Parichay Maharaja Surajmal Institute Journal of Applied Research

Deepfake Technology and Its Implementation

Tarunim Sharma[1], Vinita Tomar[2], Surbhi Pandey[3], Harshit Sharma[4]

ABSTRACT:

Lately, anew technological advancement made it hard to believe about the authenticity of the media we are seeing. This new technology is none other than Deepfake, an AI technique by virtue of which people are able to create hyper-realistic media having no originality. And the pace with which improvements are being done to increase its accuracy are rising the threats that can create havoc on society. Therefore, this paper will be providing a comprehensive understanding about deepfake, how this technology got its raise, different techniques of creating deepfake, how deepfakes are different from other technologies like CGI, photoshop and cheap fakes, latest and earlier deepfake detection models and techniques created by researchers, the crucial steps taken by different country govts., tech giants and startups to curb the falsehood spread by the means of deepfake, it also highlights fields one where deepfake technology is growing prosperously and other where it is using its malevolent tricks to harm the society. The result shows that the combined effort of every section of society is required to maintain the reliability in media and facts that we see and more improved detection techniques and tools are being researched upon to achieve this goal.

Keywords: deepfake, variational auto-encoder, CGI, cheap fakes, deepfake detection techniques, video authenticator tool, neural network

INTRODUCTION

In recent years a fascinating technology has emerged which also received huge attention all over the world. This technology is known as Deepfake that is used to manipulate images and videos using deep learning algorithms. It's a hyper-realistic technology through which one person's image can be superimposed onto other person's face, or we can put any words into anyone's mouth and can create an environment of falsehood or can make a person act in any video in which he/she may not have participated, or can also make a dead person alive or an older person look younger. The terms "deep learning" and "fake" together make Deepfake, describing the technology and the resulting forged content, whose first usage was seen on the Internet in late 2017, generated by an innovative deep learning method Generative Adversarial Networks (GANs).

In the past few years, world has experienced the taste of deep fake then it maybe through the video of David Beckham delivering an anti-malaria message in different languages for a health charity in the UK.[3] However, the most striking and menacing use cases are when people misuse the technology for heinous purposes such as when Donald Trump was being called a "complete dipshit" by Barack Obama, or Mark Zuckerberg boasted about having "total control of billions of people's stolen data", or Jon Snow making an apology for the dismal ending to Game of Thrones or when an Dessa company used the talk show host Joe Rogan's voice to utter sentences he had never said.[11]

Deep fake can be used for virtuous purposes but is hardly implemented. According to Deeptrace, the proportion of online deepfake content is increasing at a rapid rate. As per reports, during the starting of 2019 there were only 7,964 online deepfake videos, just nine months afterwards, that figure bounced to 14,678 videos.[4] Hany Farid, a UC Berkeley professor also made a statement for the surge in deepfake usage, "In January 2019, deep fakes were buggy and flickery, nine months later, I have never seen anything like how fast they are going. This is the tip of the iceberg."[1] The tally, made by a startup, for deepfake videos raised from 14,678 in 2019 to 145,277 by June of upcoming year.

The deep learning algorithms used for deep fake are indomitable and are improving at an astounding pace that an average human is unable to differentiate whether a video he is seeing is authentic or deep faked. Researchers around the globe are excited about the implications of deepfake in different fields and simultaneously are concerned about its misuse. The major field of deepfake usage is revenge pornography. As per Deeptrace delineation, September 2019, 96% of online deepfake videos were found to be related to pornography. Deepfake pornography has been non-consensual and involved the artificial synthesis of explicit videos featuring celebrities or any personal contacts. Danielle Citron, a professor at Boston University, also outlined that "Deepfake technology is being weaponized against women.".[2]

Originating from the dark corners of the web, deepfake technology is been taken forward by its application in the field of art, acting, internet meme, social media, sockpuppets and politics where the potential for mayhem is even greater. It is

[1,2] *Assistant Professor, Department of Computer Applications, Maharaja Surajmal Institute, Affiliated to Guru Gobind Singh Indraprastha University, New Delhi, India.*

