Qiming Wu

Homepage: https://harrywuhust2022.github.io/ │**Phone**: +86-15950116533 │**Email**: wqmhust@163.com
Add.: 16-503 HaiLanMingHuaYuan, Jiangyin, Jiangsu, 214400, China

EDUCATION BACKGROUND

Huazhong University of Science and Technology (HUST) Wuhan, China
Bachelor of Engineering in Electronic and Information Engineering 09/2018-06/2022
Overall GPA: 3.71/4.0
Awards & Honors:

1. The People's Scholarship in China - Scientific and Technological Innovation Scholarship, HUST (Top 7.5%) (2020, 2021);
2. The People's Scholarship in China - Perseverance Scholarship, HUST (Top 12.5%) (2019, 2020 & 2021);
3. The People's Scholarship in China - Public Welfare Scholarship, HUST (Top 15%) (2019);
4. **Second Prize**, May Fourth Speech Competition, HUST (2019)
5. **Third Prize**, Asia and Pacific Mathematical Contest in Modeling (**APMCM**) (2019)

PUBLICATIONS *(†: FIRST AUTHOR, *: UNDER REVIW.)*

- **Qiming Wu†**, Zhikang Zou, Pan Zhou, Xiaoqing Ye, Binghui Wang, Ang Li. "Towards Adversarial Patch Analysis and Certified Defense against Crowd Counting", *the proceedings of ACM Multimedia 2021*. (**Accepted**)
- ***Qiming Wu†**, Xiaohan Chen, Yifan Jiang, Pan Zhou, Zhangyang Wang. "Lottery Image Prior", *the proceedings of ICML 2022*.
- *Wenjie Qu†, **Qiming Wu†**, Zhikang Zou, Pan Zhou, Bo Li. "Bound Tightening Network for Robust Crowd Counting", *the proceedings of ICIP 2022.*
- *Wenjie Qu†, **Qiming Wu†**, Pan Zhou, Binghui Wang. "Defending against Attacks to Image Segmentation via Combining Certified Radius with Robust Training", *the proceedings of IJCAI 2022.*

PATENTS *(†:INVESTOR)*

- **Qiming Wu†**, Hongting Zhang, Pan Zhou, Zichuan Xu, Cai Fu, Xiaofeng Ding. 2021. "Momentum-based Adversarial Example Generation method against Crowd Counting System." China Patent ZL202110588717.2, (filed May 28, 2021, and issued September 21, 2021).
- **Qiming Wu†**, Wenjie Qu†, Pan Zhou, Yulai Xie, Ruixuan Li. 2021. "A Certified Radius Guided Attack, Optimization Training Method and System." China Patent ZL202110583029.7, (filed May 27, 2021, and issued September 14, 2021).

PROFESSIONAL EXPERIENCE

NVIDIA **Shanghai, China**
Deep Learning Software QA Engineer Intern, Advisor: Di Wu (Software Engineer in NVIDIA) 02/2022-Present

- Conduct GPU Software testing and test automation improvement for Nvidia Deep Learning Software products, such as cuDNN, TensorRT, Nvidia optimized Frameworks (E.g. TensorFlow, PyTorch.);
- Responsible for functionality, compatibility, and performance tests in DL SW stack release;
- Work with development teams to triage issues, root cause analysis, verify fixes, define new tests, and improve test plans.

RESEARCH EXPERIENCE

"Lottery Image Prior", Visual Informatics Group, The University of Texas at Austin Remote
Research Assistant, Advisor: Prof. Zhangyang Wang 04/2021-10/2021

- Put forward an innovative concept, given a (untrained or trained) DNN-based image prior, which have a sparse subnetwork that can be training in isolation, to match the original DNN's performance when being applied as a prior to regularizing various image inverse problems
- Got the lottery image prior by adopting the weight-sharing iterative magnitude pruning based on Lottery Ticket Hypothesis, calculating the value of loss of inputted samples, applying backpropagation technology for models, and pruning some model parameters

- Gained the excellent image prior performance after 86.58% parameters were pruned off, and these subnetworks can perform better than the dense mode, which also can be successfully transferred to different tasks with better performance than the dense model in these tasks

"Reg-IBP: Efficient and Scalable Training for Robust Neural Networks via Interval Bound Propagation",
National Laboratory for Optoelectronics, 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)
- Specifically, on the challenging CIFAR10 dataset, the verification error of models trained by Reg-IBP is 2.74% lower than that of those based on IBP when perturbation $\varepsilon = 2/255$, 4.11% lower than those trained with the state-of-the-art CROWN-IBP when $\varepsilon = 8/255$, and 7.61% lower than that based on CROWN-IBP when $\varepsilon = 16/255$.
- Wrote an IEEE paper titled "Bound Tightening Network for Robust Crowd Counting" by Latex and submitted to the *ICIP 2022* for review

"Certified Radius-Guided Attacks and Efficient Robustness Training against Deep Neural Networks",
National Laboratory for Optoelectronics, HUST Wuhan, China
Research Assistant, Advisors: Prof. Pan Zhou (HUST) & Prof. Yiran Chen (Duke) 09/2020-01/2021

- 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 titled "Defending against Attacks to Image Segmentation via Combining Certified Radius with Robust Training" with LaTex and submitted the paper to the *IJCAI 2022* for review

"Towards Adversarial Patch Analysis and Certified Defense against Crowd Counting",
National Laboratory for Optoelectronics, HUST Wuhan, China
Undergraduate Researcher, Advisors: Prof. Pan Zhou (HUST) & Xiaoqing Ye (Baidu) 09/2019-06/2020

- 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
- Wrote an EI paper with LaTex and the paper was accepted by *ACM Multimedia* 2021

EXTRACURRICULAR ACTIVITIES

Volunteer, **National Undergraduate Electronics Design Contest** 07/2019-08/2019
Reporter, **Investigation on the Status Quo of Rural Education in Xianning City, Hubei Province** 07/2019
Participant, **Present Around the World Competition Hosted by The Institution of Engineering and Technology** (**Second Prize** in the HUST Competition Area) 03/2019
Volunteer, **Library Volunteering Service Activity** 11/2018

TECHNICAL SKILLS & LANGUAGES

Computer Skills: Python, C, PHP, MySQL, PyTorch, MATLAB, LaTeX
Languages: Native Chinese, Fluent English, Basic German (A1)