Jin Ma

Ph.D. Student · Computer Science

Clemson University, Clemson, SC, 29634

✉ majinwakeup@gmail.com | 🏠 https://majinwakeup.github.io/

Profile

Jin Ma is a self-driven Ph.D. student with an outstanding 4.0 GPA, a strong research record, and industry experience. His interests center on AI trustworthiness and AI for online content safety, with a focus on the intersection of computer vision and security. His recent work spans *adversarial defense for vision perception systems*, *using Large Vision Language Models (LVLMs) for cyberbullying and misinformation detection*, and *backdoor attacks on LVLMs*.

Availability: Full-time summer internship, May 1 - August 30, 2026 (17 weeks).

Education

Clemson University *Clemson, SC, US*
Ph.D. Computer Science *Aug. 2023 - Present*

- Advisor: Dr. Long Cheng.

Cleveland State University *Cleveland, OH, US*
Ph.D. Computer Science *Aug. 2021 - Jul. 2023*

- Advisor: Dr. Hongkai Yu.

Xi'an Jiaotong University *Xi'an, Shaanxi, China*
M.E. Software Engineering *Sep. 2016 - Jun. 2019*

- Advisor: Dr. Shanmin Pang.

Xi'an Jiaotong University *Xi'an, Shaanxi, China*
B.S. Information and Computational Science *Sep. 2012 - Jun. 2016*

Selected Publications

Ma, J., Enan, A., Cheng, L., & Chowdhury, M. (2025). Understanding the Risks of Asphalt Art on the Reliability of Surveillance Perception Systems. In Transportation Research Board Annual Meeting (TRB 25).

Ma, J., Aldeen, M., Salas, C., Luo, F., Chowdhury, M., Pesé, M., & Cheng, L. (2025). DisPatch: Disarming Adversarial Patches in Object Detection with Diffusion Models. arXiv preprint arXiv:2509.04597. [*in submission*]

Ma, J., Yan, J., Aldeen, M., Anderson, E., Kavuru, T. Park, J., Luo, F., & Cheng, L. (2025). Towards Automated Context-Corrective Notes Generation for Responsible Online Social Networks. [*in submission*]

Ma, J., Aldeen, M. S., Luo, F., & Cheng, L. (2025). Few-Shot Detection of Hate Videos Using Multi-Modal Large Language Models. In Proceedings of the 1st ACM Workshop on Deepfake, Deception, and Disinformation Security.

Han, X.*, **Ma, J.***, Zhang, J., Liu, K., & Luo, F. (2025), Understanding the Constraints of RAG-Based Medical LVLMs - A Case Study in Ophthalmic Report Generation. In Proceedings of the 1st Workshop on AI-Ready Data for Science Discovery.

Yan, J., Liao, S., **Ma, J.**, Aldeen, M., Kumar, S., & Cheng, L. (2025). No Way to Sign Out? Unpacking Non-Compliance with Google Play's App Account Deletion Requirements. In 34th USENIX Security Symposium (USENIX Security 25).

Aftabi, N., Samaha, P., **Ma, J.**, Cheng, L., Harik, R., & Li, D. (2025). ViSTR-GP: Online Cyberattack Detection via Vision-to-State Tensor Regression and Gaussian Processes in Automated Robotic Operations. arXiv preprint arXiv:2509.10948.

Aldeen, M., MohajerAnsari, P., **Ma, J.**, Chowdhury, M., Cheng, L., & Pesé, M. D. (2024). An initial exploration of employing large multimodal models in defending against autonomous vehicles attacks. In 2024 IEEE Intelligent Vehicles Symposium.

Ma, J., Li, J., Guo, Q., Zhang, T., Lin, Y., & Yu, H. (2023). RXFOOD: Plug-in RGB-X Fusion for Object of Interest Detection. arXiv preprint arXiv:2306.12621.

Li, J., Xu, R., **Ma, J.**, Zou, Q., Ma, J., & Yu, H. (2023). Domain adaptive object detection for autonomous driving under foggy weather. In Proceedings of the IEEE/CVF winter conference on applications of computer vision.

Sun, H., **Ma, J.**, Guo, Q., Zou, Q., Song, S., Lin, Y., & Yu, H. (2023). Coarse-to-fine task-driven inpainting for geoscience images. IEEE Transactions on Circuits and Systems for Video Technology, 33(12).

Ma, J., Pang, S., Yang, B., Zhu, J., & Li, Y. (2020). Spatial-content image search in complex scenes. In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision.

