Research Paper

GYAN MANAGEMENT

AN INTERNATIONAL BI-ANNUAL REFEREED JOURNAL OF MANAGEMENT & TECHNOLOGY

Year 2023, Volume-17, Issue-1 (January - June)

ISSN 0974-7621 (Print)

ACS Publisher www.acspublisher.com

GIANJYOTI Institute of Management and Technology

DeepFakes- The Digital Threat in the Real World

Sandeep Singh Mankoo

Certified Ethical Hacker, Certified Cyber Forensics Professional

ARTICLE INFO

Key Words: Deepfakes; Cyber Crime; Deep Machine Learning; AI; DeepFake Videos

ABSTRACT

Objectives: Understanding and Tackling the alarming surge of Digital Imposters known as the world of DeepFakes.

Methods: Using Artificial Intelligence based Deep Machine Learning software; Cyber Forensics; Physical mind awareness and alertness! Deepfakes use Artificial Intelligence and Deep Machine Learning techniques to make fake images, of people and events, which are as attractive/ authentic as the original. Deepfakes is the next big Challenge in Cyber Security, taking the Security mindset to the next high level.

Findings: On date we have no Specialized High-Tech support at hand to handle such an extremity. We can't even imagine that if it was a crisis. The impact might be ruinous; it can be anything. In one of the recent live impersonation cases, A Mayor of Berlin thought he was having an online meeting with former boxing champion and current mayor of Kyiv, Vital Klitschko, but later on turned out to be a conversation with a deepfake, an AI generated fake videotape, looking real and authentic. Previous DeepFake videos had some tell-tale signs that a commodity/ person/ event wasn't real; edit or odd movements. Not presently.

In recent Delhi Elections, the BJP Candidate Mr. Manoj Tiwari fabricated his old speech on "Citizenship Amendment Act" into a political campaign speech to reach different linguistic voter bases, especially Haryanvi voters. Tiwari did not have any knowledge about Haryanvi, but made his political campaign message reach Haryanvi voters through DeepFake Technology.

Novelty: Massive Online Videos on Internet!

Received 08.01.2023; Accepted 10.01.2023

DOI: 10.48165/gmj.2022.17.1.8

Introduction

Ransomware has been keeping the Cyber Security Brigades and the world on its toes. The Information Security & Cyber Security challenges in this ever-expanding galaxy of Internet of Things and of cloud computing have drastically modified the dimensions of the ever-fragile cyber security domain. However, we are formally in the age of digital imposters, it is an alarming surge coming for sure, prominently known as the world of Deep Fakes.

DeepFake is a synthetic media, driven by Artificial Intelligence (AI) Technology. In this an existing image or video of a person or event is replaced with someone else's likeness.

Diving Deep in DeepFakes i.e tackling them will going to be very tough job. A normal person (both techie and non-techie) will not be able to differentiate between the real and the fake content, and that is the time, when the fake case story of unknown problem begins. With every new sunrise, DeepFakes becomes more efficient at mimicking the real people. Under the light of this emerging threat, everyone feels that they are now endangered. You don't know when you are being deceived or cheated. The current scamsters would start looking Lilliputian. One surreal scenario; think of a conference call taking place inside an office building, but how to get convinced that the identity of the person on the other side of the call is legitimate and authentic as who they say they are.

Cyber culprits are formerly using this technology phenomenon for stealing plutocrat (wealth). While Ransomware generates more news captions, Business Email Compromise (BEC) is the most expensive form of Cyber Crime today. After being so much aware and vigilant, we still fall prey to Spoofing and Phishing attacks and that too in more authentic scenarios. And at the same time if the Cyber culprits use DeepFake videos to lure us from the other end, it would be pretty more delicate and expensive to deny the request. Imagine your Master speaking to you on camera call. Generally, most organizations put at least some details of their senior leaders on the web portal. Information in the Public domain can be misused to create DeepFake. Phone calls are the most inexpensive, easy-to-use and always available tool to Scammers to generate crimes. Thus, Deepfakes are now becoming remote IT support at large organizations to get access to their sensitive information. This way, it is also being used to impact foreign operations. The FBI has issued non-technical advice on how to notice a deepfake. But deepfakes are bound to emerge as a new vector of Cyber Crime.

Pledge to Win the Double-Edged Battle of Technology.

Methodology

The DeepFake Development

Reddit, is an American Social News Networking company. Here the registered members can discuss, create, rate or enhance any content pertaining to their interests, hobbies or passion, all within the community network. One of the users named "DeepFake" used Generative Adversarial Networks (GAN assisted) to create fake videos in the year 2017. Similarly with the advancement of time, other users shared their DeepFake videos in the same Deepfake community of Reddit. They swapped the faces of many Hollywood and other actresses viz. Gal Gadot, Taylor Swift, Scarlett Johansson to create pornographic videos. Much to their interest they even created non-pornographic videos of Nicholas Cage, Barack Obama, Nancy Pelosi, Donald Trump and many more!

