Yanming Xiu

+1 (858)330-8519 | yanming.xiu@duke.edu | Durham, NC, USA

EDUCATION

Duke University Aug. 2022 – Present

Ph.D. Student, Electrical and Computer Engineering Durham, NC, USA

- **Research Interests**: Augmented Reality, Scene Understanding, Machine Learning, Computer Vision
- **GPA**: 3.86/4.0

Zhejiang University Sep. 2018 – Jun. 2022

Bachelor of Engineering in Automation (Chu Kochen Honor Class) Hangzhou, China

- **GPA**: 3.85/4.0

RESEARCH

Generative AI-Driven Task Detrimental Content Detection in Augmented Reality Jan 2024 – Present

Intelligent Interactive Internet of Things Lab Duke University

- Developed **ViDDAR**, an **obstruction attack** detection system for AR applications that prevents important real-world objects or information from being blocked. The system integrates a vision-language model, a multimodal object detection model and a segmentation model, achieving 92.15% detection accuracy with a latency of 533 ms. The paper was accepted by **IEEE VR** 2025 and selected as a special issue of **IEEE TVCG**.
- Systematically defined **visual information manipulation attacks** in AR through a proposed attack taxonomy and created AR-VIM, a dataset of 452 raw-AR video pairs. Also developed VIM-Sense, a system that combines vision-language models and optical character recognition module to detect such attacks, achieving 88.94% detection accuracy. This work is conditionally accepted by **ISMAR** 2025 and selected as a special issue of **IEEE TVCG**.
- Deployed and tested both ViDDAR and VIM-Sense on android smartphones and Meta Quest 3. A demonstration was accepted by **IEEE VR Research Demonstration** 2025.

Automated Assessment Methods for Virtual Content in Augmented Reality Nov. 2024 – Present

Intelligent Interactive Internet of Things Lab Duke University

- Contributed to the collection and annotation of **DiverseAR**, a dataset of 298 images covering a wide range of AR scenarios.
- Evaluated the ability of three state-of-the-art commercial vision-language models to perceive and describe virtual content in AR images using the DiverseAR dataset. The paper was accepted by **IEEE VR Workshop (VRW)** 2025.

Publications

Journal Publication

- **[TVCG'25] Y. Xiu**, T. Scargill, and M. Gorlatova. ViDDAR: Vision language model-based task-detrimental content detection for augmented reality. IEEE Transactions on Visualization and Computer Graphics (TVCG), 2025. (**Acceptance rate: 17.32%**)
- **[ToAppearTVCG'26] Y. Xiu** and M. Gorlatova. Detecting visual information manipulation attacks in augmented reality: a multimodal semantic reasoning approach. To appear at IEEE Transactions on Visualization and Computer Graphics (TVCG), 2025. (**Acceptance rate: 7.87%**)

Conference Proceeding

- **[SubmittedAAAI'25]**, R. chen, A. Andreyev, **Y. Xiu**, M. Imani, B. Li, M. Gorlatova, G. Tan, and T. Lan , Cognitive attacks detection in augmented reality (CADAR): a neuro-symbolic approach with particle filtering on perception graphs. Submitted to Annual AAAI Conference on Artificial Intelligence (AAAI), August 2025.
- **[SubmittedAACL'25]** S. Mim, J. Morris, M. Dhakal, **Y. Xiu**, M. Gorlatova, Y. Ding, Can a unimodal language agent provide preferences to tune a multimodal vision-language model? Submitted to International Joint Conference on Natural Language Processing and Asia-Pacific Chapter of the Association for Computational Linguistics (AACL), July 2025.

Workshop Proceeding

- **[VR'25w]** L. Duan*, **Y. Xiu*** and M. Gorlatova. Advancing the understanding and evaluation of AR-generated scenes: When vision-language models shine and stumble. In Proceedings of IEEE VR Abstracts and Workshops (VRW), 2025.
- **[SubmittedISMAR'25w] Y. Xiu**, S. Sen, J. Chilukuri and M. Gorlatova. A systematic evaluation on audio-based 3D content generation methods in augmented reality. Submitted to IEEE ISMAR UNAI workshop, 2025.

Doctoral Consortium

- **[ISMAR'25dc] Y. Xiu**. Toward safe, trustworthy and realistic augmented reality user experience. To appear at Proceedings of IEEE ISMAR-Adjunct, 2025.

Research Demonstration

- **[VR'25d] Y. Xiu** and M. Gorlatova. Vision Language Model-Based Solution for Obstruction Attack in AR: A Meta Quest 3 Implementation. In Proceedings of IEEE VR Research Demonstrations, 2025.

Poster Presentation

- **[ISMAR'24p] Y. Xiu**, T. Scargill, and M. Gorlatova. LOBSTAR: Language model-based obstruction detection for augmented reality. In Proceedings of IEEE ISMAR-Adjunct, 2024.

* Indicates equal contribution

TEACHING

Teaching Assistant for ECE 356: Computer Networks Aug 2024 – Dec 2024

Department of Electrical and Computer Engineering Duke University

- Responsibilities included setting up the course website, managing the server for homework and lab projects, supporting student learning through office hours, assisting with course assessment by copy-editing and grading quizzes and exams.

High School Research Mentor Jun. 2024 – Present

Intelligent Interactive Internet of Things Lab Duke University

- Mentored 4 students from North Carolina School of Science and Mathematics on two different projects.
- Student list: Junfeng Lin (NCSSM 2025, admitted by Stanford University); Tristan LoGuidice (NCSSM 2025, admitted by University of North Carolina, Chapel Hill); Shunav Sen (NCSSM 2026); Joshua Chilukuri (NCSSM 2026)

HONORS

Graduate Student Conference Travel Fellowship Mar. 2025

Department of Electrical and Computer Engineering Duke University

First-Tier Outstanding Scholarship May. 2021

Chu Kochen Honors College Zhejiang University