Alison Xianting Huang

or Alison Hinting Wong (Cantonese Pron.)
(+86) 13612888369 | hhhxtw02@stu2021.jnu.edu.cn | Guangzhou City, China

EDUCATION

Jinan University (China's National Project 211, Top 1.9% by CWUR 2024), JNU Homepage
Bachelor of Computer Science and Technology (All-English teaching) Sep 2021 – Jun 2025

- GPA: 85+/100
- Related Courses: Advanced Artificial Intelligence (100), Linear Algebra (90), Digital Image Processing (95), Data Structures (91), etc.
- Honors: National Ministry of Education – Hong Kong, Macau & Overseas Students Scholarship

OVERVIEW

- Contributed to 9 research papers.
- Currently involved in 1 national key project.
- Lead 1 national-level student project and 3 provincial/university-level projects.
- Awarded 10+ national/provincial/university-level recognitions.
- Research experience focuses on deep learning, with emphasis on AI security/trustworthy AI.

(This is not means I am limited to this direction. I believe the skills I've gained are transferable, and my main considerations are my research interests and the professor I work with)

PUBLICATIONS

Journal Papers

[J1] S Zhou, ***X Huang*** (Student First Author), MS Obaidat, et al. "Transferability of Adversarial Attacks on Tiny Deep Learning Models for IoT Unmanned Aerial Vehicles"

- Online: IEEE Internet of Things Journal (IoT-J, JCR Q1), DOI: 10.1109/jiot.2023.3329954
- Considering the increased instability of tiny deep learning models under adversarial attacks, we proposed a formula to quantify cross-model performance by integrating the uncertainty of the attacks and model generality. This was empirically supported by experiments combining 22 attack methods with 10 CNN structures.

[J2] K Wang, ***X Huang*** (Student First Author), C Tan, S Yiu, et al. "Optimizing Neural Network Training: A Markov Chain Approach for Resource Conservation"

- Online: IEEE Transactions on Artificial Intelligence (TAI, New issue of the Trans series), DOI: 10.1109/tai.2024.3413688
- We are the first to introduce a Markov chain model into regular training across DNN, CNN, and RNN architectures. By leveraging existing training data to predict neural network outcomes, we proposed a state transition matrix modelling approach, which uses clustering to discretise network parameters, enhancing interpretability and reducing the need for gradient propagation in repeated training.

[J3] ***X Huang***, W Li, J Pan, et al. "Alleviating Backtest Overfitting for Financial Models via TimeGAN-Enabled Time Series Data Augmentation"

- Submitted to: Finance Research Letters (FRL, JCR Q1)
- To address the issue of backtest overfitting due to insufficient financial time-series data, we introduced and fine-tuned the TimeGAN model for data augmentation, and designed an evaluation framework to systematically assess the financial characteristics, diversity, and similarity of the generated data, as well as the generalisation ability of the trained models.

[J4] K Wang, T Yan, ***X Huang***, et al. "Enhancing Interpretable Adversarial Robustness of Convolutional Neural Networks via Statistical Physics-Inspired Layer"

- Submitted to: International Journal of Computer Vision (IJCV, JCR Q1)
- Inspired by theories from statistical physics, we proposed a pluggable, lightweight embedding layer for CNNs, incorporating an innovative transformation mechanism to handle cross-scale features, reducing redundant information and enhancing robust features. Experimental results show improved robustness, outperforming same type SOTA methods, while reducing computational complexity by up to 1/3.

[J5] D Zhou, Z Song, Z Chen, ***X Huang***, et al. "Advancing Explainability of Adversarial Trained Convolutional Neural Networks for Robust Engineering Applications"

- Second Round of (Minor) Revision: Engineering Applications of Artificial Intelligence (EAAI, JCR Q1)
- For image tasks in CNNs across various industrial applications, we proposed the SSCE method. By defining 'Concept Explaining Neurons' and 'Max Activated Concept Neurons', the distribution of internal model features across 6 semantic dimensions be quantified,visualised through radar charts, areveals the model's feature preferences for different concepts, and further uncovers/supports new phenomena regarding the relationship between robustness and feature selection.

Conference Papers

[C1] D Zhou, Z Song, K Ye, ***X Huang***, et al. "Can Corner Case Unknown Objects Detection be Causal Inferenced?"

- Submitted to: AAAI Conference on Artificial Intelligence (AAAI 2025)
- To address the issue of detectors in autonomous driving scenarios being disrupted by known object features when detecting unknown objects in corner cases, we proposed a novel approach that leverages causal principles to mitigate feature interference. Our method, by incorporating innovative strategies to decouple feature interactions, reduces confusion caused by shared features offering causal interpretability, significantly outperforms both open-set and closed-set SOTA methods, particularly in metrics e.g., APu and Ru.

[C2] Z Chen, K Wang, X Lin, ***X Huang***, et al. "Unveiling Predictive Patterns in Deep Learning Classifiers"

- Submitted to: AAAI Conference on Artificial Intelligence (AAAI 2025)
- This paper explores the discoverability of hidden feature relationships and predictive mechanisms in deep learning models. We proposed an innovative algorithm that transforms the feature fusion process into a structured representation, providing a deeper understanding of the interaction logic between features. The learnability of this process was evaluated using graph-based neural networks, demonstrating enhanced model interpretability.