Later in 2018, a legitimate Desktop Application named Fake App was launched. The Fake App facilitated it users to create and share videos, wherein their faces are swapped in pictures. Zao, an app from the Chinese Mobile giant Momo, facilitated its users to superimpose their faces on videos and live clips, using a single picture. Datagrid, a Japanese AI Company, developed a deepfake that helped create a full body person from scratch. Impressions, a mobile Deepfake App launched in March 2020, catered to much needed activity, I.e., creation of Celebrity Videos on Mobile Phones.

Today the DeepFake is fully developed industry, where the word "Deep" is derived from the Machine Deep Learning concept of Artificial Intelligence (AI) technology. It involves training generative neural network architectures such as autoencoders or the aforesaid Generative Adversarial Networks (GANs).

DeepFakes has been a most attention seeker amidst its use in creating Child Sexual Abuse Material, Celebrity Pornographic Videos, Revenge Porn, Fake News, Hoaxes, Bullying and Financial Frauds. An Evoked concern from the Industry and many Governments worldwide to detect its presence anywhere and minimize its use.

The DeepFake development software are abundantly available on the internet. The most prominent among them known as DeepFaceLab is available on this link: https://github.com/iperov/DeepFaceLab

How DeepFake Works?

As mentioned earlier, the term “DeepFake” relates to the underlying technology “deep learning,” which is a subset of AI. The Deep learning algorithms, are used to solve problems where large data sets are involved. These algos provide help to swap faces in video and digital content in order to make feel the fake media as realistic.

There are several methods/techniques available for Deepfakes production, but the use of deep neural networks containing autoencoders that engages a face-swapping technique is the most common method.

In this, select a target video to use as the basis of the deepfake and then few sets of (a collection) video clips of the person you want to insert in the target.

Note: The collection videos can completely be unrelated; the target might be a short video clip from a Bollywood movie, and the videos of the said person which are required to be inserted in the film can be some random clips downloaded from Internet viz. YouTube.

The autoencoder is a deep learning AI program which is used to analyze the video clips to understand the geometry of the person face sketch from different angles and under several environmental conditions like cold, hot, aqua, dry, etc., and further mapping that person face onto the individual in the target video by discovering some shared common features.

Another AI technology, the Generative Adversarial Networks (GANs) is an append to the project, which helps to detect and improve any flaws in the deepfake among multiple cycles, making it more intense for deepfake detectors to decode the videos.

GANs are by and large used as a most popular method for creation of deepfakes, based on the study of large amounts/sets of data to implement learning of development of new prototypes that imitate the original content, with forcible labored non-deviating errorless results.

Some of these following apps and software’s help generate deepfakes easy for novice beginners, viz. the Chinese app Zao, DeepFace Lab, FaceApp (a photo editing app with built-in AI techniques), Face Swap, and the banned removed DeepNude, a specific dangerous app that generates fake nude images of women.

GitHub, an online software development open-source community holds a big number of DeepFake Apps. Quite a good number of these apps are used for pure entertainment purposes - which prevents DeepFake from Constitutional Law Prohibition - whereas other large number are far more likely to be used maliciously.

Owning of more sophisticated AI technology in the future, the DeepFake may further develop and might introduce more serious threats to the public, relating to election interference, political tension, and additional criminal activity.

The DeepFake Producers

Everyone from academics of School/College to Corporate Industrial Professionals/ researchers to amateur enthusiasts/ fanatics, small scale to large scale visual effects studios, political actors/ movers, porn producers and the list goes on!

The Technology Requirements

Being DeepFake is a serious and hectic journey of development of non-existent truth. Thus, it needs equivalent amount of hard work and dedicated efforts to create the much real life like videos! It is usually difficult to make a good deepfake on a standard computer with less of memory and graphics utilities. Therefore, almost all Deepfakes are created on high-end desktops with powerful graphics cards or with equivalent computing power in the cloud. This increases the portability of the video development and significantly reduces the processing time from n number of days to couple of hours. But we should not forget to takes experts help, too, at least to touch up the finished videos to reduce flicker and remove other visual defects. Thus, many tools are now available online to help masses develop DeepFakes. If a certain individual is not able to own a DeepFake development app, then they can approach vendor companies which can develop it for them by doing all the processing in the cloud. Mobile users can make use of the app, Zao, that lets them add their face sketches to a list of TV and movie characters on which the system has been trained.

How DeepFakes are used?

While the capability to automatically change faces to produce believable and realistic looking synthetic videotape has some intriguing benign operations (similar as in cinema and gaming), this is obviously a dangerous technology with some disquieting operations. One of the first real- world operations for DeepFakes was, in fact, to produce synthetic pornography.

