Chia-Hung Yuan

RESEARCH ENGINEER

MediaTek Headquarters, Hsinchu 30078, Taiwan

+886 988 812 983
jimmy.chyuan@gmail.com
lionelmessi6410.github.io
linkedin.com/in/chyuan-0607/
Google Scholar

Research Interests

My research interest is mainly in robust deep learning, including adversarial and trustworthy machine learning, domain adaptation, image/video restoration and enhancement, and generative model. Currently, I'm exploring the intersection of Generative AI and Edge AI to develop the on-device generative model.

Education

National Tsing Hua University *Sep. 2019 – Jul. 2021*
M.SC. IN COMPUTER SCIENCE *Hsinchu, Taiwan*
- Advisor: Shan-Hung Wu
- Thesis: Neural Tangent Generalization Attacks
- Overall GPA: 4.29/4.30 (top 1%)

National Tsing Hua University *Sep. 2014 – Jun. 2019*
B.SC. IN INTERDISCIPLINARY PROGRAM OF ENGINEERING (MATERIAL SCIENCE & QUANTITATIVE FINANCE) *Hsinchu, Taiwan*
- Overall GPA: 3.95/4.30, Major GPA: 4.01/4.30, CS-related GPA: 4.16/4.30 (top 1%)

Eberhard Karls University of Tübingen *Oct. 2016 – Jul. 2017*
EXCHANGE PROGRAM IN NANO-SCIENCE *Tübingen, Germany*

Work/Research Experiences

MediaTek *Jun. 2022 – Present*
RESEARCH ENGINEER *Hsinchu, Taiwan*
- Researched on the generative model and its application, enabling the model on edge devices.
- Researched on the intersection of deep learning and computer vision, with a focus on image/video processing algorithms like restoration and enhancement.
- Developed and deployed efficient deep learning architectures and models to real-world products. Supported product teams for commercialization, such as solution optimization, performance profiling, and benchmarking.
- Designed and developed the codebase for department, making cross-project collaboration more efficient.

MIT-IBM Watson AI Lab *Oct. 2021 – Nov. 2021*
RESEARCH INTERN *Massachusetts, USA*
- Advisor: Pin-Yu Chen / Co-advisor: Chia-Mu Yu (National Chiao Tung University)
- Researched on the intersection of meta learning, neural tangent kernel (NTK) and adversarial machine learning and published a paper "**Meta Adversarial Perturbations**" in **AAAI Workshop'22**.

DataLab, National Tsing Hua University *Sep. 2019 – Jul. 2021*
GRADUATE RESEARCH ASSISTANT *Hsinchu, Taiwan*
- Advisor: Shan-Hung Wu
- Researched on neural tangent kernel (NTK) and neural network Gaussian process (NNGP). Studied the trainability and generalization ability of neural network and published a paper "**Neural Tangent Generalization Attacks**" in **ICML'21**.
- Researched on the intersection of machine learning and computer security, with a focus on adversarial example and robustness and published a paper "**Adversarial Robustness via Runtime Masking and Cleansing**" in **ICML'20**.
- Researched on computer vision, with a focus on face recognition. Designed a face recognition model with the ability to detect and resist adversarial examples, especially for real-world attacks.

DataLab, National Tsing Hua University *Sep. 2018 – Aug. 2019*
UNDERGRADUATE RESEARCH ASSISTANT *Hsinchu, Taiwan*
- Advisor: Shan-Hung Wu

- Researched on natural language processing, with focus on document ranking and passage retrieval. Designed a model for search engine query-document ranking and achieved **13th place** in MS MARCO passage retrieval task.

Advanced Optoelectronic Materials Research Group, National Tsing Hua University *Sep. 2017 – Jun. 2018*
UNDERGRADUATE RESEARCH ASSISTANT *Hsinchu, Taiwan*
- Advisor: Hao-Wu Lin
- Researched on next-generation organic-inorganic hybrid and nano-materials.

Physics of Molecular and Biological Matter, University of Tübingen *Oct. 2016 – Jul. 2017*
UNDERGRADUATE RESEARCH ASSISTANT *Tübingen, Germany*
- Advisor: Frank Schreiber
- Researched on topography and morphology of solar cell and coupled organic-inorganic nanostructure.

Publications

Meta Adversarial Perturbations | Paper *AAAI Workshop'22*
CHIA-HUNG YUAN, PIN-YU CHEN, CHIA-MU YU *Vancouver, Canada*
- Proposed a meta adversarial perturbation (MAP), a better initialization that causes data to be misclassified with high probability after being updated through only a one-step gradient ascent update.
- MAP achieves 10-20% improvement, compared with naïve fast gradient signed method.

Neural Tangent Generalization Attacks | Paper | Video | Code | Competitions *ICML'21*
CHIA-HUNG YUAN, SHAN-HUNG WU *Virtual*
- Devised neural tangent generalization attack (NTGA), the first efficient work enabling clean-label, black-box generalization attacks against deep neural networks, making trained networks fail to generalize to unknown data.
- NTGA decreases the generalization ability sharply, i.e. 99% -> 15%, 92% -> 33%, 99% -> 72% on MNIST, CIFAR10 and 2-class ImageNet, respectively.

Adversarial Robustness via Runtime Masking and Cleansing | Paper | Video | Code *ICML'20*
YI-HSUAN WU, **CHIA-HUNG YUAN**, SHAN-HUNG WU *Virtual*
- Devised runtime masking and cleansing (RMC), a new defense method, to improve adversarial robustness.
- RMC achieves robustness ~98% on MNIST, ~85% on CIFAR-10, ~60% on ImageNet, respectively.

Honors & Awards

- **Honorary Member of The Phi Tau Phi Scholastic Honor Society of R.O.C.** (top 3% master's graduands) *2021*
- **Honorary Member of The Phi Tau Phi Scholastic Honor Society of R.O.C.** (top 1% undergraduate graduands) *2018*
- **Academic Achievement Award 3 times** (top 5% students in the class with highest GPA) *2015, 2016, 2018*
- **International Exchange Scholarship** (200,000 NTD/~$7,000) *2016*
- **1st place, Business Case Competition of Seminar on International Trade and Economy** *2016*

Patent

- Shan-Hung Wu, **Chia-Hung Yuan**, "Data Poisoning Method and Data Poisoning Apparatus". US Patent App. No. US17/705,411. TW Patent No. TWI814213B.

Skills & Others

Teaching Assistant	CS565600 Deep Learning, National Tsing Hua University: Fall 2019, Fall 2020
Reviewer	NeurIPS'19-21, ICML'20-21, ICLR'21, AAAI'20-21, CVPR'21, IJCAI'20, CIKM'19-20
Languages	Mandarin (Native); English (Fluent, GRE 325/340; TOEFL 109/120); German (Intermediate)
Programming	C/C++, Python, Swift, React Native, HTML, CSS, JavaScript, Matlab
Libraries/Tools	TensorFlow, Keras, Jax, PyTorch, OpenCV, Scikit-learn
Interests	Football (I have a YouTube channel!), Photography, Travel, Bartending, Ice Skating