[C3] J Wu, Z Chen, J Qiu, *X Huang*, et al. "BitSliceTrans: An Attack–Free Method to Quickly Remove Adversarial Noise Using Bitwise Operations"

- Submitted to: AAAI Conference on Artificial Intelligence (AAAI 2025)
- Given the computational burden of current adversarial training methods and the challenge of balancing robustness and efficiency, we proposed the BitSliceTrans method. This approach utilizes an innovative bitwise transformation to filter out adversarial noise with constant time complexity, improving robust accuracy during preprocessing.

[C4] D Zhou, X Zhang, J Wu, *X Huang*, et al. "MAED: An Adaptive Defense Framework for Black–Box Query Attacks"

- Pre–submission: Conference on Computer Vision and Pattern Recognition (CVPR 2025)
- Building on advanced feature transformation and abstraction techniques, we proposed the MAED method to defend against query–based black–box attacks. Experiments show that our approach surpasses SOTA methods and offers a more comprehensive defense against both score–based and decision–based query attacks.

––––––

- I contributed to idea optimisation [J1–J4, C3–4], conducted literature reviews [J1–J5, C1–2, C4], handled experimental design, coding, and analysis [J1–J4, C4], worked on mathematical proofs and theory [J1–J3, C4], assisted with paper framework design [J1–J3, C2–C4], drafting [J1–J4, C3–C4], figures design and chart visualisation [J1–J5, C1], etc.
- 'Student First Author' refers to cases where the supervisor is listed as the first and the student as the second one, JNU policy recognises the student's contribution as equivalent to first authorship, common in mainland China.
- In line with the commitment to protect unpublished work with collaborators, key details are omitted from the public CV. We welcome interested parties to reach out for further discussion and feedback in a private setting.

PROJECTS & COMPETITIONS

National Key Research and Development Program of China

"Research and Application Demonstration of Key Technologies for Cross–Sector & Region Social Credit Governance" (Project Number: 2022YFC3303200, Total budget: 47.78M RMB ≈ 5.19M GBP)

2022 – Present (Project Member)

- Subproject 3 – Research on Model Validity, Fairness Testing, and Transparent Reasoning
- The Program is one of the highest–level projects in China. I have been focusing on the fairness of the model. I have participated in literature reviews and field research related to the practical application of the model. I am collaborating with partner institutions to complete the modeling of fairness indicators, code development, and detailed fevaluation of the models, based on AI Fairness 360, What–If Tool, etc. and drafting 10+ documentation and reports.

Kaggle Competitions

Ranked in the top 1.56% out of 205,737 participants globally (as of Oct 2024), Kaggle Profile

1. Participate in: "Home Credit – Credit Risk Model Stability" (Top 4%, Silver Medal)
2. Participate in: "Child Mind Institute – Detect Sleep States" (Top 7%, Bronze Medal)

Innovation & Entrepreneurship Projects

"University Mutual Assistance Platform Based on Fair Machine Learning (Time Bank Model)"

2022 – 2023 (Project Leader)

- Join: National College Students Innovation & Entrepreneurship Training Program (National Level Project, Received a 20,000 RMB ≈ 2,172 GBP grant)
- Participate in: Innovation and Entrepreneurship Competition of JNU for HK, Macau (Bronze Medal)
- Participate in: Challenge Cup – Extracurricular Academic & Technological Competition of JNU (Bronze Medal)

"Digital Human Age Stage Image and Voice Preservation – Creating Timeless Family Memories"

2023 – 2024 (Project Leader)

- Participate in: Internet Plus – Innovation & Entrepreneurship Competition of JNU (Industry Proposition Track, by SenseTime) (Bronze Medal)
- Participate in: China International College Students' Innovation and Entrepreneurship Competition of JNU (Silver Medal)

"Robust Control Methods for Industrial Vision Systems Based on Trusted Deep Learning"

2022 – 2023 (Project Member)

- Participate in: Internet Plus – Innovation and Entrepreneurship Competition of JNU (Bronze Medal)

"AI Box: Open Platform for AI System Security Evaluation"

2023 – 2024 (Project Leader)

- Join: Challenge Cup – Extracurricular Academic and Technological Innovation Plan of JNU (University Level, Received a 2,000 RMB ≈ 217 GBP grant)
- Participate in: Challenge Cup – National College Entrepreneurship Competition of JNU (Silver Medal)

"LawQuery – Law LLM Based on Generative Artificial Intelligence"

2023 – 2024 (Project Member)

- Participate in: Fisherman Cup – Innovation & Entrepreneurship Competition of JNU (Silver Medal)

Programming & Mathematical Modeling Competitions

1. Participate in: "China Computer Federation: CAT National Algotithm Elite Competition" (Top 7%, Second Prize)
2. Participate in: "ShuWei Cup – International Mathematical Contest in Modeling" (Top 14%, Honorable Mentions)

SKILLS

- Languages: Python (Proficient), C/C++, Java, HTML/CSS/JS, SQL; Latex, Matlab
- Technologies/Frameworks: Machine Learning and Deep Learning (PyTorch), Data Statistics, Basic Development

STUDENT WORK

- College Debate Team (Captain, Awarded Outstanding One)
- Python Tutoring Group for College Freshmen (Leader)
- Teaching Assistant (Fall 2024, Course: Data Structure)