In 2017, a reddit stoner named" DeepFakes" created a forum for porn that featured face- shifted actors. Since that time, porn (particularly vengeance porn) has constantly made the news, oppressively damaging the character of celebrities and prominent numbers. According to a Deeptrace report, pornography made up 96 of deepfake vids set up online in 2019.

Deepfake videotape has also been used in politics. In 2018, for illustration, a Belgian political party released a videotape of Donald Trump giving a speech calling on Belgium to withdraw from the Paris climate agreement. Trump no way gave that speech, still it was a deepfake. That wasn't the first use of a deepfake to produce deceiving videos, and tech- smart political experts are bracing for a unborn surge of fake news that features convincingly realistic deepfakes.

Of course, not all deepfake videotape poses an empirical trouble to republic. There is no deficit of deepfakes being used for humor and lampoon, similar as chips that answer questions like what would Nicolas Cage look like if he is appeared in" Aggressors of the Lost Ark"?

Results and Discussion

The DeepFakes Detection

- **Unnatural Eye Movements**- Eyes tilting towards one particular side, not blinking or not maintaining the eye-contact with the other person or camera lens.
- **Unnatural Lip Movements**- Irrespective the words spoken, there is no respective lip movement, or the lips are in motion, even in the absence of the audio speech.
- **Unnatural Facial Expressions**- Facial expressions do not change as per the context of the words spoken or when heard from another person. The shocking news or excitement news does not display likewise facial expressions.
- **Awkward Face position with respect to other subjects**- Facing towards a blank part of the room, or towards an angle which does not have any object or person in focus.
- **Difference between skin color tones**- Patchy skin appears when two different skin tone bodies are mixed or joined digitally.
- **Angle formed by the Shadow of the human body**- Shadows formed by the overhead light will be shorter as compared to any other angle of light projected on the body. But if every time the shadow remains the same, irrespective of light than its fake shadow.
- **Awkward looking body posture**- Long legs and short arms or vice versa. The body may be leaning towards a specific side or an angle, throughout the program, or one particular sitting posture is difficult to maintain for a longer duration.
- **Unnatural Body Movement**- Being in the presence of some senior political leader or country head, the body movement cannot prolong till the conversation lasts. The body movement is curtailed to maintain decorum. Hence, it's a flaw.
- **Emotionless Body**- No matter whosoever or whatsoever is being presented on the screen, if the body of the person does not show similar emotions, then it's a flaw.
- **Artificial Hair looks**- Artificial hair produced digitally can be spotted easily, as they do not move exactly the same way with the head movement.

Even it holds the same truth for the artificial digitally produced beards on the male persons.

- **Unnatural Teeth**- Small jaw line and larger teeth, or vice versa. Even the same style or set of teeth in every person mouth during some live video conversation depicts the DeepFake.
- **Non-aligned body parts**- Some where the arms are shorter in proportion to rest of the body or legs, etc. Or sometimes the fingers of the hand are of different size/ color as compared to other parts of the body. It's a flaw.

DeepFakes Advantages

- **Research**- New digital personal avatars can be created in Entertainment or Training world. These created avatars can be used for styling hairs/ dresses-outfits/ etc in digital stores. Many large companies of the world introduced their product usage through AI based avatars during the pandemic times.
- **Professional Trainings**- Product based training is more easily demonstrated using digital avatars, rather than live people. Digital seminars, classroom learning sessions, car driving to aircraft flying all can be done through these digital avatars.
- **Theatre and Art Forms**- Many Digitally produced theaters plays or digitally produced movies like Ice-Man, Mougli, or other animated cartoon movies are easy to produce as the chance of re-takes gets drastically reduced. Only the change in script may automatically bring in the new action. Same for the spoken dialogs with special ascent, can be done in matter of minutes.

DeepFakes Disadvantages

- **Sockpuppets**- A DeepFake image creation of a non-existent person, who are found active both in online and traditional media is known as Sockpuppets.
- **Politics**- DeepFakes are extensively being used in maligning the political image of Politicians around the world.
- **Pornography**- The pioneer project of DeepFake was pornography, where many famous female actresses' likeness was used without their consent.
- **Blackmail**- A cryptocurrency mining hardware under the DeepFake technology is meticulously being used to generate fake blackmail emails in bulk, that falsely incriminate a victim.

DeepFake as in accordance with Indian IT Law

At present, India does not have any specific law for Deepfake cybercrime, but combination of various other laws can be done to deal with this Deepfakes. The following laws can be helpful in providing an instant relief to a cybercrime victim:

IT Act 2000:

- **Section 66D** depicts that when any communication device or computer resource is used (with) mala fide (intention) in order to cheat or impersonate any individual, then the culprit can get imprisonment of three years with the payment of fine up to Rs 1 lakh.
- **Section 66E.** This Section is violated by DeepFake, when an individual's privacy is breached under capture, publish or transmission of their personal images takes place in mass media. The culprit gets imprisonment of three years with the payment of fine up to Rs 2 lakh as a punishment.
- **The Copyright Act, 1957:** Under Section 51 of this Act, the use of any property that belongs to or owned by another person on which the latter person (the second party) has an exceptional right, violates the Law Act. However, the law permits some exceptions to this clause.

