Student Assistant for Audio and Video Deepfake Generation and Detection

Deepfakes, powered by deep learning, are advancing rapidly in creating hyper-realistic audio and video, offering benefits in entertainment and creative industries. However, they also present serious security, privacy, and ethical risks, including identity fraud, disinformation, and content manipulation. As deepfakes become more prevalent, concerns around detection and mitigation grow. Detection techniques aim to identify altered content and prevent misuse, while privacy risks arise from ML models replicating identities without consent. Additionally, fairness and bias in datasets can distort both generation and detection algorithms.

For our research projects, where we investigate open challenges in deepfake generation and detection, we are looking for excellent student assistants who are motivated to contribute to these cutting-edge research areas. Your tasks include

- Conduct experiments to analyze the generation and detection of deepfakes in both centralized and distributed systems.
- Implement audio and video deepfake generation algorithms and analyze their security, privacy, and fairness aspects.
- Develop detection techniques to counter deepfake threats and protect against misuse.
- Explore new attack- and defense strategies to improve the robustness and security of deepfake-related technologies.

Prerequisites

- Good knowledge in computer security, privacy, and deep learning.
- Experience with Python.
- Recommended: Experience with ML libraries in Python, such as Pytorch or TensorFlow.
- Familiarity with audio/video processing techniques is a plus.
- Strong analytical skills and motivation to work both independently and in a team

Contact

If you are interested in this highly relevant and trending topic, contact Sasha Behrouzi and Kavita Kumari via info@trust.tu-darmstadt.de to learn more. Please include a brief overview of your study background and a transcript of records

Technische Universität Darmstadt
FB Informatik – System Security Lab
S2|20 (CYSEC Gebäude)
Pankratiusstraße 2
64289 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

June 2024