeling	Shanghai, China

Projects

2020	TSAIL Group , the Development of “Adversarial Robustness Evaluation for Safety” (ARES) Platform	Beijing, China
2020	Institute of Image Communication and Networks Engineering in SJTU , Grading Diagnosis of Human Cataract Based on Slit-lamp Image	Shanghai, China
2019	Google Summer of Code 2019 , the Optimization of OpenCV.js with WebAssembly Threads and SIMD	Shanghai, China
2019	Intel Asia Pacific R&D Center , Implementation and Optimization of Web Machine Learning Inference Engine Based on WebAssembly (graduation project of B.S.)	Shanghai, China
2018	Ministry of Education&Huawei , Design of Smart Home Based on OceanConnect Platform	Shanghai, China
2017	Excellent Engineer Training Program , Design of Intelligent Tracking and Obstacle Avoidance Remote Control Car Based on Arduino and Android Platform	Shanghai, China

Work Experience

Intel Asia Pacific R&D Center

MACHINE LEARNING ENGINEER (INTERN)

Shanghai, China

Jul. 2018 - Sep. 2019

HUAWEI NOAH'S ARK LAB

AI ENGINEER (INTERN)

Beijing, China

Sep. 2021 - Now

Honors & Awards

2020	Intel Scholarship	Shanghai, China
2020	First Grade of Outstanding Postgraduate Scholarship of Shanghai Jiao Tong University	Shanghai, China
2019	Excellent Intern of Intel Asia Pacific R&D Center	Shanghai, China
2018	C Scholarship of Shanghai Jiao Tong University	Shanghai, China
2017	National Encouragement Scholarship	Shanghai, China
2016	Cyrus Tang Scholarship	Shanghai, China

Skills

ML Frameworks	Pytorch, Tensorflow, OpenCV, Matlab
Programming Languages	C/C++, Python, JavaScript(WebAssembly), Node.js, LaTeX
	Chinese, English