Report A Cyber Crime, Including Deep Fake

Call directly to the National Cyber Crime Helpline on 1930. Or report such a crime on https://cybercrime.gov.in

DeepFake Examples

Donald Trump deepfake

On 04 May 2016, Jimmy Fallon performed a Deepfake skit on NBC's The Tonight Show, where he dressed up as Donald Trump and further enacted in telephone conversation with Barack Obama, where he bragged about his own win in Indiana. Jimmy Fallon's face was transformed into Donald Trump but the audio track was kept intact. Derpfakes founder, uploaded this Deepfake video on YouTube with a comedic intent.

Barack Obama deepfake

On 17 April 2018, a DeepFake of Barack Obama abusing and calling names to Donald Trump was uploaded on YouTube. This DeepFake video was created and produced by American actor Jordan Peele, BuzzFeed and Monkeypaw Productions. The intent of this video was to highlight the massive malicious consequences and power of DeepFakes which can make anyone say anything.

Kim Jong-un deepfake

RepresentUs, a nonpartisan advocacy group created Deepfakes of North Korean leader Kim Jong-un.

Vladimir Putin deepfake

RepresentUs, a nonpartisan advocacy group created Deepfakes of Russian president Vladimir Putin. The DeepFakes of Kim Jong-un and Vladimir Putin were planned to be aired as commercials with an intention to interfere in the US Elections and further shock Americans to realize about their fragile democracy and also demonstrate the power of media news to influence the Country's path, irrespective of credibility! Well, these commercials were never aired due to sensitive reactions of Americans towards it!

Volodymyr Zelenskyy deepfake

On 16 March 2022, a tiny little deepfake videotape circulated on social media of Ukraine's President Volodymyr Zelenskyy supposedly influencing his Army men to lay down their arms and handover themselves to Russia forces during the 2022 Russian irruption of Ukraine. Russian social media boosted it, but Facebook and YouTube removed it, after it was debunked. Twitter allowed the videotape in tweets where it was exposed as a fake, but said it would be taken down if posted to deceive people. Hackers worked the intimation into a live scrolling- on Ukraine24-a television station as text news, and the brief videotape was presented on the station's website in addition to false claims that the President Zelenskyy has left Kyiv, the country's capital city. It was not instantly cleared that who created the deepfake, to which Zelenskyy responded with his own videotape, saying," We do not plan to lay down any arms. Until our victory."

Manoj Tiwari deepfake

An Indian Politician under the aegis of BJP party, used the DeepFake technology to deliver his old speech on "Citizen Amendment Act" to new fake speech on Delhi Elections. The content of the speech was doctored using AI Technology. The speech being in Hindi was dubbed and telecasted in Haryanvi Language pertaining to the electoral people of Haryana.

Conclusion

In order to create Zero Trust society, the progressive but harmful sabotage deep sabotage attack DeepFakes will cause high level of unrest and distress in the entire society. Zero Trust Society means, where the living people may not engage in bringing the real truth, but will may go with videos to understand the fake truth!

The usage of AI will help us distinguish the real bad actors and fake videos among the largest pool of DeepFakes.

References

Information about the DeepFake which is an independent and non-proprietary content on Wikipedia. https://en.wikipedia.org/wiki/Deepfake

Deepfakes session into the state of deepfakes and how the technology highlights an exciting but dangerous future. https://www.slideshare.net/JarrodOverson/deepfakes-how-they-work-and-what-it-means-for-the-future

Deep fake positive or negative? https://www.slideshare.net/KrushnaliTiwari/deep-fake-248066788?next_slideshow=248066788

The Guardian explains how AI-generated fake videos are becoming more common (and convincing). https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

The Businessinsider depicts everything you need to know about the AI-powered fake media. https://www.businessinsider.in/tech/how-to/what-is-a-deepfake-everything-you-need-to-know-about-the-ai-powered-fake-media/articleshow/80411144.cms

The GitHub repository for all DeepFake software. https://github.com/iperov/DeepFaceLab

What Is Deep Fake Cyber Crime? What Does Indian Law Say About It? https://www.outlookindia.com/business/what-is-a-deep-fake-cyber-crime-what-does-indian-law-say-about-it--news-196761

Deepfake Videos Of BJP's Manoj Tiwari Circulated During Delhi Polls https://www.outlookindia.com/website/story/india-news-deepfake-videos-of-bjps-manoj-tiwari-circulated-during-delhi-polls-report/347584?utm_source=related_story