# Hao Cui

Email: cuihao.leo@gmail.com
cuih7@uci.edu
Telephone: +1 858-262-3756
Website: https://cvhc.cc/
https://www.ics.uci.edu/~cuih7
GitHub: @cuihaoleo

## Education

### University of California, Irvine 2020–Today

*Ph.D.* in Networked Systems (GPA: 3.931/4.000, Expected Graduation: Dec. 2024)

### University of Science and Technology of China 2017–2020

*M.Eng.* in Electronics and Communication Engineering (GPA: 3.18/4.30)

### University of Science and Technology of China 2013–2017

*B.Eng.* in Computer Science and Technology (GPA: 3.71/4.30)

*B.Sci.* in Geophysics (GPA: 3.47/4.30)

## Awards

| | |
|---|---|
| **UC Irvine EECS Department Fellowship** | Sep. 2020 – Feb. 2021 |
| **Kaggle Deepfake Detection Challenge**, 2nd place / 300,000 USD | Jun. 2020 |
| **IJCAI-19 Alibaba Adversarial AI Challenge**, 1st place in defense track / 5,000 USD | Aug. 2019 |
| **11th Competition of Physical Research Experiment of USTC**, Special Prize | Dec. 2015 |

## Experience

### UCI Networking Group & ProperData Lab, UC Irvine

*Graduate Student Researcher* / Ph.D. Advisor: Prof. Athina Markopoulou

**Automated privacy policy analysis** 2021-Today

- Proposed PoliGraph, a novel framework that uses knowledge graphs to encode privacy policies.
- Built NLP tools based on spaCy and HuggingFace libraries that use various NLP techniques, notably zero-shot classification and coreference resolution, to extract information from privacy policies.

**Inspecting privacy leakage on VR devices** 2020-2021

- We decrypted network traffic on Oculus VR handsets by using Frida to bypass certificate validation.
- Compared network flows against privacy policies to audit flow-to-policy consistency of VR apps.

### Syntiant Corp., Irvine, CA

*Machine Learning Engineer Intern* / Manager: Sean McGregor

**Exploring biases of voice recognition models** Summer 2021

- Conducted experiments to measure biases of keyword spotting models in gender, age and accents.
- Packaged PyTorch-based scripts into Docker containers to be used in the existing data pipeline.

### CAS Key Laboratory of Electromagnetic Space Information, USTC

*Research Assistant* / Advisor: Prof. Weiming Zhang

**DeepFake video forgery detection** 2020

- Implemented an ensemble classifier that uses WS-DAN and Xception to detect Deepfake frames.
- 2nd place in the Kaggle Deepfake Detection Challenge, a prize competition organized by Facebook.

**Multi-stage defense against adversarial examples for images** 2018–2019

- Proposed a hybrid defense against adversarial attacks on CNN-based image classifiers that combines: adversarial training, model ensemble, multi-scale random filtering and abnormal result detection.
- 1st place in the defense track of the IJCAI-19 Alibaba Adversarial AI Challenge.

**Covert screen-camera communication / Robust image watermarking against screen-shooting** 2017–2020

- Proposed UnseenCode, an invisible on-screen barcode scheme for covert communication and image watermarking, which uses unobtrusive high-frequency color fluctuation on the screen to encode data
- Implemented the UnseenCode demo in C++ and Java that runs on desktop and Android phone.
- Presented the work in both oral and demonstration sessions in IEEE INFOCOM 2019.

# Publications

[1] **H. Cui**, R. Trimananda, A. Markopoulou and S. Jordan, "PoliGraph: Automated Privacy Policy Analysis using Knowledge Graphs," *under review, preprint on arXiv:2210.06746*, Oct. 2022.

[2] R. Trimananda, H. Le, **H. Cui**, J. T. Ho, A. Shuba and A. Markopoulou, "OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR," *in Proc. of USENIX Security Symposium 2022*, Boston, USA, Aug. 2022.

[3] H. Bian, **H. Cui**, K. Liu, Z. Hang, D. Chen, W. Zhou, W. Zhang, and N. Yu, "CDAE: Color Decomposition-based Adversarial Examples for Screen Devices," *in Information Sciences*, 2021.

[4] J. Zhang, D. Chen, J. Liao, H. Fang, W. Zhang, W. Zhou, **H. Cui**, and N. Yu, "Model Watermarking for Image Processing Networks," *in Proc. of the AAAI Conference on Artificial Intelligence*, New York, USA, Feb. 2020.

[5] H. Fang, W. Zhang, Z. Ma, H. Zhou, S. Sun, **H. Cui**, and N. Yu, "A Camera Shooting Resilient Watermarking Scheme for Underpainting Documents," *in IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 30(11), Nov. 2020.

[6] **H. Cui**, H. Bian, W. Zhang, and N. Yu, "UnseenCode: Invisible On-screen Barcode with Image-based Extraction," *in Proc. of IEEE INFOCOM 2019*, Paris, France, Apr. 2019.

[7] H. Fang, W. Zhang, H. Zhou, **H. Cui**, and N. Yu, "Screen-Shooting Resilient Watermarking," *in IEEE Transactions on Information Forensics and Security*, Vol. 14(6), Jun. 2019.

[8] **H. Cui**, and X. Zha "Parallel Image Registration Implementations for GMTSAR Package," *in Seismological Research Letters*, Vol. 89(3), Feb. 2018.

# Skills

**Research**: privacy policy & nature language processing, image watermarking, machine learning security

**Programming**: proficient in Python, C/C++, UNIX shell; basic knowledge in Java, Kotlin, JavaScript, Rust

**Computer Vision**: OpenCV, PyTorch, Tensorflow

**Web Development**: Flask, SQL, browser automation

**GPU Programming**: CUDA, OpenCL, ArrayFire

**NLP**: spaCy, NLTK, HuggingFace

**Mobile & IoT**: Android, Arduino

**DevOps**: Linux, Git, Docker, Podman

# Other Activities

*Server Administrator* of the CAS Key Laboratory of Electromagnetic Space Information 2017–2020

- Managed a computing cluster consisting of 14 Linux servers with 74 GPUs.
- Built the network infrastructure (routers/switches/VPN access) from scratch.

*Teaching Assistant* for the Computer Programming A course at USTC 2016–2018

*President* of the USTC Linux User Group 2015–2016

*CTO & Vice President* of the USTC Linux User Group 2014–2015

- As one of the largest Linux user groups in China, we hold various events to promote free software to university students, and we provided online services like software mirrors to Chinese Linux users.