Deepfake - Video

3 min

Photoshop has been around for ages, and with it, a skilled user could make anything look real. Because of this, many people argue that images have lost some credibility when presenting the truth. And while computer graphics can create and recreate countless things, we, as people, can recognize the signs of computer animation.

Unfortunately, with the advent of deepfakes, video-based content is becoming harder and harder to decipher. As with all AI, continued advancement has led to massive improvements in artificially created content. And while some of this content has been used for good, malicious actors are never far behind when adopting new technology.

The exact way these models are created varies, but many use a Generative Adversarial Network (GAN). Within a GAN, two neural networks are simultaneously trained in such a way that they compete against one another. In these models, one network operates as a generator, creating new content based on previously provided data. The other network serves as the discriminator, which attempts to determine how realistic the content from the generator is.

By allowing these models to compete, they both slowly improve one another. Given enough time, the generated content soon becomes nearly undisguisable from the source material.

In a recent example of the dangers of these models, in 2022, a deep fake video was maliciously uploaded to a Ukrainian new site. In the video a low-resolution copy of the president of Ukraine can be seen asking his army to surrender to Russian forces. While it is evident that something seems off in the video, the unexpected nature caught many people off guard. Following the release of the video, multiple press releases were made to assure the Ukrainian forces that the video was a deepfake.

Even though the video may not have been as high quality as some today, the message and nature of the content required significant government action to ensure the overall safety and security of the Ukrainian people. This type of misinformation creates a dangerous reality.

Of course, attacks of this nature are not solely focused on international politics either. In early October of 2023, scammers attempted to use a deep fake video masquerading as Mr. Beast, as well as several BBC broadcasters. Videos were found circulating on social media, which appeared to be Mr. Beast stating he was running “the world’s largest iPhone 15 giveaway.” The video indicated that he was giving away iPhones for $2. Videos faking the BBC broadcasters appeared to show the broadcasters supporting investment opportunities. Unfortunately, it’s not known how many users fell victim to these attacks.

However, given that these attacks continue to occur, it is likely that these types of deepfakes are successful in their overall goals for fraud.


ORIGINAL
DEEPFAKE
M HONEST
Y *THIS* ONE
M HONEST
Y *THIS* ONE