[3,4] *Student, Department of Computer Applications,Maharaja Surajmal Institute, Janakpuri, New Delhi*

easy to imagine the harm that could happen if forged videos are rendered before the entire population that they believe to be true. Its doubtless that this technology constitutes high risk to politics with regard to fake media surfacing as real, but the more tangible threat is the idea of deepfakes making the real appear fake.[9]

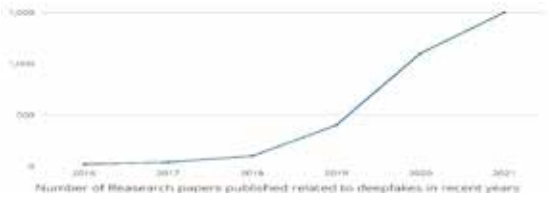

Figure 1: Image showing the rise in concern for deepfake and the significance to work for its solution.

Today we are at a state of inflection and require strong actions to protect our society from the unusual effects of deepfake. The perception of a world where seeing is no longer believing seems precarious. Therefore, a complete knowledge of such technology is required to know how it is created, what techniques are used in creation, what detections techniques are been developed to protect the society, digitally, from such hoax and what steps the government, public and giant tech companies are taking to restore the trust of people on real digital things and what is the future scope of this technology.

THE CREATION OF DEEPFAKE / HOW IT IS CREATED

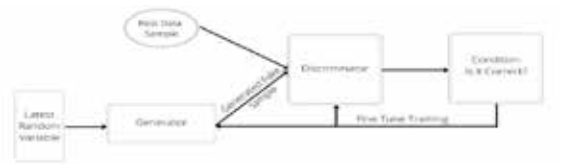

Figure 2: Image showing the GAN technique used in creating deepfake.

Deepfake technology was developed by researchers at academic institution in the beginning of 1990s.However, its usage began in the year 2017 with the rise of deep learning technique which made the creation of high precision deepfake videos simple. Nowadays, most of the deepfakes are produced using deep learning that uses general Generative Adversarial Networks (GANs) a class of neural networks which is used for unsupervised learning. GANs are mainly comprised of a system of two neural network models that contend against one other and analyze, capture and copy the variations within a dataset.

When creating deepfake these two neural networks of GAN are set to confront one another in order to produce an output that looks as real as possible. The two networks are, generally, known as generator and discriminator. The generator, generates a deepfake image using the given dataset and tries to deceive the discriminator. On the other hand, the discriminator scrutinizes the generated image to classify it as real or fake. During the whole process generator tries to mislead discriminator and repeatedly generate forge images until they are specified as authentic by the discriminator.

Another technique used for the creation of deepfake videos is Variational Auto-Encoder [VAE] which also uses deep learning networks. In this technique, VAEs are trained to encode images into low-dimensional representations and then decode those representations back into images. The images of faces used for both training sets can be sorted by applying a facial recognition algorithm to a dataset of videos to capture different poses and lighting conditions that naturally occur. Afterwards, the encoder which is trained on many different faces is combined with the decoder that is trained with the face one want in a particular video which generates the deepfake. Generating deepfakes using this technique is comparatively easier than GAN but the deepfake generated using VAEs are not as realistic as those generated using GAN.[20]

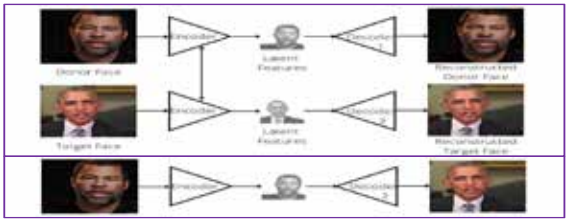

Figure 3: Image showing the VAE technique of creating deepfake.

HOW DEEPFAKE IS DIFFERENT FROM OTHER TECHNOLOGIES:

A) DEEPFAKE AND CGI

The advances in the audiovisual sector have compelled to inspect the false elements created by computer, replacement of faces or even rejuvenating actors to make them look younger, creating a dead or non-living thing alive. And nowadays, the most talked techniques in this domain are: CGI and deepfakes.

