Peyton Hall

Lab 6 Question 1

Deep Fakes Research

There are many deep learning techniques being used to detect deep fakes. Primarily, convolutional neural networks (CNNs), which "extract visual features from frames or facial regions of the input video" [MDPI 5]. These networks can be trained to spot irregular patterns in the skin, background noise, and lighting that suggest manipulation. One of the most efficient ways in detecting deep fakes is to examine blinking patterns. For example, according to MDPI, one study "observed one of the vital features of human facial activity, that is, eye blinking rate, for authenticating the physiological signal that is not properly incorporated in the synthesized fake videos, as demonstrated in Figure 1" [MDPI 3]. Figure 1 displayed frame-by-frame observations extracted from a video of Tucker Carlson speaking, where "authors calculated the average time duration between consecutive eye blinks and the average time of eye blinking to be noticed for detecting real or fake videos." Carlson is a phenomenal example for this study because, as his audiences likely recognize, he has very distinct mannerisms. Moreover, researchers are exploring the use of recurrent neural networks (RNNs), which "are proposed to extract the features at various micro and macroscopic levels for detecting Deepfake" [ieeexplore]. Researchers are also using long short-term memory networks (LSTMs). They are used when "image/video contents are hashed and encoded" [ieeexplore]. These are some of the main techniques.

Generative adversarial networks (GANs) are also significant in deep fake detection. They can be defined as follows: "Generative adversarial networks (GANs) are generative and sophisticated deep learning technologies that can be applied to generate fake images and videos that [are] hard for a human to identify from the true ones" [Almars, scrip.org 1]. They work by training two models simultaneously: a generator that creates images and a discriminator that attempts to detect whether an image is real or fake. This method enhances the detection models' ability to distinguish variations between authentic and manipulated content.

There are many ethical issues related to deep fakes. The most notable include privacy, misinformation, and trust in media. The ability to create realistic videos or images can bring misuse and abuse in various forms. That could include creating false evidence, impersonating public figures, or manipulating election processes. These issues could bring about serious threats to peoples' reputations. If misinformation spreads rapidly, harmful consequences follow. Consent can be another issue. Without a person's consent, is it right to use deep fakes that falsely portray them? Most people would agree not. Legal frameworks could protect individuals from harm caused by these deep fakes.

These insights point out how advancements in technology can bring about good and bad results. As the field of machine learning evolves, technical and ethical laws should be developed continuously. Ethical rules would manage the risks that come with deep fake technologies.

https://www.mdpi.com/2079-9292/13/1/95 [MDPI]

https://ieeexplore.ieee.org/document/9721302 [ieeexplore]

https://www.scirp.org/journal/paperinformation?paperid=109149 [Almars, scrip.org]