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**
- TOFEL: **101**, GRE: **321+3**
- Scholarship: Lei Jun Computer Undergraduate Scholarship （雷军计算机本科生奖学金）(2%)

PUBLICATIONS

- **Bowei Tian**, R. Du, Y. Shen. FairViT: Fair Vision Transformer via Adaptive Masking. Submitted to ICASSP (in rebuttal, receives positive comments from 3/3 reviewers).
- X. Gong*, **Bowei Tian***, M. Xue, Y. Wu, Y. Chen, Q. Wang. An Effective and Resilient Backdoor Attack Framework against Deep Neural Networks and Vision Transformers. Submitted to TDSC.
- X. Gong, **Bowei Tian**, M. Xue, Y. Chen, Q. Wang, M. Sun. MEGATRON: Backdooring Vision Transformers with Invisible Triggers. In submission.
- M. Xue, Y. Zeng, S. Gu, Q. Zhang, **Bowei Tian**, C. Chen. SDE: Early Screening for Dry Eye Disease with Wireless Signals. In Ubicomp/IMWUT.
- **田博为**, 曹雨欣, 王骞, 龚雪鸾, 沈超, 李琦. Adversarial sample defense methods and devices based on model inversion methods 基于模型反演方法的对抗样本防御方法和设备. CHN Patent.
- 曹雨欣, **田博为**, 王骞, 龚雪鸾, 沈超, 李琦. A Deep Neural Network Model Inversion attack defense method and device 一种深度神经网络模型反演攻击防御方法及设备. CHN Patent.
- A co-authored paper submitted to a top-conference in MIT-IBM Watson AI Lab.

RESEARCH INTERESTS

- AI Security and Privacy & Computer Vision & Interpretability
- **My research goal** is to find out what the "**information**" in all kinds of neural network means, in which we can formalize it and save huge amount of deduction and transportation price and time. Some preliminary trials: eigenvectors as information, information entropy as information, eta.
- **My working style** is **idea-oriented** and somehow **logical**.

RESEARCH EXPERIENCE

UCI 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
- Experimental results show the proposed methods achieve higher accuracy than alternatives, 6.72% higher than the best alternative while reaching a similar fairness result.
- Submitted to International Conference on Acoustics, Speech and Signal Processing (ICASSP).

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%+.
- Submitted to a top-conference in security.

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

- Extend proposed QoE attack method of Deep Neural Networks (DNN).
- It is shown that we can increase the attack success rate much 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 patents: *Adversarial Sample Defense Methods and Devices based on Model Inversion Methods* and *A Deep Neural Network Model Inversion attack defense method and device.*

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

Research Assistant for Prof. Chuang Gan, **Rapper Pose Recognition and Generation** 06/2023-Present

- Cooperate with Prof. Chuang Gan and Mr. Jiaben Chen.
- Regenerate the codes of Openpose (PAMI 2019) and TALKSHOW (CVPR 2023).
- Reorganize the motion-data from rappers on Youtube and regularize them by the YOLO algorithms to build part of pipelines.
- The co-authored paper is submitted to a top-conference.

SELECTED PROJECTS

Game Development: Pac-Man 07/2021

- Designed a role play game that allows users to play against the ghost (AI) and eat as many beans as possible in a maze
- Utilized C programming language and A* algorithm to traverse all the location of the maze to avoid the ghost and set direction for movement to eat beans
- Achieved a high score that defeated 90%+ rivals

SKILLS

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