Yuying Li

+1 913-938-3212 — yuyingli@ku.edu — Lawrence, Kansas

Research Interests

- Security in AI/ML: Adversarial Machine Learning, Generative AI Security, Privacy-preserving Machine Learning
- Responsible AI: AI Misinformation and Misusage, Usable Security of AI Systems
- Advancing AI Applications: Improving Generative Models, Developing Multimodal AI Systems, and Optimizing AI for Cross-disciplinary Challenges in Domains

Work Experience

Security Benefit, Investment IT Team Intern, Topeka, KS, USA July 2022 – May 2023

- Automated business processes, maintained databases, and designed & developed web applications.

Education

University of Kansas, Lawrence, KS, USA
PhD in Computer Science (GPA: 3.94) 2023 – Present

- Advisor: Prof. Bo Luo, Prof. Fengjun Li

University of Kansas, Lawrence, KS, USA
Bachelor in Computer Science (GPA: 3.83) 2019 – 2023
Cybersecurity Certificate
Business Minor

Publications

Yuying Li, Zeyan Liu, Junyi Zhao, Liangqin Ren, Fengjun Li, Jiebo Luo, Bo Luo. "The Adversarial AI-Art: Understanding, Generation, Detection, and Benchmarking." In *European Symposium on Research in Computer Security (**ESORICS**)*, 2024. (Acceptance rate: 16%)

Teaching Experience

Graduate Teaching Assistant, University of Kansas 2023 – Present

- **EECS 678 Introduction to Operating System** – Fall 2024
- **2024 GenCyber Summer Camp for Teachers** – July 2024
- **MVI Summer Project** – Summer 2024
- **EECS 565 Introduction to Information and Computer Security** – Spring 2024
- **EECS 678 Introduction to Operating System** – Fall 2023

Projects

The Adversarial AI-Art: Understanding, Generation, Detection, and Benchmarking, University of Kansas 2024

- Developed a state-of-the-art AI image dataset ARIA. Performed a large-scale user study to assess the human ability to distinguish AI images. Evaluated state-of-the-art AI image detectors, and developed a ResNet-50 classifier to analyze its accuracy and transferability on the ARIA dataset.
- Published a paper on this project, which was accepted by the *European Symposium on Research in Computer Security (**ESORICS**)*, 2024. I presented this work at the conference.

Multiview Multi-model AI Image Detection, University of Kansas 2024

- Implemented a multiview multimodel approach to improve the accuracy of AI image detection systems.
- The paper will be submitted soon.

Deepfake AI Audio Dataset and Detection, University of Kansas 2024

- Led a team of undergraduate summer interns to create a dataset of deepfake AI-generated audio, and developed detection algorithms to identify deepfake audio content and prevent misuse.

Face Expression Recognition, University of Kansas 2024

- Utilized multiple machine learning models to classify different facial expressions, enhancing human-computer interaction.

Delegated Signature Authorization Application, Security Benefit 2023

- Designed an Angular web application to help the company manage investment delegated signature authorization.

House Price Prediction, University of Kansas 2023

- Employed multiple machine learning models (scikit-learn, XGBoost) to predict house prices in Seattle.

Retriever, University of Kansas 2022

- Developed a mobile app using React Native and Back4App to help users recover lost items. Available on Android and iOS.

Skills

- **Programming Languages**
  - **Proficient**: Python, C++/C, JavaScript, TypeScript, PHP, SQL
  - **Knowledgeable**: Haskell, Java, Rust, Go, Bash, Perl, LLVM, Assembly
- **Frameworks & Tools**: PyTorch, TensorFlow, React Native, Node.js, Docker, Git, MySQL, PostgreSQL
- **Languages**: Chinese (Native), English (Proficient)

Scholarship & Awards

- **Rock Chalk Scholarship**, The University of Kansas 2019 – 2023
- **EECS Robb Award**, The University of Kansas 2024
- **Graduate Scholarly Presentation Travel Award**, The University of Kansas 2024

Professional Service

Student Volunteer at ACM Conference on Computer and Communications Security (CCS),
Salt Lake City 2024

- Captured photographs during sessions, breaks, and social events.
- Collaborated with CCS office staff to post updates on social media.