Zixuan Huang

Beijing University of Posts and Telecommunications, 10 Xitucheng Road, Haidian District, Beijing, China

（+86）13810705181 | Hzx707482606@bupt.edu.cn

EDUCATIONAL BACKGROUND

Beijing University of Posts and Telecommunications, International School   Beijing, China

Joint Program with Queen Mary University of London, School of Electronic Engineering and Computer Science

Bachelor of Science in E-Commerce Engineering with Law; GPA: 85.41/100   **Sep. 2021 - Present**

- **Core Courses:** College Computer (88), Programming Fundamentals-C language (84), Intro Java Programming (84), Scientific Research Literacy and Innovation Ability (about CNN) (88), Operational Research (86), Python Data Analysis and Visualization (95)，Foundation of Artificial Intelligence in Intelligent Medical Field (87), Intelligent Image Recognition (96)

- Third-class scholarship of BUPT   **Dec. 2022. 2023**

- Excellent Student Cadre of BUPT   **Dec. 2022**

SKILLS

Programming: C, HTML, CSS, JS, MySQL, Python, Java

Frameworks & Tools: PyTorch, Anaconda, CUDA, JSP+SERVELT, matplotlib, pandas

Interest or Expertise：Deep Learning, Computer Vision, Large Language Model, Machine Learning

RESEARCH & INTERNSHIP EXPERIENCES

Adversarial Robustness via Deformable Convolution with Stochasticity   **Jun. 2024 - Present**

Advisor: Chang Xu, School of Computer Science, University of Sydney

- Developed a randomized defense strategy to significantly improve model accuracy under adversarial attacks. Achieved accuracy improvements across CIFAR-10, CIFAR-100, ImageNet, and models including ResNet18, ResNet34, ResNet50, WideResNet, Vit.

- Utilized stochastic deformable convolution (DCS), applying masks to simulate DCS to enhance robustness against adversarial attacks.

- Designed the optimal sampling points, randomness, and locations in DCS. Improved **26.07%** robust accuracy under AutoAttack on CIFAR-10 compared to the baseline (achieving SOTA) and contributed a paper as a co-first author to be submitted to ICML 2025.

Robot Exploration Data Management Website Construction   **Jun. 2023 - Dec. 2023**

Coordinator, Experimental Center, School of Computer Science, BUPT, Advisor: Jing Li

- Designed and interacted the front-end web page, back-end part and database. Realized registration, login, modify password, modify record, display data (including text, picture, video), operation error prompt and other functions.

- Constructed the website using JSP+SERVELT architecture. Docked with the actual robot and succeed.

Fruit Recognition   **2023**

Machine learning engineer, China Mobile R&D Center for Network Planning and Optimization, Advisor: Duo Shi

- Developed a fruit recognition model using the ResNet18 architecture, achieving an accuracy of 88.59%.

- Compared the effects of three training methods on ResNet18, 34, 50, selecting the most stable and efficient approach. Gained a deep understanding of the ResNet architecture. Additionally, explored and experimented with Vision Transformer (ViT) in the task.

Front-end and Back-end Internships   **Jul. 2022 - Aug. 2022**

Software engineer, Digital design and Development Center, China Mobile Group Design Institute, Supervisor: Qiang Fei

- Completed the layout of simple form filling interface and commodity interface, using HTML and CSS.

- Learned **HTML, CSS, part of JS and Vue**. Understood the communication engineering and mastered some important computer concepts, including artificial intelligence, cryptography and information security, blockchain.

LEADERSHIP

Member of the College Volunteer Association Office   **Oct. 2021 - June. 2023**

- Held Lei Feng Month activities and led the volunteer evaluation meeting, the school-level volunteer association exchange meeting.

- Managed and oversaw the financial operations of the entire department as the head of the finance team.