Qidong Huang

Ph.D, University of Science and Technology of China

Building No.7, USTC West Campus
Hefei, Anhui, China
(+86) 13085060686
hqd0037@mail.ustc.edu.cn

Short Biography

Qidong Huang is a PhD student at University of Science and Technology of China. He has published more than 7 papers at top1-tier conferences and journals, such as CVPR/ICCV/AAAI/TIP/TCSVT. His research interests focus on vision transfer learning (e.g., prompt learning for vision pretrained models) and artificial intelligence security (e.g., adversarial examples and anti-DeepFake). He is the reviewer of many top conferences (including CVPR, ICCV, ECCV) and top journals (TNNLS, PR).

Education

09/2020–present **PhD of Cyberspace Security**, *University of Science and Technology of China*, Hefei, China, CAS Key Laboratory of Electromagnetic Space Information. Supervised by Prof. Weiming Zhang.

09/2016–06/2020 **Bachelor of Information Security**, *School of Information Science and Technology, University of Science and Technology of China*, Hefei, China.

Skills

- ⋆ **Expertise in vision prompt learning :** I have been researching the prompt learning for large-scale vision pretrained models and published one paper on top-tier computer vision conferences, in which I propose DAM-VP, a data diversity-aware method for efficient and adaptive vision prompt learning. This work alleviates the mismatch between vision prompts and downstream data diversity.
- ⋆ **Expertise in artificial intelligence security :** I have been studying artificial intelligence security since 2020, including adversarial attack&defense and anti-DeepFake. For adversarial attack, I propose SI-Adv, a shape-invariant attack for 3D point cloud recognition which great boosts the imperceptibility of adversarial examples. For adversarial defense, I propose a contrastive adversarial training framework for robust point cloud recognition named PointCAT. Besides, our work for improving adversarial robustness of masked autoencoders has been recently accepted by ICCV 2023. For anti-DeepFake, we are the first to propose the concept of "initiative defense" against DeepFakes by proactively protecting users' facial privacy before the manipulation, unlike previous ex-post countermeasures like DeepFake detection.

Publications (First Author)

- ⋆ **Qidong Huang**, Xiaoyi Dong, Dongdong Chen, Yinpeng Chen, Lu Yuan, Gang Hua, Weiming Zhang, Nenghai Yu. Improving Adversarial Robustness of Masked Autoencoders via Test-time Frequency-domain Prompting. *International Conference on Computer Vision (ICCV), 2023.*
- ⋆ **Qidong Huang**, Xiaoyi Dong, Dongdong Chen, Weiming Zhang, Feifei Wang, Gang Hua, Nenghai Yu. Diversity-Aware Meta Visual Prompting. *Conference on Computer Vision and Pattern Recognition (CVPR), 2023.*
- ⋆ **Qidong Huang**, Xiaoyi Dong, Dongdong Chen, Hang Zhou, Weiming Zhang, Nenghai Yu. Shape-invariant 3D Adversarial Point Clouds. *Conference on Computer Vision and Pattern Recognition (CVPR), 2022.*

- ⋆ **Qidong Huang***, Jie Zhang*, Wenbo Zhou, Weiming Zhang, Nenghai Yu. Initiative Defense against Facial Manipulation. *AAAI Conference on Artificial Intelligence (AAAI), 2021.* (*Qidong Huang and Jie Zhang contribute equally.)
- ⋆ **Qidong Huang**, Xiaoyi Dong, Dongdong Chen, Hang Zhou, Weiming Zhang, Kui Zhang, Gang Hua, Nenghai Yu. PointCAT : Contrastive Adversarial Training for Robust Point Cloud Recognition. *IEEE Transactions on Image Processing (TIP), Major Revision.*

Publications (Collaborate)

- ⋆ Kui Zhang, Hang Zhou, Jie Zhang, **Qidong Huang**, Weiming Zhang, Nenghai Yu. Ada3Diff : Defending against 3D Adversarial Point Clouds via Adaptive Diffusion. *ACM International Conference on Multimedia (MM), 2023*
- ⋆ Han Fang, Dongdong Chen, **Qidong Huang**, Jie Zhang, Zehua Ma, Weiming Zhang and Nenghai Yu. Deep Template-based Watermarking. *IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2020.*
- ⋆ Jie Zhang, Dongdong Chen, **Qidong Huang**, Jing Liao, Weiming Zhang, Huamin Feng, Gang Hua, Nenghai Yu. Poison ink : Robust and invisible backdoor attack. *IEEE Transactions on Image Processing (TIP), 2022.*

Services

- ⋆ Reviewer for CVPR 2022, 2023
- ⋆ Reviewer for ICCV 2023
- ⋆ Reviewer for ECCV 2022
- ⋆ Reviewer for ICPR 2022
- ⋆ Reviewer for IEEE Transactions on Neural Networks and Learning Systems (TNNLS)
- ⋆ Reviewer for Pattern Recognition (PR)

Awards & Honors

2021 China National Scholarship