Qiming Wu

(ACM Member & IEEE Student Member)

Email: qimingwu@hust.edu.cn | Address: Room B309, National Laboratory for Optoelectronics (NLO), Huazhong University of Science and Technology, 430000, China

EDUCATION

Huazhong University of Science and Technology (HUST) Wuhan, China

Bachelor of Engineering in Electronic Information Engineering 09/2018-Present

Overall GPA: 3.7/4.0

Awards & Honors:

1. The People's Scholarship in China - Scientific and Technological Innovation Scholarship, HUST (Top 5%) (2020 & 2021);
2. The People's Scholarship in China - Perseverance Scholarship, HUST (Top 7%) (2019, 2020 & 2021);
3. The People's Scholarship in China - Public Welfare Scholarship, HUST (Top 10%) (2019);
4. **Second Prize**, May Fourth Speech Competition, HUST (2019);
5. **Third Prize**, Asia and Pacific Mathematical Contest in Modeling (**APMCM**) (2019)
6. China-Japan Youth Ambassador (2017)

TECHNICAL SKILLS & LANGUAGES

Computer Skills: Python, C, PHP, MySQL, PyTorch, MATLAB, LaTeX

Languages: Native Chinese, Fluent English, Basic Germany (A1)

PUBLICATIONS (†: *FIRST AUTHOR*, *: *UNDER REVIEW*)

- **Q. Wu**†, Z. Zou, P. Zhou, X. Ye, B. Wang, A. Li, "Towards Adversarial Patch Analysis and Certified Defense against Crowd Counting", *In Proceedings of **ACM Multimedia**, 2021. (**Poster**, **Accept rate: 542/1942 = 27.9%**)*
- *__Q. Wu__†, X. Chen, Y. Jiang, P. Zhou, Z. Wang, "Lottery Image Prior", *In Proceedings of **International Conference on Learning Representations** (ICLR), 2022.*
- *W. Qu †, **Q. Wu**†, P. Zhou, P. Xu, B. Li, "Reg-IBP: Efficient and Scalable Training for Robust Neural Networks via Interval Bound Propagation", *In Proceedings of **IEEE International Conference of Computer Vision** (ICCV), 2021.*
- *W. Qu†, **Q. Wu**†, P. Zhou, B. Wang, "Certified Radius-Guided Attacks and Efficient Robustness Training against Deep Neural Networks", *In Proceedings of **IEEE Symposium on Security and Privacy**, 2021.*

PATENTS

1. *"**A Certified Radius-Guided Attack Method, Optimization Training Approach and System**", Patent Number: ZL202110583029.7, China National Intellectual Property Administration, 2021.*
2. *"**Momentum-based Method and System for Generating Adversarial Examples against Crowd Counting Models**", Patent Number: ZL202110588717.2, China National Intellectual Property Administration, 2021.*

RESEARCH EXPERIENCE

"*Towards Adversarial Patch Analysis and Certified Defense against Crowd Counting*", Department of Computer Vision Technology, Baidu Inc. (Remote) Shanghai, China

*Intern, Mentor: Xiaoqing Ye (**Senior Researcher & Engineer**), Zhikang Zou (**R&D Engineer**)* 12/2020 - 04/2021

- Aimed to establish the first set of robustness evaluation benchmark on the crowd counting task and provide a new way for researchers to solve the robustness problem of vulnerable deep learning models towards evasion attack
- Employed Python to build adversarial robustness CNN-based crowd counting models on the Linux-based deep learning server
- Incorporated the congested scene information into the adversarial patch to degrade the performance of crowd counting systems by perturbing less than **6%** of image pixels whereby the attacked Mean Absolute Error (MAE) is sevenfold than normal
- Put forward the first regression model-based Randomized Ablation (RA) to better enhance the adversarial robustness of crowd counting models than Adversarial Training (ADT) considered that MAE of RA is 5 lower than ADT on clean samples and 30 lower than ADT on adversarial examples
- This paper was accepted by the *Proceedings of **ACM Multimedia (MM) 2021 (Top conference on multimedia, CCF-A)***.

