# BOHENG LI

+86 13558893177 ◇ Wuhan, China

Email ◇ LinkedIn ◇ Homepage

## EDUCATION

**Wuhan University**, Wuhan, China 2020 - Present

*B.E. in Information Security* *Expected to graduate with first-class honors*

GPA: 3.91/4.0, Average Score (Credit Weighted): 93.4/100.

Overall Ranking: 1/157, China National Scholarship 2022 (Top 0.2% nationwide)

**Chengdu Foreign Languages School**, Chengdu, China 2014 - 2020

*Middle and High School, Honor Class in Olympic in Informatics (OI)*

## PAPERS UNDER REVIEW (SELECTED)

†: equal contribution, co-first author ✉: corresponding author

Ziheng Huang†, **Boheng Li**†, Yan Cai, Run Wang✉, and Shangwei Guo. "What can Discriminator do? Towards Box-free Ownership Verification of Generative Adversarial Networks" Submitted to the IEEE/CVF Conference on Computer Vision and Patten Recognition (**CVPR**), 2023

Lingzhou Mu†, **Boheng Li**†, and Run Wang✉. "Defending Watermark Removal Attack on DNN Models via Utility Disruption" Submitted to the IEEE/CVF Conference on Computer Vision and Patten Recognition (**CVPR**), 2023

Dongyu Yao, **Boheng Li**✉, and Run Wang. "DIDA: Dual-level Interaction for Domain Adaptive Semantic Segmentation" Submitted to the IEEE International Conference on Multimedia and Expo (**ICME**) , 2023

Run Wang✉, Jixing Ren, **Boheng Li**, Tianyi She, Chenhao Lin, Liming Fang, Jing Chen, Chao Shen, and Lina Wang. "Free Fine-tuning: A Plug-and-Play Watermarking Scheme for Deep Neural Networks" Submitted to the International Joint Conference on Artificial Intelligence (**IJCAI**), 2023

## RESEARCH EXPERIENCES

**AntiE: Exploring Remote Sensing-Empowered Emergency Monitoring Technology** Jan 2021 - Oct 2022
**College Students' Innovative Entrepreneurial Training Plan Program.** Wuhan University *Wuhan, China*
Advisors: Prof. Qingxiang Meng, Prof. Xiaoliang Meng, and Prof. Linqing Liu.

- Served as the co-founder of the team AntiE, which aims at developing emergency monitoring technologies such as emergency transit satellite inquiry, multi-UAV planning, and disaster chain coupling derivation via remote sensing techniques. Our goal is to provide accurate, timely, and comprehensive decision-making references for emergency management departments.
- Implemented project website and project's core algorithms in multi-UAV planning & satellite constellation configuration based on a real-time hexagonal coverage evaluation. We did a comprehensive evaluation of emergency shelters in Wuhan City and our suggestions were accepted by the government. We also got 2 papers published at the 29th International Conference on Geoinformatics and have applied for 4 patents, all are currently in their substantive examination phase.
- We have won many prizes and honors, including the **Gold Reward** of the 8th China International College Students 'Internet+' Innovation and Entrepreneurship Competition, the highest and most valuable competition award for Chinese college students (national-wide). Our technology has been adopted by the Ministry of Emergency Management of Foshan, Chengdu, and Wuhan. We have signed cooperation intentions with dozens of known enterprises in China Mainland.

**AI Lifecycle Security and its Good Use** Aug 2021 - Present
**Research Intern.** Key Laboratory of Aerospace Information Security and Trusted Computing *Wuhan, China*
Advisor: Prof. Run Wang.

- I explore the weakness of Deep Learning models in their lifecycles (e.g., adversarial attacks, backdoor attacks, model extraction attacks) and their countermeasure defenses. I also made efforts on turning these weaknesses into good use, applying on privacy protection and Intellectual Property (IP) protection of deep learning models.

- For attacks, we proposed a flexible and stealthy physical-world conditional backdoor attack via lighting, which can launch threatful backdoor attacks in a single blink. For defenses, we explore naturalness-aware perturbations to efficiently defend against backdoor threats while preserving their normal functions.
- We also made efforts in practical manners for DNN IP protection. We developed a plug-and-play watermarking scheme for DNNs, which can be easily cooperated with multiple models without tedious fine-tuning. We also ingeniously explored the potential of the Discriminator in a well-trained GAN to apply for a practical box-free ownership verification scheme. Furthermore, we developed a simple technique that can defend against the powerful watermark removal attack via utility disruption, assuring its practicability in real-world applications.

## COMPETITION AWARDS (SELECTED)

- **Gold Reward**. The 8th China International College Students "Internet+" Innovation and Entrepreneurship Competition. *2022.11*
- **First Prize**. The 2022 China Mobile Creator Marathon "OnePoint" Special Competition on Spatio-temporal Information. *2022.11*
- **First Prize**. The 15th Chinese Collegiate Computing Competition National Finals. *2022.09*
- **Second Prize**. The Lanqiao Cup Competition National Finals. *2022.08*
- **First Place in Second Prize**. The 2018 National Olympic in Informatics, Sichuan Provincial Competition. *2018.11*

## SCHOLARSHIPS AND HONORS (SELECTED)

- **Pacemaker to Merit Student** (Award Rate: 60/59774=0.1%, 60 candidates per year in WHU), Wuhan University *2022.11*
- **China National Scholarship** (Award Rate: 0.2% national-wide), Ministry of Education, China *2022.10*
- **First Class Scholarship of WHU** (Award Rate: 5% department-wide), Wuhan University *2022.10*
- **Merit Student** (Award Rate: 10% department-wide), Wuhan University *2021.10*
- **HUANG Zhangren Scholarship** (Award Rate: 60/59774=0.1%, 60 candidates per year in WHU), Wuhan University *2021.10*
- **First Class Scholarship of WHU** (Award Rate: 5% school-wide), Wuhan University *2021.10*
- **Excellent Student Cadre** (Award Rate: 924/59774=1.5%) Wuhan University *2021.06*

## ACADEMIC SERVICES

- Sub-Reviewer, International Joint Conference on Artificial Intelligence (IJCAI), 2023
- Sub-Reviewer, IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023
- Sub-Reviewer, AAAI Conference on Artificial Intelligence (AAAI), 2023
- Teaching Assistant, Artificial Intelligence (AI), Undergraduate Students, Fall 2022.

## SKILLS

- Programming Languages: C/C++, Python, JavaScript
- Libraries: Numpy, Pandas, PyTorch, OpenCV, Vue, React
- Developer Tools: Git, LaTeX, VS Code, PyCharm, Jupyter Notebook
- Languages: Mandarin & Sichuan Dialect (Native), English (Fluent)