The CGI technique, also known as computer generated images are used in entertainment industry like movies, advertisements or video games, etc. It is used to recreate scenes that would rather have been expensive or say impossible to create in real life than to generate them through advanced computing techniques. At extreme levels, scenes that if it wasn't the CGI then it would have been impossible to achieve them, such as a deceased artist giving their special appearance in movies. Example includes movies like Avatar, Avengers, Titanic and many more.

Figure 4: Image showing CGI used in the movie "Pirates of the Caribbean".

Figure 5: Image showing the use of Deepfake to swap one person's face with another person.

On the other side the Deepfake technique is generated by AI computing like deep learning and facial recognition, often used in entertainment mainly to supersede faces, rejuvenate them or age them in an ultra-realistic way. It is created by computer and requires data of two real sources. It is formed such that the features of a model "A" are analyzed to replace the face with that of another model "B", whose face has been selected for substitution. Sometimes, special effects (also known as vfx) are also used to banish the excess. There are many deepfake examples, such as deepfake roundtable featuring Tom Cruise, George Lucas, Ewan McGregor and more.[7]

B) DEEPFAKE AND PHOTOSHOP

Both deepfakes and photoshopped images frame synthetic media based on a source. Though, the consequences of deepfakes are more alarming, as their production and utilization involved an element of performance.

Deepfakes are created after a thorough analysis of large hoard of data. Today's deepfake creating softwares are far from Photoshop's simplicity and accuracy. Applications like, Snapchat uses AI methods to apply filters to individuals' faces but it does not come under the category of deepfakes. Reason being that, deepfakes are those which have potentiality to trick others, and perhaps meaningfully affect their lives. They are new, but are also easy to create. The dangerous part of the technology is that, unlike older media editing techniques, it is easily comprehensible to people with no technical skill. If there are ample number of images or videos of an occasion then it would be relatively easy to produce credible manipulations effortlessly using AI.

While photoshop is used to modify pictures of real people by creating synthetic pixels to enhance a given image. A degree of similarity is there with deepfake because of its ability to change the

Figure 6: Image showing a picture being modified using photoshop

Figure 7: Image showing an actor video de-aged using deepfake technique.

expression of person's face, but the quality of these alterations is less sophisticated. Referring to slight changes such as forging a person to uphold to some beauty perfection, but significant changes with entertainment intentions are ample. To photoshop an image or video it requires softwares and tools, not any AI technology. And it is therefore, much complicated or say impossible to manipulate individual images with photoshop when thousands of original images exist.

C) DEEPFAKES AND CHEAPFAKES

Many terms are prevalent similar to deepfake like cheap fakes, shallow fakes. Cheap fakes are sometimes interchange for shallow fakes that are audiovisual (AV) artifices created with low price softwares easily available as compared to deepfakes tools. They are produced through Photoshop, lookalikes, re-contextualizing footage, speeding, or slowing videos. The videos created does not use any deep learning or machine learning methods but are confined to straightforward techniques present on video editing softwares.

Both Deepfakes and cheap fakes vary in technical sophistication and application. A highly realistic and refined deepfake, will be purge of any flaws and indistinguishable from a genuine video by an algorithm.

DEEPFAKE DETECTION TECHNIQUES

The creation of deepfake detection technique is very crucial to end the falsehood that is being spread as it does affect the belief system of society. As deepfake generation techniques are upgrading day by day analogous to them deepfake detection techniques are also being advanced to leave no stone unturned. Hence researchers are continuously working in finding an impeccable detection technique to track down even the most realistic deepfake. Keeping this in mind researches for detection techniques have been made and are still ongoing.

The following table list some of these techniques.

Table 1: Deepfake detection techniques.