"*Lottery Image Prior*", Visual Informatics Group (VITA Laboratory), ECE Department, University of Texas at Austin. (Remote) Austin, United States

*Research Intern, Advisor: Prof. Zhangyang Wang (**UT Austin**)* 04/2021 - 10/2021

- Aimed to find the sparse network with the image prior property (***LIP***, which benefits image inverse problems such as denoising, inpainting and super-resolution for its low-computational cost and better performances)
- Employed Python and Anaconda to find the matching subnetworks of multi models (Untrained neural network: Deep Image Prior (DIP model); Pretrained neural network: PGAN) via *Lottery Ticket Hypothesis* on the Linux-based deep learning server
- Successfully find the matching subnetworks that their performances are comparable or even better than the full model (DIP model: sparsity range from **20%** to **87%**; PGAN: sparsity range from **5%** to **36%**)
- We also find that these found subnetworks of DIP models are able to transfer across images from various domains and we also propose the novel method: ***Weight-sharing Lottery Image Prior***, which aims to find the subnetworks that can transfer across different image restoration tasks. Our results show that LIP could transfer across the inverse problems like denoising, inpainting and super-resolution in the setting of DIP models. Also, ***LIP*** could transfer successfully from the compressed sensing task to the inpainting task in the setting of ***Generative Adversarial Nets (GANs)***.
- Wrote an EI paper with LaTeX and submitted to the *Proceedings of International Conference on Learning Representations (ICLR), 2022.*

"*Certified Radius-Guided Attacks and Efficient Robustness Training against Deep Neural Networks*", NSF Industry-University Cooperative Research Center (IUCRC) for Alternative Sustainable and Intelligent Computing (ASIC), Duke University (Remote) Durham, United States

*Research Intern, Advisors: Prof. Binghui Wang (**IIT**) & Prof. Yiran Chen (**Duke**)* 08/2020 - 02/2021

- Presented the first CR-guided evasion attack and robustness retraining strategy to better enhance the robustness of DNN models based on the observation that CR can reveal internal weakness information of DNN models
- Utilized Python to design a new evasion attack and defense method for semantic segmentation and image classifier based on the deep learning server of Linux system
- Conducted the white-box adversarial attack with CR-guided method and its effect is much better than the FGSM (Fast Gradient Sign Method) with MioU ratio: **0.34** VS **0.43**
- Wrote an EI paper with LaTeX and submitted the paper on the *IEEE Security and Privacy* 2021 for review

"*Reg-IBP: Efficient and Scalable Training for Robust Neural Networks via Interval Bound Propagation*", Big Data Intelligence and Information Security Laboratory, HUST Wuhan, China

*Research Assistant, Advisors: Prof. Pan Zhou (**HUST**) & Prof. Bo Li (**UIUC**)* 12/2020-04/2021

- Adopted Python to propose a multi-step training strategy based on interval bound propagation with a carefully designed regularization term named Reg-IBP that is adaptive to both image classification and regression problems to resolve present challenges for deterministic certified defenses given their tight robustness bounds
- Used regularization knowledge in the optimization theory of machine learning and added L1 regularization in the robust training of the model to improve the performance, which is verified by two popular crowd counting datasets (ShanghaiTech part A and part B), along with three image classification datasets (MNIST, CIFAR-10, and Tiny-ImageNet)
- Wrote an EI paper with LaTeX and submitted the paper to the *ICCV* 2021 for review

EXTRACURRICULAR ACTIVITIES

1. *Volunteer*, do preparation works for the talk of **Prof. Yingyan Lin** (**Rice University**) to students in Big Data Intelligence and Information Security Lab, HUST 10/2020
2. *Volunteer*, do preparation works for the talk of **Prof. Binghui Wang** (**CS Department, Illinois Institute of Technology, IIT**) to students in Big Data Intelligence and Information Security Lab, HUST 07/2020
3. *Volunteer*, do preparation works for the talk of **Prof. Cihang Xie** (**University of California Santa Cruz**) to students in Big Data Intelligence and Information Security Lab, HUST 06/2020
4. *Volunteer*, during the visit of **Prof. Le Song** (**Deputy Department Chair at Mohamed bin Zayed University of Artificial Intelligence**) to Huazhong University of S & T (HUST) 12/2019
5. *Volunteer*, National Undergraduate Electronics Design Contest 07/2019 - 08/2019
6. *Basketball Player*, **Most Valuable Player (MVP)**, The 19th Basketball Competition of the School of Electronics Information and Communications (EIC), Huazhong University of S & T (HUST) 06/2019
7. *Volunteer*, during the visit of **Prof. Brian A. Barsky** (**University of California Berkeley**) to Huazhong University

of S & T (HUST) 05/2019

8. *Participant*, Present Around the World **(PATW)** Competition Hosted by The Institution of Engineering and Technology **(IET, U.K)** (**Second Prize** in the HUST Competition Area) 03/2019
9. *Volunteer*, Library Volunteering Service, the library of Hubei Province, China 11/2018