

Jin Ma

PH.D. CANDIDATE · COMPUTER SCIENCE

Clemson University, Clemson, SC 29634

☎ (216) 354-5756 | ✉ jin7@clemson.edu | 🏠 majinwakeup.github.io | 🎓 Google Scholar

Profile

Jin Ma is a Ph.D. candidate in Computer Science at Clemson University specializing in trustworthy AI and cybersecurity at the intersection of computer vision and machine-learning security. His research examines vulnerabilities in vision-based perception systems, generative-model-based adversarial defenses, and applications of large vision-language models (LVLMs) to online content safety and misinformation mitigation. His research is informed by prior industry R&D experience and interdisciplinary collaborations across security, multimedia, and intelligent systems.

Research interests: Trustworthy AI, Robust Vision-Based Perception Systems, Multimodal Web Safety.

Education

Clemson University

PH.D. COMPUTER SCIENCE

• Advisor: Dr. Long Cheng; GPA: 4.0 / 4.0.

Clemson, SC, USA

Aug. 2023 – Aug. 2027 (expected)

Cleveland State University

PH.D. STUDIES IN COMPUTER SCIENCE

• Advisor: Dr. Hongkai Yu; GPA: 4.0 / 4.0.

Cleveland, OH, USA

Aug. 2021 – Jul. 2023

Xi'an Jiaotong University

M.E. SOFTWARE ENGINEERING

• Advisor: Dr. Shanmin Pang.

Xi'an, Shaanxi, China

Sep. 2016 – Jun. 2019

Xi'an Jiaotong University

B.S. INFORMATION AND COMPUTATIONAL SCIENCE

Xi'an, Shaanxi, China

Sep. 2012 – Jun. 2016

Selected Publications

Citation Summary (September 2026): 750+ citations · *h*-index: 11 · *i*10-index: 11 (* Equal contribution; † Undergraduate mentee)

PEER-REVIEWED AND ACCEPTED PUBLICATIONS

Ma, J.*, Enan, A.*, Cheng, L., & Chowdhury, M. (2026). Understanding the risks of asphalt art to the reliability of vision-based perception systems. *Transportation Research Record*. [In press].

Yan, J., Liao, S., **Ma, J.**, Aldeen, M. S., Kumar, S., & Cheng, L. (2025). No way to sign out? Unpacking non-compliance with Google Play's app account deletion requirements. In *Proceedings of the 34th USENIX Security Symposium (USENIX Security 25)*, 3277–3296.

Wang, F., Sun, F., Fan, M., Zhou, J., **Ma, J.**, Chen, C., Shu, J., & Zhang, L. Y. (2025). FLAME: Flexible and lightweight biometric authentication scheme in malicious environments. In *Proceedings of the 41st Annual Computer Security Applications Conference (ACSAC 2025)*, 411–424.

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 (3D-Sec '25)*, 32–35.

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 2025 IEEE International Conference on Data Mining Workshops (ICDMW 2025)*, 96–102.

Aldeen, M. S., 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 *Proceedings of the 2024 IEEE Intelligent Vehicles Symposium (IV 2024)*, 3334–3341.

- Li, J., Xu, R., Liu, X., **Ma, J.**, Chi, Z., Ma, J., & Yu, H. (2023). Learning for vehicle-to-vehicle cooperative perception under lossy communication. *IEEE Transactions on Intelligent Vehicles*, 8(4), 2650–2660.
- 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 (WACV 2023)*, 612–622.
- Liu, X., Li, J., **Ma, J.**, Sun, H., Xu, Z., Zhang, T., & Yu, H. (2023). Deep transfer learning for intelligent vehicle perception: A survey. *Green Energy and Intelligent Transportation*, 2(5), 100125.
- 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), 7170–7182.
- 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 (WACV 2020)*, 2492–2500.

PREPRINTS AND MANUSCRIPTS UNDER REVIEW

- Ma, J.**, Yan, J., Aldeen, M. S., Anderson, E.[†], Kavuru, T.[†], Park, J. K., Luo, F., & Cheng, L. (2026). Towards automated community notes generation with large vision-language models for combating contextual deception. *arXiv preprint arXiv:2603.22453*.
- Ma, J.**, Aldeen, M. S., Salas, C., Luo, F., Chowdhury, M., Pesé, M. D., & Cheng, L. (2025). DisPatch: Disarming adversarial patches in object detection with diffusion models. *arXiv preprint arXiv:2509.04597*.

Conference Presentations

- Jan. 2026. Poster: *Understanding the Risks of Asphalt Art on the Reliability of Surveillance Perception Systems*. Transportation Research Board (TRB) Annual Meeting, Washington, D.C., USA.
- Oct. 2025. Poster: *Potential Risks of Asphalt Arts on the Reliability of Perception Systems*. IEEE Secure Development Conference (SecDev 2025), Indianapolis, IN, USA.
- Oct. 2023. Poster: *ICOAR: Integrative Cyberinfrastructure for Online Abuse Research*. IEEE Secure Development Conference (SecDev 2023), Atlanta, GA, USA.

