Yuhao Sun

https://hanssuny.github.io
Email : syh3327@mail.ustc.edu.cn
Mobile : +8618839231761

Education

- **University of Science and Technology of China (USTC)** Hefei, P.R.China
  Master of Information and Communication Engineering; GPA: 3.78/4.30 (88.8/100) *Sept 2023 – Present*
- **University of Science and Technology of China (USTC)** Hefei, P.R.China
  Bachelor of Information Security; GPA: 3.65/4.30 (87/100) *Sept 2019 – Jun 2023*
  - Wang Xiaomo Talent Program in Cyber Science and Technology

Research Interest

- **AI security**: Facial Privacy, Safe & Responsible Generative Model

Publications

- DiffAM: Diffusion-based Adversarial Makeup Transfer for Facial Privacy Protection

  Yuhao Sun, Lingyun Yu, Hongtao Xie, Jiaming Li, Yongdong Zhang.

  IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2024.
- UIAMark: Unified Identity and Attribute Watermarking for Source Tracing and Proactive Deepfake Detection

  Peiqi Jiang*, **Yuhao Sun***, Lingyun Yu, Hongtao Xie, Yun Song.

  To be submitted. (scores in IJCAI 2024: 7,5,5,5,5)

Experience

- **Concept Erasing in Diffusion Models** USTC
  Advisor: Prof. Yongdong Zhang, Prof. Hongtao Xie *Jan 2024 - Present*
  - Implemented existing methods for concept erasing.
  - Analyzed the robustness of existing methods against paraphrase attacks and inversion attacks.
  - Explored the vision-based method for concept erasing from the perspective of conditional distributions.
- **Dual Watermarking for Deepfake Tracing and Detection** USTC
  Advisor: Prof. Hongtao Xie *Nov 2023 - Feb 2024*
  - Proposed a unified attribute and identity watermarking framework for Deepfake tracing and detection.
  - Achieved Deepfake-agnostic detection by leveraging the inherent fragility of high-level facial semantic information (i.e., facial-relevant attributes and identity features).
  - Experiments show that our method achieves a BER of 0.0389% across different distortions and an average detection accuracy of 97.36% across various Deepfake methods in the black-box setting.

  Submitted to International Joint Conference on Artificial Intelligence (IJCAI), 2024
- **Adversarial Makeup Transfer for Facial Privacy Protection** USTC
  Advisor: Prof. Yongdong Zhang, Prof. Hongtao Xie *Jul 2023 – Nov 2023*
  - Proposed a novel diffusion-based adversarial makeup transfer method for facial privacy protection, intending to craft adversarial faces with high visual quality and black-box transferability.
  - Introduced a text-guided makeup removal module to establish the deterministic relationship between non-makeup and makeup domains, offering precise cross-domain alignment guidance for makeup transfer.
  - Proposed a CLIP-based makeup loss for refined makeup generation. It consists of a makeup direction loss and a pixel-level makeup loss, which jointly control the direction and distance of makeup generation.

  Accepted by IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2024

- **Initiative Defense against Deepfakes** USTC
  B.Eng Thesis. Advisor: Prof. Hongtao Xie *Dec 2022 – May 2023*
  - Designed a GAN-based adversarial attack method against Deepfake models.
  - Introduced a dual-branch perturbation generation module with separate controls for perturbation magnitude and perturbation location.
  - Introduced a high-frequency constraint module to enhance the fidelity of adversarial samples.

  Outstanding Undergraduate Thesis of USTC (Top 5%)

Honors

- Lan Feng Scholarship (Top 5%) *Oct 2021*
- Wang Laoji Scholarship (Top 10%) *Nov 2022*
- Scholarship for Talent Program in Basic Disciplines *Oct 2020*
- College Mathematics Competition, 2nd Prize in Anhui Province *Nov 2020*
- College Mathematical Modeling Competition, 2nd Prize in Anhui Province *Dec 2021*

Skills

- **Programming Languages**: Python, C/C++, Java, Matlab
- **Software**: Linux, Visual Studio Code, LATEX, Markdown

Teaching Assistant

- EE1509.01 – Introduction to Multimedia Content Intelligent Analysis *Spring 2024*

Extracurricular Activities & Interests

- USTC EEIS department Basketball Team *Sept 2019 – Present*
  - Won the championship of the USTC Basketball League for five consecutive years from 2019 to 2023.