

Jingmiao Zhang

📍 Hefei, China ✉ Email@USTC ✉ Gmail 🔗 Webpage

Education

University of Science and Technology of China (USTC)

Hefei, China

B.E. in Information Security

Sept 2019 – Jun 2023

- Core Courses: Elements of Information Theory, Foundation of Algorithms, Operating System, Compiler Theory, Introduction to Cryptography, Computer Security, Network Security Protocols

University of Science and Technology of China (USTC)

Hefei, China

M.E. in Computer Science and Technology

Sept 2023 – Jun 2026

- Core Courses: Design and Analysis of Algorithms, Advanced Computer Networking, Advanced Database Systems, Edge and Cloud Computing, Introduction to Combinations, Computational Number Theory

Research Interests

Security and privacy in intelligent systems, especially in IoT, machine learning, and trustworthy AI.

Publications

- SpeechGuard: Recoverable and Customizable Speech Privacy Protection.** [Paper]
Jingmiao Zhang, Suyuan Liu, Jiahui Hou, Zhiqiang Wang, Haikuo Yu, Xiang-Yang Li.
In *The 34th USENIX Security Symposium*, 2025.
- Task-Oriented Training Data Privacy Protection for Cloud-based Model Training.** [Paper]
Zhiqiang Wang, Jiahui Hou, Haifeng Sun, *Jingmiao Zhang*, Yunhao Yao, Haikuo Yu, Xiang-Yang Li.
In *The 34th USENIX Security Symposium*, 2025.
- AMoS: Autonomous Multimodal POI Standardization without Extra Annotation.** [Website]
Suyuan Liu, *Jingmiao Zhang*, Haikuo Yu, Yan Zhang, Yuetian Wang, Guobin Shen, Xiang-Yang Li.
In *IEEE International Conference on Computer Communications (INFOCOM)*, 2025.
- 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.
Submitted to IWQoS 2025.

Research Experience

Summer Workshop Participant

Online

National University of Singapore (NUS)

May 2022 – Jul 2022

- Attended lectures on simulation, security, big data, and cloud computing.
- Contributed as part of a four-member team to complete a practical project and course paper.

Task-Oriented Speech Data Protection

USTC

Supervised by *Prof. Xiang-Yang Li*

Feb 2023 – Mar 2024

- Focus: Developed SpeechGuard, a system for recoverable and customizable speech privacy protection, enabling fine-grained access control over both acoustic and content privacy.
- Designed a multi-parameter warping function with an inverse transform for reversible acoustic privacy protection.
- Developed an adaptive encryption mechanism for automated/manual sensitive text protection and permission-based content recovery.
- Introduced a hierarchical access control model, allowing listeners to recover varying levels of information based on assigned keys and warping parameters.
- Outcome: First-author paper SpeechGuard accepted at USENIX Security 2025, demonstrating superior anonymity, sensitive content confidentiality, and attack resistance over three baseline systems.

User Context Awareness

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 seamlessly integrates digital information into the physical world without compromising visual aesthetics.
- Conducted a quantitative analysis of screen-camera noise and designed an adaptive encoding algorithm that dynamically distributes data across multiple DCT coefficients, enabling mathematically bounded, noise-aware encoding while optimizing imperceptibility and robustness.
- Enhanced U²-Net with Edge-Constraint Loss to improve boundary detection and localization of encoded regions in captured images.
- Outcome: Co-first author paper InvisiCode under review, demonstrating 784 bits per frame throughput at BER<0.05, significantly surpassing previous intra-frame methods while maintaining imperceptibility across various screen-camera setups.

Backdoor Attacks on Speech Large Models

Online

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

Feb 2025 – Ongoing

- Researching backdoor attacks and defenses in speech models, with a focus on real-time continuous attack strategies and countermeasures.

Industry Experience

Algorithm Engineer Intern

Hefei, China

NIO Inc.

Sept 2023 – Mar 2024

- 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 cost comparison between EC modes, improving storage efficiency.
- Implemented hot stripe simulation and load-balanced EC disk scheduling strategies.

Honors

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

Service

Volunteer, Youth Volunteer Association, USTC	Sept 2019 – Jul 2022
Teaching Assistant, Computer Security, USTC	Mar 2023 - Jun 2023
Teaching Assistant, Fundamentals of Algorithms, USTC	Sept 2024 – Jan 2025

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

Hobbies

Minesweeper, Traveling, Reading, Fitness