Research Experience

Clemson University — Trustworthiness of AI

Clemson, SC, USA

ADVISOR: DR. LONG CHENG

Aug. 2023 – Present

- Investigated adversarial vulnerabilities in vision perception systems; developed diffusion-based defense architectures (*DisPatch*) against physical adversarial patches and quantified edge perception reliability under real-world visual perturbations.

Clemson University — AI for Online Content Safety

Clemson, SC, USA

ADVISOR: DR. LONG CHENG

Aug. 2023 – Present

- Formulated multimodal systems leveraging foundation models (LLMs/LVLMs) for few-shot hate video detection and automated community notes generation to counter contextual misinformation and facilitate online safety interventions.

Singapore University of Technology and Design — Biometric Authentication

Singapore

ADVISOR: DR. JIANYING ZHOU

May 2024 – Aug. 2024

- Developed multimodal biometric authentication architectures combining complementary physiological and behavioral signals and integrated cryptographic protocols to prevent spoofing and adversarial tampering.

Cleveland State University — Autonomous Vehicles & Object Detection

Cleveland, OH, USA

ADVISOR: DR. HONGKAI YU

Aug. 2021 – Jul. 2023

- Researched robust perception for autonomous vehicles under adverse weather and lossy V2V communication, and developed multimodal RGB-X fusion models for object-of-interest detection.

Brookhaven National Laboratory — Collision Avoidance Systems

Upton, NY / Cleveland, OH, USA

ADVISORS: DR. YONGHUA DU, DR. LU MA, DR. YUEWEI LIN, DR. HONGKAI YU

Mar. 2022 – Jul. 2023

- Engineered real-time computer vision pipelines for workspace collision avoidance in scientific beamline facilities, implementing spatio-temporal video object segmentation and multi-object tracking architectures.

Xi'an Jiaotong University — Image Retrieval

ADVISOR: DR. SHANMIN PANG

Xi'an, Shaanxi, China

Sep. 2016 – Jun. 2019

- Conducted research on semantic and spatial-content image retrieval, developing deep feature aggregation, similarity propagation, and heat diffusion graph re-ranking methods for complex scene queries.

Teaching & Mentoring Experience

TEACHING EXPERIENCE

Clemson University

Clemson, SC, USA

TEACHING ASSISTANT

Aug. 2023 – Present

Assisted course instruction across undergraduate and graduate levels; responsibilities included holding weekly office hours, grading coursework and exams, developing hands-on laboratory exercises, and delivering occasional guest lectures:

- **Cybersecurity & Systems:** CPSC 4200/6200 Computer Security Principles (Fall 2026); CPSC 4240/6240 System Administration and Security (Fall 2026).
- **Artificial Intelligence & Data Science:** CPSC 8430 Deep Learning (Fall 2024, Spring and Fall 2025 [Coursera]); CPSC 4300/6300 Applied Data Science (Spring 2024); CPSC 4030/6030 Computer Data Visualization (Fall 2023).
- **Foundations & Core Theory:** CPSC 3120 Introduction to Design and Analysis of Algorithms (Spring 2026).

UNDERGRADUATE RESEARCH MENTORSHIP

Clemson University

Clemson, SC, USA

RESEARCH MENTOR

Jan. 2025 – Present

- **Addison Key** (Summer and Fall 2026): Mentored an incoming honors undergraduate researcher through Clemson's competitive EUREKA! research program, guiding foundational training in vision-language-action model security.
- **Ethan Anderson & Taran Kavuru** (Spring and Fall 2025): Mentored two undergraduate students on evaluating multimodal vision-language models for online misinformation detection, culminating in a co-authored research paper.

Peer Review

2027	International AAAI Conference — AI for Social Impact Track (AISIT),	Reviewer
2026	International AAAI Conference on Web and Social Media (ICWSM),	PC Member
2026	ACM International Conference on Multimedia (ACM MM),	PC Member
2025	Transportation Research Board Annual Meeting (TRB),	Reviewer
2025	IEEE Transactions on Dependable and Secure Computing (TDSC),	Reviewer
2025	The ACM Web Conference (WWW),	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 (ACM MM),	Reviewer

Industry Experience

Chengdu Hsintiao Medical Technology Co., Ltd.

Chengdu, China

ALGORITHM ENGINEER

Oct. 2020 – Aug. 2021

- Developed deep learning algorithms for medical image segmentation and automated clinical feature extraction.
- Optimized model training and inference pipelines for deployment on healthcare computing platforms.

Southeast Research Institute of China Unicom

Fuzhou, China

RESEARCH & DEVELOPMENT ENGINEER

Aug. 2019 – Sep. 2020

- Collected and annotated surveillance datasets under varied river conditions, training lightweight detection models.
- Built and deployed a computer vision system for real-time floating trash detection on rivers for environmental monitoring.