Bowei Tian

boweitian@outlook.com | +86-13677130812

EDUCATION

Wuhan University, Wuhan, CHN 09/2020-06/2024

Bachelor of Engineering in **Information Security**, expected in June 2024

- Cumulative GPA: **3.90/4**; Average Score: **91.3/100**; Ranking: 10/167 (all students in my major)
- Scholarship: Lei Jun Computer Undergraduate Scholarship (top 2%)

PUBLICATIONS

- **B. Tian**, R. Du, & Y. Shen. 2023. **FairViT: Fair Vision Transformer via Adaptive Masking**. International Conference on Acoustics, Speech, and Signal Processing (ICASSP) (under review)
- X.Gong*, **B. Tian***, M. Xue, Y. Wu, Y. Chen & Q. Wang. 2023. **An Effective and Resilient Backdoor Attack Framework against Deep Neural Networks and Vision Transformers**. IEEE Transactions on Dependable and Secure Computing (TDSC) (under review)
- X. Gong, **B. Tian**, M. Xue, Y. Chen, Q. Wang, & M. Sun. **MEGATRON: Backdooring Vision Transformers with Invisible Triggers**. (under review)
- M. Xue, Y. Zeng, S. Gu, Q. Zhang, B. Tian & C. Chen. SDE: SDE: Early Screening for Dry Eye Disease with Wireless Signals. In Ubicomp/IMWUT
- **B. Tian**, Y. Cao, Q. Wang, X. Gong, C. Shen & Q. Li. **Adversarial Sample Defense Methods and Devices based on Model Inversion Methods**. CHN Patent
- Y. Cao, **B. Tian**, Q. Wang, X. Gong, C. Shen & Q. Li. **A Deep Neural Network Model Inversion Attack Defense Method and Device**. CHN Patent
- J. Chen, X. Yan, S. Cen, Q. Ma, K. Qian, Y. Chen, K. Su, B. Tian, L. Lu & C. Gan. Virtuoso in the Virtual: Building Digital Rappers with Coherent Vocals and Human Motion. (in preparation)

RESEARCH EXPERIENCE

Shen's Lab, University of California, Irvine 06/2023-Present

Research Assistant for Prof. Yanning Shen, **Fairness on Vision Transformers** 06/2023-Present

- Aimed to improve the fairness-accuracy tradeoff of vision transformers
- Conducted experiments and proved that the proposed methods achieve higher accuracy than alternatives, 6.72% higher than the best alternative while reaching a similar fairness result
- Submitted a paper to ICASSP as the first author

Network Information System Security & Privacy (NIS&P) Lab, Wuhan University 04/2022-Present

Research Assistant for Prof. Qian Wang, **Backdoor on Transformers** 10/2022-Present

- Intended to limit the scope of trigger to raise the stealthiness of backdoor in transformers and manipulate the attention mechanism called "Attention diffusion" to improve attack elasticity
- Created Python codes based on PyTorch/Colab to realize scope limitation and attention diffusion
- Achieved high stealthiness and efficiency, surpassing the baselines in Vision Transformers by 25%+
- The paper is under review in a top-conference.

Research Assistant for Prof. Qian Wang, **Backdoor against Neural Networks** 04/2023-07/2023

- Extended the proposed QoE attack method of Deep Neural Networks (DNN)
- It is shown that we can increase the attack success rate by as much as 82% over baselines when the poison ratio is low and achieve a high QoE of the backdoored samples.
- Submitted to IEEE Transactions on Dependable and Secure Computing (TDSC)

Research Assistant for Dr. Meng Xue, **Dry Eye Disease Detection** 01/2023-05/2023

- Proposed to use radar, a more convenient, contactless, and ubiquitous way, to detect Screening dry eye disease
- Analyzed the structure of focal loss-based Transformer model in Colab to detect dry eye disease
- Ran various kind of ablation studies, reorganizing codes and implementing functions such as data enhancement, dataset splitting, model fine-tuning
- A paper titled "SDE: Early Screening for Dry Eye Disease with Wireless Signals" is accepted in Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMMUT)

Research Assistant for Prof. Qian Wang, **Model Inversion Defense** 04/2022-01/2023

- Utilized Python to design API for several large-scale databases (including ImageNet, CIFAR-10, and GTSRB)
- Established and analyzed codes of GAN model raised in the latest model inversion paper MIRROR (NDSS'22)
- Produced two CHN patents

MIT-IBM Watson AI Lab, Massachusetts Institute of Technology 09/2023-Present

Research Assistant for Prof. Chuang Gan, **Rapper Pose Recognition and Generation** 09/2023-Present

- Cooperated with Prof. Chuang Gan and Mr. Jiaben Chen.
- Regenerated the codes of Openpose (PAMI 2019) and TALKSHOW (CVPR 2023).
- Reorganized the motion-data from rappers on Youtube and regularize them by the YOLO algorithms to build part of pipelines.
- The co-authored paper is in preparation.

SKILLS

- Programming Language: C/C++, Python, MATLAB