Lin Li (李淋)

PhD student in Machine Learning, Department of Informatics, King's College London, London, UK
Phone: +86 189 0022 0595 | Email: lin.3.li@kcl.ac.uk | Page: treelli.github.io | Git: github.com/TreeLLi

RESEARCH INTEREST

- Trustworthy ML: robustness, safety and interpretability
- Data-centric ML: better augmenting and utilizing training data for improved performance and efficiency

EDUCATION

M.Phil/PhD, Department of Informatics, King's College London, London, UK Oct. 2019 – Mar. 2024

- Supervisors: Dr. Michael Spratling (primary) and Dr. Dimitrios Letsios
- Thesis: *Towards Robust Visual Classification through Adversarial Training*

MSc, Department of Computing, Imperial College London, London, UK Oct. 2017 – Sep. 2018

- Advisor: Prof. Wayne Luk
- Grade: Overall Distinction (Exam + Thesis)
- Thesis: *Understanding Deep CNNs via Interpretable Individual Units*

BBM, Department of Finance, Xiamen University, Xiamen, China Sep. 2013 – June 2017

- Advisor: Prof. Zheng Qiao
- Grade: GPA: 3.67/4.00**;** top 10% in the department
- Thesis: *Quantitatively Measuring Investor's Sentiment via Search Index*

PROFESSIONAL EXPERIENCE

Research Intern, Robotics X Lab, Tencent, Shenzhen, China Dec. 2021 – Oct. 2022

- advised by: Dr. Lipeng Chen
- project: Advancing Robots with Greater Dynamic Dexterity: A Large-scale Multi-modality and Multi-perception Dataset for Humanoid Throw-Catch Learning

Teaching Assistant, Department of Informatics, King's College London, London, UK Jan. 2021 – Dec. 2021

- courses: Machine Learning and Pattern Recognition, Introduction to Artificial Intelligence
- additional work: automated code assessment tool for students' courseworks.

Co-funder, Firefly Technology, Xiamen, China Aug. 2016 – Jun. 2017

- product: a location-based social network mobile application
- fund: Jinyuan Startup Fund, Xiamen University (Management School) and Yanwu Hacker Space

PUBLICATIONS

1. **Lin Li**, Michael Spratling, Data augmentation alone can improve adversarial training, International Conference on Learning Representations (ICLR), 2023.
2. **Lin Li**, Michael Spratling, Understanding and combating robust overfitting via input loss landscape analysis and regularization, Pattern Recognition (PR), 2023
3. Jianing Qiu, **Lin Li**, Jiankai Sun, and Jiachuan Peng, Peilun Shi, Ruiyang Zhang, Yinzhao Dong, Kyle Lam, Frank P.-W. Lo, Bo Xiao, Wu Yuan, Dong Xu, Benny Lo, Large AI Models in Health Informatics: Applications, Challenges, and the Future, IEEE Journal of Biomedical and Health Informatics (JBHI), 2023
4. **Lin Li**, Michael Spratling, Improved Adversarial Training Through Adaptive Instance-wise Loss Smoothing, in submission, 2023
5. **Lin Li**, Jianing Qiu, Michael Spratling, AROID: Improving Adversarial Robustness through Online Instance-wise Data Augmentation, in submission, 2023
6. **Lin Li**, Yifei Wang, Chawin Sitawarin, Michael Spratling, OODRobustBench: benchmarking and analyzing adversarial robustness under distribution shift, in submission, 2023
7. **Lin Li**, Haoyan Guan, Jianing Qiu, Michael Spratling, Learning to Prompt Vision-Language Models for Adversarial Robustness, in submission, 2023
8. Jianing Qiu, Jian Wu, Hao Wei, and Peilun Shi, Minqing Zhang, Yunyun Sun, **Lin Li**, Hanruo Liu, Hongyi Liu,

Simeng Hou, Yuyang Zhao, Xuehui Shi, Junfang Xian, Xiaoxia Qu, Sirui Zhu, Lijie Pan, Xiaoniao Chen, Xiaojia Zhang, Shuai Jiang, Kebing Wang, Chenlong Yang, Mingqiang Chen, Sujie Fan, Jianhua Hu, Aiguo Lv, Hui Miao, Li Guo, Shujun Zhang, Cheng Pei, Xiaojuan Fan, Jianqin Lei, Ting Wei, Junguo Duan, Chun Liu, Xiaobo Xia, Siqi Xiong, Junhong Li, Benny Lo, Yih Chung Tham, Tien Yin Wong, Ningli Wang, Wu Yuan, VisionFM: a Multi-Modal Multi-Task Vision Foundation Model for Generalist Ophthalmic Artificial Intelligence, in submission, 2023

PROJECTS

Detecting objects for hotel rooms, Microsoft, London, UK 2018

- co-supervised by Dr. Anandha Gopalan, Mr. Lee Stott
- implemented Faster-RCNN using CNTK to detect items in the pictures for automatical labeling of the facilities
- the entire system was deployed as a web application
- Blog (Microsoft), Git, Report, Presentation, Opensource Contributions, Demo

HONORS & AWARDS & GRANT

PGR Research Support, King's College London 2023

King's-China Scholarship, King's College London and China Scholarship Council (CSC) 2019

1st Class (Xiangyu) University Scholarship, Xiamen University 2016

Excellent Academic Performance Scholarship, Xiamen University 2015

3rd prize winner, Jinyuan Creativity and Startup Contest, Xiamen City 2016

3rd prize winner, ChinaNet Dream Accelerator Programming Contest, China 2015

TALKS & PRESENTATIONS

Data augmentation can improve adversarial training, AI Time Youth PhD Talk 2023

Data augmentation for adversarial robustness, ADA talk, King's College London 2023

Defending DNNs against adversarial examples, Departmental Research Showcase, King's College London 2023

ACADEMIC SERVICE

- **reviewer**: NeurIPS

SKILLS

- **Languages**: Mandarin, English, Southern Min
- **Programming languages**: Python, C++, C, Java, Objective-C
- **Machine learning**: deep neural network, convolutional neural network, vision transformer, visual classification, adversarial attack and defense, automated machine learning, diffusion models
- **Machine learning frameworks**: PyTorch, TensorFlow

REFEREES

Dr. Michael Spratling
Reader, Department of Informatics, King's College London, London, UK
Phone: +44 020 7848 2027, Email: michael.spratling@kcl.ac.uk

Dr. Benny Lo
Reader, the Hamlyn Centre & the Department of Surgery and Cancer, Imperial College London, London, UK
Phone: +44 (0)20 7594 0806, Email: benny.lo@imperial.ac.uk

Dr. Lipeng Chen
Senior Research Scientist, Robotics X Lab, Tencen, Shenzhen, China
Phone: +86 18267157219, Email: lipengchen@tencent.com