Bowei Tian

btian1@umd.edu | Personal website

EDUCATION

University of Maryland, College Park, MD, USA 09/2024-05/2029

1st year Ph.D. student of Electrical and Computer Engineering, expected in May 2029

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

Bachelor degree of Engineering in Information Security, received in June 2024

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

PUBLICATIONS

- **B. Tian**, R. Du, Y. Shen. 2024. **FairViT: Fair Vision Transformer via Adaptive Masking**. European Conference on Computer Vision (ECCV)
- M. Xue*, Y. Zeng*, S. Gu, Q. Zhang, **B. Tian**, C. Chen. 2024. **SDE: SDE: Early Screening for Dry Eye Disease with Wireless Signals**. The ACM international joint conference on Pervasive and Ubiquitous Computing (Ubicomp/IMWUT)
- **B. Tian**, Y. Cao, Q. Wang, X. Gong, C. Shen, Q. Li. 2023. **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. 2023. **A Deep Neural Network Model Inversion Attack Defense Method and Device**. CHN Patent

PREPRINTS

- **B. Tian**, Z. Wang, S. He, W. Ye, G. Sun, Y. Dai, Y. Wu, A. Li. 2024. **Towards counterfactual fairness thorough auxiliary variables**.
- X.Gong*, **B. Tian***, M. Xue, Y. Wu, Y. Chen, Q. Wang. 2024. **An Effective and Resilient Backdoor Attack Framework against Deep Neural Networks and Vision Transformers**.
- X. Gong, **B. Tian**, M. Xue, Y. Chen, Q. Wang, M. Sun. 2023. **MEGATRON: Backdooring Vision Transformers with Invisible Triggers**.
- Z. Wang, **B. Tian**, Y. He, Z. Shen, L. Liu, A. Li. 2024. **One Communication Round is All It Needs for Federated Fine-Tuning Foundation Models**.
- S. He, T. Ge, G. Sun, **B. Tian**, X. Wang, A. Li, D. Yu. 2024. **Router-Tuning: A Simple and Effective Approach for Enabling Dynamic-Depth in Transformers**.
- W. Ye, S. Chen, Z. Shen, Y. He, Z. Wang, G. Sun, **B. Tian**, A. Li. 2024. **ECHO: Enhanced Cognitive Operations Robotics**.

PREVIOUS 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
- The paper "FairViT: Fair Vision Transformer via Adaptive Masking" is accepted in the European Conference on Computer Vision (ECCV 2024).

MIT-IBM Watson AI Lab, Massachusetts Institute of Technology 09/2023-11/2023

Research Assistant for Prof. Chuang Gan, **Rapper Pose Recognition and Generation** 09/2023-11/2023

- 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.

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%+

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

SKILLS

- Programming Language: C/C++, Python, MATLAB, SPSS, Web Development