Researchers	Proposed Model/ Technique	Results	Limitations	Future Scope
i. Luca Guarnera, Oliver Giudice, Sebastiano Battiato[17]	**i.** Detecting forensics trace hidden in images: a sort of fingerprint left in the image generation process. **ii.** Using Expectation Maximization (EM) algorithm, and extracting set of local features specifically addressed to model the underlying convolutional generative process.	**i.** Tests with VGG-1614 achieved the best result of 53% of accuracy in the binary classification task. **ii.** Fingerprint proven effective in discriminating between images generated by recent GANs architectures used to generate realistic people's face.	A deep learning approach is not able to extract what the proposed approach was able to.	**i.** To investigate the role of the kernel dimensions. **ii.** To adapt the method in situations on the "wild" without any a priori knowledge of the generation process.
ii. Shruti Agarwal, Hany Farid, Ohad Fried, Maneesh Agrawala[18]	**i.** Detecting the dynamics of the mouth shape visemes that are occasionally inconsistent with a spoken phoneme. **ii.** Focused on the visemes associated with words having the sound M (mama), B (baba), or P (papa) in which the mouth must be completely close to pronounce these phonemes.	**i.** Method can detect state-of-the-art, lip-sync deep fakes. **ii.** For high-stakes cases, showing that an analyst can manually verify video authenticity. **iii.** For large scale cases, showing the efficacy of two automatic approaches: one using hand-crafted features that requires no large training data, and one using a CNN.	**i.** Extension of mbp phonemes is not trivial and will require modeling the possible variance of each viseme and co-articulation. **ii.** Gathering a large labelled dataset of mouth almost closed or open, with a few pixels difference is challenging.	**i.** To develop unsupervised methods to automatically differentiate between complete and almost complete mouth closure. **ii.** To obtain better results using a trained network on a large corpus of people.
iii. Tianxiang Chen, Avrosh Kumar, Parav Nagarsheth, Ganesh Sivaraman, Elie Khoury[19]	A robust end-to-end deep learning framework for voice spoofing(audio deepfake) detection, detecting spoofed audio generated from a wide variety of unknown TTS and VC systems with high accuracy.	**i.** Increase in generalization ability by adding Freq Augment layer and large-margin cosine loss and applying data augmentation **ii.** EER of 1.26% on ASVspoof 2019 evaluation set, a remarkable improvement over the state-of-the-art.	**i.** Investigation not done for different low level audio features **ii.** Only two known techniques are present in the evaluation set.	Data augmentation is an important approach towards better generalization.
iv. Rene Amerini, Leonardo Galteri, Roberto Caldelli, Alberto Del Bimbo[21]	**i.** A sequence-based approach dedicated to investigate possible dissimilarities in the temporal structure of a video. **ii.** Extraction of optical flow fields to exploit inter-frame correlations to be used as input of CNN classifiers.	**i.** Results achieved on FaceForensics++ dataset are very promising. **ii.** This feature is able to point out some existing dishomogeneities between the two analyzed cases.	None	To evaluate the reliability of optical flow fields for deepfake video identification by testing against more datasets and with other neural networks
v. David Guera Edward J. Delp[22]	**i.** A temporal-aware pipeline to automatically detect deepfake videos. **ii.** System using a convolutional neural network (CNN) to extract frame-level features to train a recurrent neural network (RNN) that identify if video is manipulated.	Using a simple convolutional LSTM structure, and making accurate prediction whether a video is manipulated or not in less than 2 seconds.	None	To search, how to create more robust system for fabricated videos using unseen techniques during training.