Professional Experience

2020-2021	**Algorithm engineer**, Chengdu Hsintiao Medical and Technology Company. Chengdu. Contact: 4001268228, hatas@hsintiao.com
2019-2020	**Research & Development engineer**, Southeast Research Institute of China Unicom. Fuzhou. Contact: Xiaodan Su, xdsu@iue.ac.cn

Research Experience

Clemson University - Trustworthiness of AI *Clemson, US*

Advisor: Dr. Long Cheng *Aug. 2023 - Present*

- Research on AI model vulnerabilities and defenses, ranging from defending object detectors against adversarial patch attacks to analyzing backdoor attacks on large language models (LLMs) and large vision–language models (LVLMs).

Clemson University - AI for Online Content Safety *Clemson, US*

Advisor: Dr. Long Cheng *Aug. 2023 - Present*

- Research on online content safety leveraging LLMs and LVLMs for cyberbullying and misinformation *detection*, coupled with credible, evidence-backed explanations to foster a responsible web ecosystem (*intervention*).

Singapore University of Technology and Design - Biometric Authentication *Singapore*

Advisors: Dr. Jianying Zhou *May. 2024 - Aug. 2024*

- Developed multimodal biometric authentication systems that integrate complementary physiological and behavioral signals, augmented with secure protocols to mitigate spoofing and adversarial manipulation.

Brookhaven National Laboratory - Collision Avoidance System *Cleveland, US*

Advisors: Dr. Yonghua Du, Dr. Lu Ma, Dr. Yuewei Lin, Dr. Hongkai Yu *Mar. 2022 - Jul. 2023*

- Equipment collision is a serious problem in workspace. This project aimed to build a real-time collision avoidance system with the help of computer vision methods, such as video object segmentation and tracking techniques.

Xi'an Jiaotong University - Image Retrieval *Xi'an, China*

Advisor: Dr. Shanmin Pang *Sept. 2016 - Jun. 2019*

- Conducted research on image retrieval by enhancing traditional content-based image retrieval, and introducing a spatial–content image retrieval approach that prioritizes semantic cues and spatial relationships.

Presentations

Fall 2025. Poster: *Potential Risks of Asphalt Arts On The Reliability of Perception System*. SecDev 2025, Indianapolis, USA.

Fall 2023. Poster: *ICOAR: Integrative Cyberinfrastructure for Online Abuse Research*. SecDev 2023, Atlanta, USA.

Teaching Experience

Teaching Assistant

Spring 2025	**CPSC 8430 Deep Learning (Coursera)**, Teaching Assistant	*Clemson University*
Fall 2024	**CPSC 8430 Deep Learning**, Teaching Assistant	*Clemson University*
Spring 2024	**CPSC 4300/6300 Applied Data Science**, Teaching Assistant	*Clemson University*
Fall 2023	**CPSC 4030/6030 Data Visualization**, Teaching Assistant	*Clemson University*

Mentoring

2025	**Ethan Anderson, and Taran Kavuru**, Undergraduate Students	*Clemson University*

Peer Review

2025	**Transportation Research Board Annual Meeting (TRB)**,	*Reviewer*
2025	**The ACM Web Conference**,	*Reviewer*
2025	**IEEE International Conference on Distributed Computing Systems (ICDCS)**,	*Subreviewer*
2025	**IEEE International Conference on Computer Software and Applications (COMPSAC)**,	*Subreviewer*
2025	**ACM Advances in Social Networks Analysis and Mining (ASONAM)**,	*Subreviewer*
2022-2024	**ACM International Conference on Multimedia**,	*Reviewer*

Honours and Awards

2024	**Certification of Appreciation (Volunteer)**, ACM AsiaCCS.
2024	**Badge of Recognition**, The ACM Web Conference.
2019	**Excellent graduation thesis**, Xi’an Jiaotong University.
2019	**Excellent graduate**, Xi’an Jiaotong University.
2018	**Successful participation**, National Graduate Mathematical Contest in Modeling (CN).
2018	**Zhonghui scholarship**, Xi’an Jiaotong University.

Skills

Knowledge Base

- Mathematics: linear algebra, mathematical analysis, probability and statistics, etc.
- Computer science: machine learning, deep learning, computer vision, algorithms, operating system, etc.

Programming

- Programming language: python, Matlab, c/c++.
- Deep learning framework: PyTorch, Tensorflow, Keras.
- Operating system: Linux, Windows.