Even Deepfake fraud detection tools can be deceived

Fake news is really becoming a worldwide problem. Deepfake is part of that mess.

In the era of internet growth as well as social media platforms with billions of users today, fake news is really becoming a problem worldwide. Deepfake is part of that mess.

Deepfake is a technology that synthesizes human images based on artificial intelligence (AI) using a machine learning technique called Generative Adversarial Network. With this feature, it is often used to create fake news and malicious scams. Deepfake videos began to flood the internet a few years before the bad actors realized they could be used to defame personal reputation, illegally profit and spread false political information. With the continuous improvement of AI algorithms, Deepfake is becoming more and more difficult to detect than ever.

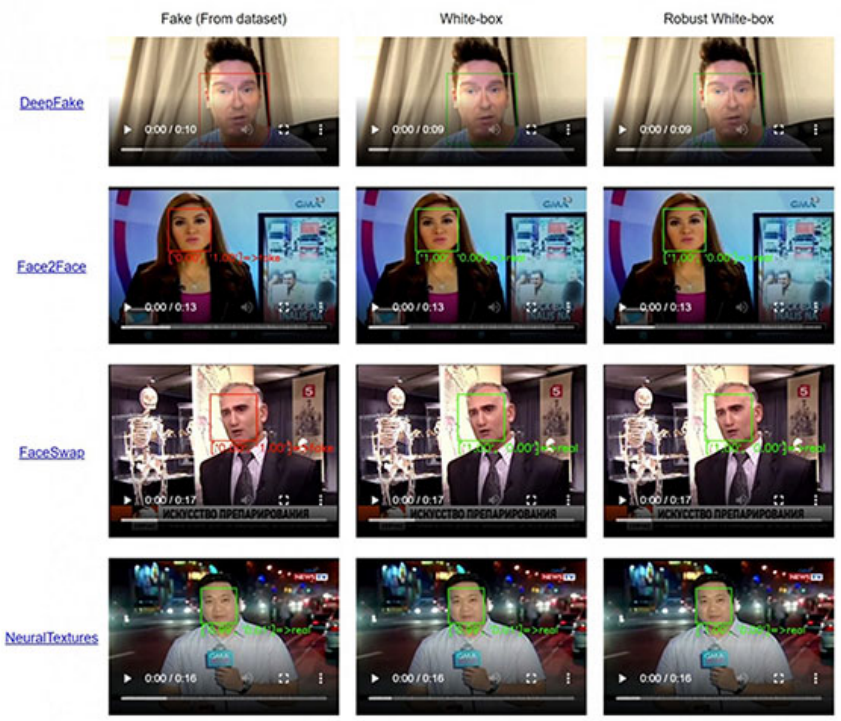
In response to the Deepfake problem, security experts have developed AI tools that can decipher the code composition as well as the smallest details of a pixel-level image and video to detect phishing. . But when this security technology is gradually becoming effective, difficulties continue to appear.

A team of researchers from the University of San Diego recently found a relatively simple method to deceive the very latest AI-based fake video detection systems.

Accordingly, the team has made a few code tweaks to the fake videos synthesized using existing Deepfake creation methods. Specifically, for codecs compressing images and videos, thereby creating complex contradictory disturbances that the Deepfake detection tool could not decipher and leave fake content.

The first image below shows the Deepfake detection tool working properly, while the second video shows what happens when researchers make some tweaks designed to deceive the detection tool. Deepfake, although the difference is almost imperceptible to the naked eye.

Basically, fake video detection tools examine each frame of the video to identify abnormal changes. The University of San Diego research team has developed a process to put jamming information into each frame, causing the Deepfake detection tool to assume that the video is normal.



This study has shown that modern counterfeit video detection systems still contain serious limitations. In essence, it can be concluded that malicious 'highly skilled' agents could find a way to deceive all of the existing Deepfake identification tools.

You finished reading the article "**Even Deepfake fraud detection tools can be deceived**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com