EAGER: SAVED: Secure Audio and Video Data from Deepfake Attacks Leveraging Environmental Fingerprints

Challenge:

- Deepfaked video, audio or photos are highly disturbing and able to mislead the public, raising further challenges in policy, technology, social, and legal aspects.
- "Fighting fire with fire" approaches lead to an endless AI arms race.

Solution:

- To secure audio and video data streaming against deepfake attacks leveraging unique environmental fingerprints, i.e. the Electrical Network Frequency (ENF) signals embedded when the video/audio was generated.

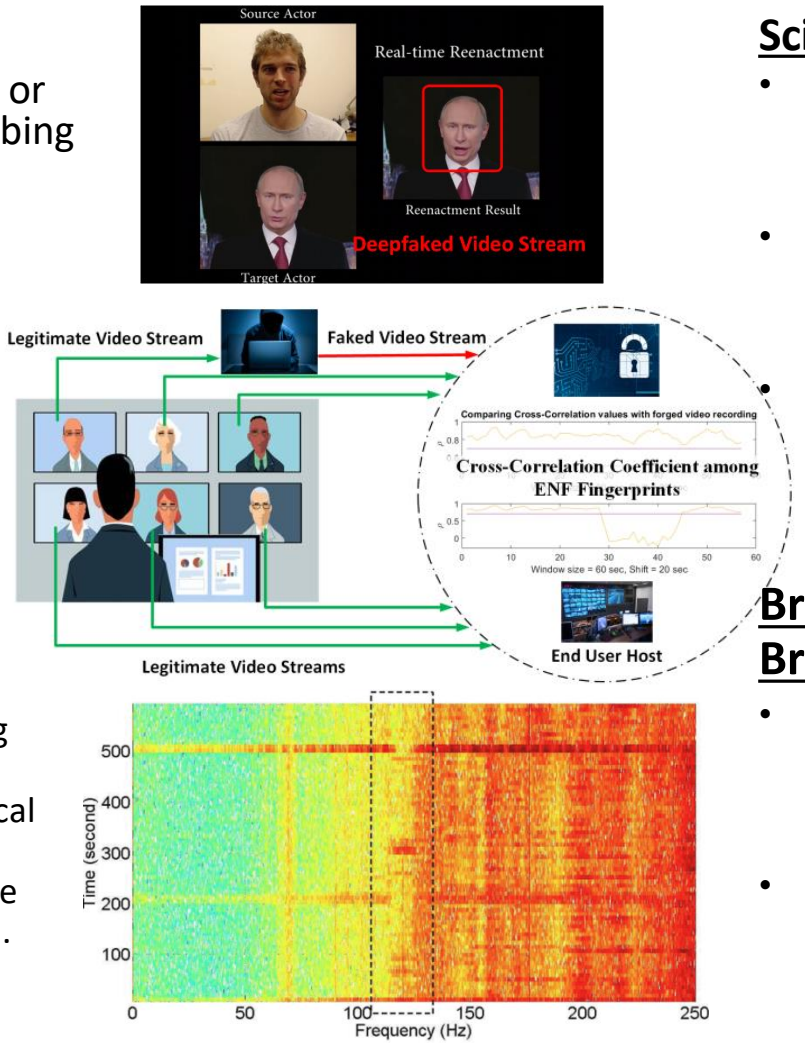

Figure 1. Detecting deepfake attacks using ENF signals as a unique fingerprint.

Scientific Impact:

- A deeper understanding of deepfaked AVS data in terms of embedded, invisible electromagnetic signals.
- A comprehensive exploration of ENF signals as a spatial-temporal correlated environmental fingerprints.
- A robust IoVT in edge computing paradigm being capable of online, real-time detection of fake AVS.

Broader Impact and Broader Participation:

- This project advances the research frontier of data security toward more reliable, secure, real-time AVS applications.
- It enhances mission-critical, delay-sensitive applications where fake or false inputs will cause disastrous consequences.
- Underrepresented and minority students are recruited and trained.

Project Number: CNS-2039342

Institution: Binghamton University
Contacts: Dr. Yu Chen
ychen@binghamton.edu