

Jingmiao Zhang

📍 Hefei, China ✉ jingmiao@mail.ustc.edu.cn 🔗 <https://glycineeeee.github.io>

Education

University of Science and Technology of China (USTC)
M.E. in Computer Science and Technology

Hefei, China
Sep 2023 – Present (Expected Jun 2026)

University of Science and Technology of China (USTC)
B.E. in Information Security

Hefei, China
Sep 2019 – Jul 2023

Research Interests

- **Security and Privacy:** Secure and Trustworthy AI; Adversarial Machine Learning; Mobile and Network Security; System Security; Privacy-Preserving Computation.
- **Mobile and Intelligent Systems:** Edge Intelligence; Ubiquitous Computing; Embodied AI; Agentic AI.

Publications

1. SpeechGuard: Recoverable and Customizable Speech Privacy Protection. **Jingmiao Zhang**, Suyuan Liu, Jiahui Hou, Zhiqiang Wang, Haikuo Yu, Xiang-Yang Li. **USENIX Security**, 2025. [Paper] [Slides] [Video]
2. Task-Oriented Training Data Privacy Protection for Cloud-based Model Training. Zhiqiang Wang, Jiahui Hou, Haifeng Sun, **Jingmiao Zhang**, Yunhao Yao, Haikuo Yu, Xiang-Yang Li. **USENIX Security**, 2025. [Paper]
3. AMoS: Autonomous Multimodal POI Standardization without Extra Annotation. Suyuan Liu, **Jingmiao Zhang**, Haikuo Yu, Yan Zhang, Yuetian Wang, Guobin Shen, Xiang-Yang Li. **IEEE INFOCOM**, 2025. [Paper]
4. InvisiCode: Boosting Intra-Frame Screen-Camera Communication by Breaking Through Noise Limitations. Haikuo Yu[†], **Jingmiao Zhang**[†], Haohua Du, Kaiwen Guo, Xiang-Yang Li. [†]Co-first authors. **IEEE/ACM IWQoS**, 2025. [Paper] [Code]

Research Experiences

School of Computing Summer Workshop

Online

Supervised by [Prof. Hugh Anderson](#), National University of Singapore

May 2022 – Jul 2022

- Explored audio watermarking algorithms and proposed a hybrid scheme combining DWT and LSB methods to improve robustness and imperceptibility, as part of a four-member research project.

Personalized Privacy Protection for Unstructured Data

USTC

Supervised by IEEE/ACM Fellow [Prof. Xiang-Yang Li](#) and [Prof. Jiahui Hou](#)

Feb 2023 – Mar 2024

- Focus: Addressed privacy risks in user-generated data by developing protection mechanisms for speech, visual content, and datasets that adapt to different permission groups or machine learning tasks.
- Designed SPEECHGUARD, a recoverable and customizable speech privacy protection system that integrates multi-parameter reversible warping and adaptive text encryption with hierarchical access control, achieving strong privacy without losing usability. SPEECHGUARD demonstrates superior anonymity, sensitive content confidentiality, and attack resistance over three baseline systems.
- Contribution: First author of SPEECHGUARD, accepted at **USENIX Security 2025**, leading ideas, experiments, and writing; also contributed to another paper on task-oriented data privacy protection.

Autonomous Multimodal POI Standardization

USTC

Supervised by [Prof. Xiang-Yang Li](#) and [Dr. Guobin Shen](#), HKUST(GZ)

Nov 2023 – Jul 2024

- Focus: Developed a multimodal POI standardization framework that generates standardized location representations from informal user text, uncertain indoor positioning, and Wi-Fi signals.
- Designed a nearest-neighbor matching algorithm integrating trajectory-aware GeoEncoder, ChineseBERT-based text embeddings, and Wi-Fi features, followed by FINCH clustering and contrastive learning for iterative refinement, achieving over 10% higher recall and improved POI matching robustness compared with baseline systems.
- Contribution: Participated in idea discussions and baseline reproduction. Second-author paper AMoS accepted at **IEEE INFOCOM 2025**.

