




Guanyu Hou (侯冠宇)

 (+44) 07990071823 |  guanyu.hou@student.manchester.ac.uk |  [Hoempage](#)

Education

Chengdu University of Technology	2021.9 - 2025.7
SoftwareEngineering	Undergraduate
GPA 3.3, 1st Honor Degree	
CDUT Sino-British Collaborative Education (with Oxford Brooks University)	
The University of Manchester	2025.9 - present
Master of Science in Artificial Intelligence	PGT

Publications

Evaluating Robustness of Large Audio Language Models to Audio Injection: An Empirical Study	2025.5 - Accept
The 2025 Conference on Empirical Methods in Natural Language Processing (EMNLP 2025) (CCF-B)	
Guanyu Hou, Jiaming He, Yinhang Zhou, Ji Guo, Yitong Qiao, Rui Zhang, Wenbo Jiang	
When Hallucinated Concepts Cross Modals: Unveiling Backdoor Vulnerability in Multi-modal In-context Learning	2025.2- Accept
ACM Multimedia Asia 2025 (ACM MM Asia) (CCF-C)	
Guanyu Hou, Jiaming He, Yitong Qiao, Jiachen Li,Zihan Wang, Qiyang Song, Hongwei Li,,Wenbo Jiang	
PRESS: Defending Privacy in Retrieval-Augmented Generation via Embedding Space Shifting	2024.9 - online
2025 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2025) (CCF-B)	
 https://ieeexplore.ieee.org/document/10887843	
Jiaming He*, Cheng Liu*, Guanyu Hou* , Wenbo Jiang, Jiachen Li (* equal contribution)	
Watch Out for Your Guidance on Generation! Exploring Conditional Backdoor Attacks against Large Language Models	2024.11 - online
The 39th Annual AAAI Conference on Artificial Intelligence (CCF-A) (Oral, top 5%)	
 https://ojs.aaai.org/index.php/AAAI/article/view/34819	
Jiaming He, Wenbo Jiang, Guanyu Hou , Wenshu Fan, Rui Zhang, Hongwei Li	
Data Stealing Attacks against Large Language Models via Backdooring	2024.7- Online
Electronics (JCR-Q2)	
 https://www.mdpi.com/2079-9292/13/14/2858	
Jiaming He, Guanyu Hou* , Xinyue Jia, Yangyang Chen, Wenqi Liao, Yinhang Zhou, Rang Zhou (* Corresponding Author)	
Weaponizing Tokens: Backdooring Text-to-Image Generation via Token Remapping	2025.3- Accepted
IEEE International Conference on Multimedia&Expo 2025 (ICME 2025) (CCF-B)	
Jiaming He, Wenbo Jiang, Guanyu Hou , Qiyang Song, Guo Ji and Hongwei Li	
Embedding Based Sensitive Element Injection against Text-to-Image Generative Models	2024.4 - online
2024 9th International Conference on Intelligent Computing and Signal Processing (ICSP 2024)	
 https://ieeexplore.ieee.org/document/10743442	
Benrui Jiang, Kan Chen, Guanyu Hou , Xiying Chen, Jiaming He (Equal contribution)	

Academic Experience			
AAAI 2026 Reviewer			2025.8
Language			
English			
IELTS 7.0			
Tools			
Programme Languages	Machine Learning	Database	Development Tools
Python, Java, C/C++	Pytorch, Sklearn	MySQL	Git, JIRA