Tao Bai

Ph.D.
School of Computer Science & Engineering
Nanyang Technological University
Singapore

bait0002@ntu.edu.sg
https://tao-bai.github.io/

Research Interests

Adversarial Machine Learning, Image Forensics

Security and Privacy

Education

Ph.D. Computer Science, Nanyang Technological University, Singapore — Jan. 2019– Aug. 2022
Advisors: Prof. Jun Zhao, Prof. Bihan Wen

B.E. Remote Sensing, Wuhan University, China — Sept. 2014–Jun. 2018

Experiences

Research Assistant — Feb. 2018–Oct. 2018
Services Computing Technology and System Lab, Huazhong University of Science and Technology
Advisor: Prof. Hong Huang
Topic: Data Mining, Scientific Impact Analysis

Research Assistant — Nov. 2018–Dec. 2018
School of Computer Science & Engineering, Nanyang Technological University
Advisor: Prof. Jun Zhao
Topic: Privacy-preserving Data Analytic

Research Intern — Jun. 2021–Dec. 2021
Huawei 2012 laboratories, Singapore
Advisors: Dr. Lin Hsiao Ying and Dr. Chengfang Fang
Topic: Adversarial Attack, Object Detection, Transformer

Research Intern — May. 2022–Aug. 2022
SONY AI, Tokyo
Advisors: Dr. Lingjuan Lyu
Topic: Adversarial Robustness, Model Compression

Publications

PREPRINTS

1. **T. Bai**, J. Zhao, L. Guo, and B. Wen. Adversarial Purification through Representation Disentanglement. *arXiv preprint arXiv:2110.07801*, 2021. Under Review of TDSC.
2. **T. Bai**, J. Zhao, and B. Wen. Guided Adversarial Contrastive Distillation for Robust Students. *arXiv preprint arXiv:2009.09922*, 2020. Under Review of TIFS.
3. J. Zhao and **T. Bai**. Reviewing and Improving the Gaussian Mechanism for Differential Privacy. *arXiv preprint arXiv:1911.12060*, 2019. In submission.
4. L. Sun, J. Zhao, X. Ye, S. Feng, T. Wang, and **T. Bai**. Conditional Analysis for Key-Value Data with Local Differential Privacy. *arXiv preprint arXiv:1907.05014*, 2019.

JOURNAL ARTICLES

5. **T. Bai**, J. Zhao, J. Zhu, S. Han, J. Chen, B. Li, and A. Kot. Towards Efficiently Evaluating the Robustness of Deep Neural Networks in IoT Systems: A GAN-based Method. *IEEE Internet of Things Journal*, pages 1–1, 2021.
6. **T. Bai**, J. Luo, and J. Zhao. Inconspicuous adversarial patches for fooling image recognition systems on mobile devices. *IEEE Internet of Things Journal*, pages 1–1, 2021.

CONFERENCE ARTICLES

7. J. Luo, **T. Bai**, and J. Zhao. Generating Adversarial yet Inconspicuous Patches with a Single Image (Student Abstract). *Proceedings of the AAAI Conference on Artificial Intelligence*, 35(18):15837–15838, May 2021.
8. **T. Bai**, J. Luo, J. Zhao, B. Wen, and Q. Wang. Recent Advances in Adversarial Training for Adversarial Robustness. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI-21*, pages 4312–4321, 8 2021. Survey Track.
9. **T. Bai**, J. Zhao, J. Zhu, S. Han, J. Chen, B. Li, and A. Kot. AI-GAN: Attack-Inspired Generation of Adversarial Examples. In *2021 IEEE International Conference on Image Processing (ICIP)*, pages 2543–2547, 2021.

Open Source

tao-bai/attack-and-defense-methods Github
A curated list of papers on adversarial machine learning (adversarial examples and defense methods).
https://github.com/tao-bai/attack-and-defense-methods

Harry24k/adversarial-attacks-pytorch Github
PyTorch implementation of adversarial attacks.
https://github.com/Harry24k/adversarial-attacks-pytorch

Awards

National Endeavor Scholarship, China 2015, 2017

First prize, Top 1.1%, 2016
Contemporary Undergraduate Mathematical Contest in Modeling, China

First Grade Scholarship, China 2017

Meritorious Winner, Mathematical Contest In Modeling, US 2017

Research Scholarship, Singapore 2019–Present

University Teaching for Teaching Assistants 2021

Teaching

1. Teaching Assistant | Nanyang Technological University 2019-2020, Sem 1/2
   CZ1012/CE1012 Engineering Mathematics
2. Teaching Assistant | Nanyang Technological University 2019-2020, Sem 2/Special Term 1
   CZ3006/CE3005 Computer Networks
3. Teaching Assistant | Nanyang Technological University 2019-2020, Sem 1
   CZ3006 Net-Centric Computing
4. Teaching Assistant | Nanyang Technological University 2020-2021, Sem 1
   CZ2001 Algorithms

Professional Service

Senior Program Committee

IEEE SmartGridComm 2022

IEEE PIMRC - Workshop on Metaverse 2022

Associate Editor and Editorial Board

Journal of Artificial Intelligence and Big Data 2021

Journal Reviewing

IEEE Transactions on Information Forensics and Security (T-IFS)

IEEE Transactions on Network Science and Engineering (TNSE)

IEEE Internet of Things Journal (IoTJ)

IEEE Transactions on Dependable and Secure Computing (TDSC)

Machine Learning

Remote Sensing

Frontiers in Computer Science

Conference Reviewing

The 29th International Joint Conference on Artificial Intelligence 2020

AAAI 2021 Workshop: Towards Robust, Secure and Efficient Machine Learning 2021

The 17th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2022) 2022

IEEE SECON 2022 2022

Thirty-Seventh AAAI Conference on Artificial Intelligence 2023

IEEE/CVF Winter Conference on Applications of Computer Vision (WACV) 2023

MENTORING

Chua Shan Jing (NTU SCSE, 2019)

Terence Chan Chin Leng (NTU SCSE, 2019)

Luo Jinqi (NTU SCSE, 2020)

Chan Yan Cheng Jarod (NTU SCSE, 2020)

Kant Mannan (NTU SCSE, 2020)

Cao Shuxin (NTU EEE, 2020)

Lu Yuhao (SJTU, 2020)

Wang Xiaoyu (XJTU, 2020)

Zhao Peizhu (NTU SCSE, URECA, 2020)

Jin Chengkai (NTU SCSE, 2021)