Noise-Aware Screen-Camera Communication

USTC

Supervised by [Prof. Xiang-Yang Li](#) and [Prof. Haohua Du](#)

Jan 2024 – Jan 2025

- Focus: Developed INVISICODE, a noise-aware, imperceptible, and high-capacity screen-camera communication system that embeds digital information into images without compromising visual quality.
- Designed an adaptive DCT-based encoding algorithm with an optimized and lightweight U²-Net for precise region localization, achieving 784 bits per frame at BER<0.05 and significantly outperforming prior intra-frame methods.
- Contribution: Participated in idea discussions, optimized and lightweighted the U²-Net model, and contributed to most of the paper writing (excluding evaluation). Co-first author paper accepted at **IEEE/ACM IWQoS 2025**.

Backdoor Attacks on Large Audio Language Models

Online

Supervised by [Prof. Yuan Hong](#), University of Connecticut

Apr 2025 – Ongoing

- Focus: Investigating backdoor vulnerabilities and corresponding defenses for multimodal and large audio language models, emphasizing real-time, continuous acoustic triggers and robustness across deployment conditions.
- Surveying state-of-the-art multimodal models (e.g., Qwen3-Omni, Mini-Omni2, MiniCPM-O 2.6) and establishing an evaluation pipeline to measure attack effectiveness and stealthiness.
- Contributing to the experimental framework by curating multilingual speech datasets and trigger variants, and implementing baseline insertion and evaluation.

Internships

Algorithm Engineer Intern

Hefei, China

NIO Inc.

Sep 2023 – Mar 2025

- Designed a privacy protection solution for speech data generated in in-cabin and after-sales services.
- Enabled decryption of protected data for specific information based on user or task permissions.

Algorithm Engineer Intern

Hefei, China

Huawei Technologies Co., Ltd.

Jul 2024 – Oct 2024

- Simulated full and incremental EC (Erasure Coding) workflows for distributed SSU modeling.
- Designed algorithms for IO aggregation and EC mode cost comparison to improve storage efficiency.
- Implemented hot stripe simulation and load-balanced EC disk scheduling strategies.

Academic Awards

| | |
|---|------------------------------|
| Graduate Academic Scholarship, USTC (¥12000×3) | Sep 2023, Sep 2024, Sep 2025 |
| Second Prize, Ubiquitous Intelligent Sensing Technology Innovation Application Competition, CCF | Nov 2024 |
| National Scholarship (top 0.2% in China) , Ministry of Education, China (¥20000) | Oct 2024 |
| Longfor Scholarship, USTC & Longfor Properties Co., Ltd. (¥5000) | Sep 2022 |
| Meritorious Winner, Mathematical Contest in Modeling (MCM), COMAP | Feb 2022 |
| Gold Medal, International Genetically Engineered Machine Competition (iGEM) | Nov 2021 |
| Outstanding Student Scholarship, USTC (¥1000) | Sep 2021 |

Services

| | |
|--|---------------------|
| Teaching Assistant, Freshman Seminar (Prof. Xiang-Yang Li) | Sep 2024 – Present |
| Teaching Assistant, Fundamentals of Algorithms (Profs. Xiang-Yang Li & Haisheng Tan) | Sep 2024 – Jan 2025 |
| Teaching Assistant, Computer Security (Prof. Shaoyin Cheng) | Mar 2023 – Jun 2023 |
| Volunteer Team Leader, Youth Volunteer Association, USTC | Sep 2019 – Jul 2022 |

Skills

Programming languages: Python, C/C++, MATLAB, Java, Swift
Web Technologies: HTML, CSS, JavaScript
Deep Learning Tools: PyTorch, Tensorflow
Miscellaneous: MySQL, Linux, Git, LaTeX, Markdown
Language: English: Professional working proficiency (TOEFL 92), Chinese: Native