vi. Yuezun Li, Siwei Lyu[23]	Detecting distinct artifacts due to the resolution inconsistency between warped face area and surrounding context artifacts by comparing the generated face areas and their surrounding regions with a dedicated Convolutional Neural Network (CNN) model.	**i.** Invideo-based evaluation metric, ResNet network still performs ~ 15% better than VGG16. **ii.** The CNN model is effective in detecting the existence of such artifacts.	Predesigned network structure is currently being for this task (e.g., resnet or VGG)	**i.** To evaluate and improve the robustness of detection method with regards to multiple video compression. **ii.** To explore dedicated network structure for the detection of DeepFake videos
vii. Ping Liu, Yuewei Lin, Yang He, Yunchao Wei, Liangli Zhen, Joey Tianyi Zhou, Rick Siow Mong Goh, Jingen Liu[24]	**i.** To apply automated machine learning to search neural architectures for deepfake detection. **ii.** Predicting the real or fake label for each given sample and also locating the potential manipulation region with few dependences on prior knowledge.	**i.** (ADD)Method outperforms previous non-deep learning methods (Steg+SVM [45] and Cozzolino [82]) by a large margin (10% ~ 20%). **ii.** Locating the potential manipulation regions in a efficient manner with few dependence on prior knowledge.	**i.** Potential manipulation region learning strategy will not work well if the fake image is entirely synthetic. **ii.** Method suffers when encountering low-quality images.	To research highly advanced search methods and spaces to improve the prediction ability of model.
viii. Xurong Li, Kun Yu, Shouling Ji, Yan Wang, Chunming Wu, Hui Xue[25]	**i.** A novel Patch&Pair Convolutional Neural Networks (PPCNN) to distinguish Deepfake videos or images from real ones. **ii.** Constructed a two-branch learning framework.	**i.** The AUC score of models are higher than previous methods except on Mesonet-data with same origin dataset. **ii.** PPCNN significantly outperforms previous detection methods on the YouTube dataset.	For Mesonet-data, only the patch-based CNN branch is used to classify the fake images.	To combine with forensic technologies, to detect complex deepfakes with different compression levels and resolutions.

Generalization of all the developed deepfake detection techniques is necessary in order to identify all ranges of deepfake whether low or high quality. However, some detection techniques seem inefficient at this point and can only detect deepfake for a particular type of dataset. Sometimes, the deepfake generation techniques becomes so advanced that the present detection techniques are no longer able to serve the purpose. That is why researchers keep developing creative techniques with innovative approaches. Some of the latest deepfake detection techniques are described below.

- Recurrent convolutional models – The recurrent convolution model is a class of deep learning that uses recurrent neural network which is used for visual object recognization. Using this technique, a lot of tools have been made by various organizations that can be used to detect deepfakes but it's not as prominent as Microsoft's video authenticator.
- Biological Signal Analysis – This technique of deepfake detection is presented by Yuezen Li. This technique detects facial movements like eye blinking etc using different deep learning models like convolutional neural network (CNN) and recursive neural network (RNN) to detect if the media is modified.
- **Steps Taken by Different Countries Government and Tools Made by Tech Giants and Startups to Regulate the Use of Deepfake**

For the present, there is no ambiguity in stating that rather using deepfake technology in a healthy way it is being proving noxious for people. Evil-doers are using it as a weapon mainly against women, political leaders, celebrities for blackmailing, demolishing one's life, defaming and satirizing them. The belief system of people, i.e., seeing is believing, is tried to be pulled down in a digital age where everyone is connected through technology and spreading hatred for other person, misinformation about an issue is a very critical problem. However, it would not be erroneous to remark that using deepfake technology in a positive manner will be beneficial for the people itself. For instance, it can be used in the field of education to teach historical figures, art to present a deceased actor or creating digital voices of people who lost their voices due to some reason, and for public awareness. This implies that deepfake cannot not be banned entirely but need to regulate its use. Hence, measures and tools are required to be framed by countries governing authorities and tech companies to save its people from deepfake disservice.[14]

- **Steps Taken by Different Countries Government**

In the United States, law has been passed making it illegal to disseminate false content about any political leader before elections with an intend to deceive voters or defame leaders. To simplify the complaint process for individuals seen in pornographic deepfake a private right of action law for individuals was introduced. Some Acts like IOGAN

and NDAA are helping other institutions to work jointly in research of deepfake standards, its detection and generation techniques, and ways to find solution for them.

