DEC 2019 - VOLUME I

Deep Fake- AI threats to Cyber security

When AI takes identify thefts to next level

INTUITION PUBLISHING PTE LIMITED

DeepFake comes from “deep learning” and “fake”. Artificial Intelligence technology used to create fake videos and audio that look and sound real. With the recent advances in AI technology DeepFake are now virtually indistinguishable from originals.

Previously only available to studio professionals, there are numerous websites and mobile applications allowing anyone to create DeepFake videos and audio. So what is the problem with this new technology you might ask? Well it all started in some dark seedy part of the internet, where the faces of famous Hollywood actresses were being morphed onto inappropriate movies. This taken identity theft on a whole new level, if you can take pictures, video & audio and alter in such a way, it is very easy to impersonate anyone.

People will believe what they want to believe due to the way our brains works, deep fact checking of visual or audio cues are often overlooked. Additionally, confirmation bias is a tendency where once we have formed an opinion, we cherry-pick information that confirms our prejudices. Situations are not perceived objectively, leading to misjudgements and false information. All of this plays into the power of DeepFake and misinformation.

This year, a U.K. based energy firm’s CEO was scammed over the phone and ordered to transfer €220,000 into a Hungarian bank account by an individual, using audio DeepFake technology to impersonate the voice of the parent company's chief executive. It’s the first noted instance of an AI generated voice DeepFake used in a vishing scam, though it certainly won’t be the last.

In May 2019, Nancy Pelosi (speaker of the United States House of Representatives) was the subject of two videos, one of which had the speed slowed down to 75 percent, and another which edited together parts of her speech at a news conference. Both videos were intended to make Pelosi appear as though she was slurring her speech. President Donald Trump shared the latter video on Twitter, captioning the video "'Pelosi Stammers Through News Conference'". These videos were featured by many major news outlets, which brought DeepFake to the attention of the United States House Intelligence Committee.

The manifestation of DeepFake makes identifying videos as spoof or genuine increasingly difficult. People need to know how fast information can be altered with DeepFake technology, and that the problem is not a technical one, but one to be solved by trust in information and journalism.

Caption: The accessibility of DeepFake technology has created a new wave of social engineering attacks for which your current cyber security defences may not be prepared.

The primary concern is that humanity could fall into an age in which it can no longer be determined whether a medium's content corresponds to the truth. DeepFake created for malicious use, such as fake news, will be even more harmful if nothing is done to spread awareness of DeepFake technology.

Part of the problem is the shift in how younger generations access news and information. Long gone are the days of reading the Sunday papers and evening news, most people today are glued to their mobile devices and accessing news and information through social media feeds and influencers. We are in the era of “Fake-News” and trust in information has been seriously eroded. From election influencing, mass social engineering and even political parties themselves being caught in the act of creating fake news.

What can be done to prevent such problems? The most popular technique is to use algorithms similar to the ones used to build the DeepFake to detect them. By recognizing patterns in how DeepFake are created, the algorithm can pick up subtle inconsistencies.

Researchers have developed automatic systems that examine videos for errors such as irregular blinking patterns of lighting. This technique has also been criticized for creating a "Moving Goal post" where anytime the algorithms for detecting get better, so do the DeepFake!

Other techniques include the use of Blockchain Technology which verify the source of the media. Videos will have to be verified through the ledger before they are shown on social media platforms. With this technology, only videos from trusted sources would be approved, decreasing the spread of possibly harmful DeepFake media.

Intuition-Know How

The Intuition Know-How Library consists several tutorials related to this article:

- **FinTech**
  - Blockchain Structure & Security
  - Smart Contracts & Blockchain Applications
  - Cryptocurrencies & Initial Coin Offerings (ICOs)
  - Robotic Process Automation (RPA)
  - Artificial Intelligence (AI)
  - And More...
- **Cyber Security Awareness (GCHQ-UK Certified Training)**
  - Passphrases
  - Preventing Identity Theft
  - Device Security
  - Malware & Breach Recovery
  - Social Engineering
  - And More…

For Intuition blended learning related to this article, some of our popular workshops include:

- Cutting Edge Technology In Finance – Big Data, Artificial Intelligence And Machine Learning
- Disruptive Technology In Financial Services
- The Fintech Revolution: Crypto Currencies, Blockchain, DLTs & Applications

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours.
Get in touch with your Intuition account manager at apacinfo@intuition.com for more details

Related News Articles

- *Terrifying new Chinese app Zao lets anyone make a deepfake-Digital Trends-Sept 2019*
- *A Voice Deepfake Was Used To Scam A CEO Out Of $243,000-Forbes-Sept 2019*
- *The real news on ‘fake news’: politicians use it to discredit media, and journalists need to fight back-The Conversation-Oct 2019*