Cognitec White Paper

Countering Facial Image Forgeries and Manipulations

Recent years have seen significant advances in face forgery and manipulation methods that make it possible to create genuine-looking images and videos with modified facial identities.

Deepfakes in particular—the exchange of a face in an image or a video with the face of a different person—have become known to a wider public due to media coverage on high-profile cases.

Methods

Various types of face forgery and manipulation (see [1]) may be used to spoof a face recognition system. In that context, these types appear to be the most relevant:

- **Deepfake:** Replacing the face of one person in an image or video with the face of another person
- **Morphing:** Creating an artificial biometric face sample that resembles the biometric information of two or more individuals
- **De-identification:** Removing the identity information present in a face image or video. The deepfake method is one way to achieve this.

Spoofing face recognition systems

The spoofing of a face recognition system may serve either 1) to simulate a different identity that is known to the system, in order, for example, to gain access to something, or 2) to hide one's identity.

In this context and based on the above forgery and manipulation methods, the following threats should be considered:

- Deepfakes might be used for presentation attacks with video replays, that could even overcome a simple presentation attack check employing a stimulus/response method, e.g., asking the user to blink, smile, nod, or turn the head.
- Morphing might be used for obtaining an ID document that can be successfully used by a different person in biometric identity checks, e.g., in automated border control gates.
- De-identification might be used to manipulate surveillance videos, with the goal to conceal the occurrence of a certain person.

Deepfake example: Burt Reynolds replaces Sean Connery in a James Bond scene

Morphing example 1: Face in the middle is a mixture of the two outer images

Morphing example 2: Using a less sophisticated method produces a morphed image of poor quality

Automatic detection

A potential countermeasure against such threats is the automatic detection of face forgeries. Such measures are subject of the EU project iMARS [2], in which Cognitec participates and which focuses on morphing detection.

The drawback of this approach: Even if current forgeries may be detected with high probability, we expect that forgery and manipulation methods will improve. Therefore, manipulated images will be harder to detect, requiring improved detection methods in turn, and resulting in an "arms race".

Cognitec maintains the opinion that creating a sustainable detection method is impossible or, at least, extremely hard.

Upfront prevention

Cognitec suggests a much better solution that would prevent forgeries from entering a biometric system in the first place: Securing all processing steps from capturing a biometric sample to presenting it to the biometric system. Establishing such security includes:

1. Capturing biometric sample

- have control over the sensor, i.e., the (digital) camera
- make sure the captured face belongs to a real person in front of the sensor, and check for a presentation attack through human supervision or a suitable automated method

2. Transmitting the captured sample to the computer/network running the biometric system

- prevent any outside access to the transmission channel, or
- add digital signatures to the samples and use end-to-end encryption between the sensor and the biometric system

3. Presenting the sample to the biometric system

- prevent unauthorized access to the biometric system, including unauthorized presentation of biometric samples

Summary

In sum, Cognitec advocates organizational and technical measures to prevent facial forgeries from entering a biometric system upfront, instead of augmenting the system with forgery detection techniques that have to keep up with ever-improving face manipulation methods.

References

[1] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales and Javier Ortega-Garcia. DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection. arXiv preprint:2001.00179v3, 2020.

[2] https://imars-project.eu/

Images

Deepfake example:

https://www.youtube.com/watch?v=xkqflKC64IM

Morphing example 1:

https://computingforpsychologists.wordpress.com/2011/09/11/image-morphing-and-psychology-research-a-case-study

Morphing example 2:

https://commons.wikimedia.org/wiki/File:Morphing5images.jpg

Cognitec

The trusted face recognition company since 2002