India has no such explicit laws for deepfake as it rarely has been affected or has seen cases related to deepfake. However, the IT Act outlines punishment for publication of sexual and explicit content involving adults and children which is also applicable to deepfake pornographic content. So, there is no direct law to regulate deepfake but there is a need to have few as once deepfake make its root in India it could have catastrophic effects at a higher rate.[5]

China is also combating this widespread technology by creating laws stating that every app providers label deepfake content and other online platforms to identify and remove any other unlabeled content immediately. Cyberspace Administration of China (CAC) is responsible for regulating all these laws and to take any action done in opposition to that as a crime. Under China's new regulation, to be abide from March 1 2022, all the social platforms are prohibited from recommending any kind of synthetic content on their platform, i.e., it is the responsibility of the companies to detect and eliminate false content.[10]

European Union is also taking initiatives by making laws to manage with this deepfake technology by protecting privacy to people's data, making copyright laws and labeling deepfake content. Apart from this there are still many countries having no specific laws to curb this technology.[6]

- **Steps Taken by Tech Giants**

In September, 2020, Microsoft launched a Video Authenticator Tool which analyses the stock-still images, videos and provides a confidence score or, say, percentage chance and identifies the media as manipulated or genuine. When analyzing video, the tool provides percentage for each frame of the video in real time. The concept behind the tool is that it detects the blending boundary of the deepfake and subtle fading or greyscale elements that might not be detectable by the human eye. The training of tool was done on the public dataset, Face Forensic++, and was tested on Deepfake Detection Challenge Dataset.

Microsoft also introduced a new technology that detect any manipulated content and also assures the public of the authenticity of the media being viewed. The technology has been divided into two components, one is built into Microsoft Azure enabling content creator to add digital hashes and certificates to content and the other checks these certificates and matches hashes and tell about its authenticity and accuracy.[15]

Ahead of U.S. 2020 elections, Twitter announced new policy regarding deepfakes, synthetic and doctored media. According to it the users will be prohibited from sharing any kind of manipulated or synthetic media or content that is likely to cause harm. Such content will be tested on a specified criteria and if meets all those criteria then it will be removed from platform. Content that fulfill fewer criteria will be labeled as altered and will provide users with more context before reposting.

Facebook also framed policy to remove deepfakes and any edited content, but not any parody or satire, aimed with spreading misinformation. It also launched, in September 2019, along with other leading partners a global Deepfake Detection Challenge to ensure the development of detection tools. They created a highly realistic deepfake dataset of a varied group of artists and was made accessible to all the participants involved in developing deepfake detection models.[8]

- **Startups Tackling Deepfake**

Apart from Tech giants' startups are also finding solutions for the rising problems of deepfake and forgery. Implying that startups too are conscious and capable of developing tools with high performance and such technical minded startups have been discussed below.[16]

OARA, a spanish startup developed a tool which is assisting governing bodies, individuals and businesses in authenticating and verifying digital identity and media. It also generates photos and videos by embedding user identity, timestamp, GPS coordinates to ensure its realiability.

Senitel, a startup from Estonia, created a detection model following Defense in Depth approach. The model consists of a large dataset of deepfake and neural network classifiers that checks for the genuineness of media and identifies which is doctored one.

The, Dutch startup, Sensity provided a visual threat intelligence platform and an application programming interface (API) for identifying and countering deepfake. It browses over hundreds of sources across dark and open web to gather visual threat intelligence and then uses it to detect harmful visual media with its associated risks. Its AI detectors are also able to identify synthetic and AI based manipulation techniques.

Swiss startup Quantum Integrity deep learning technology has customizable algorithms and detects image and video deepfake, for instance, false accident reporting, fake documents, etc. It provides companies with various advantages such as time saving, reduced forgery, fast and accurate decision making.

Indian startup, Group Cyber ID, has also taken a move to ensure authentic and secure data in organisations. It provides digital forensic based solutions for digital components. It also created a multi-layer security strategy of technologies and procedure in cyber defense and digital forensics. It authenticates digital infrastructure and finds the risks in internal and external data of organisation and also secures network, devices from attacks.

- **Implementation of Deepfake in various fields**

Since so far, we have seen that deepfake is mostly used with a malicious intent rather using it for a good cause. This can be because, we, the people has not explored the technology to its full length and has not seen the bright side where it is been utilized for a better future without harming anyone's feeling. This is the case with each and every new technology that it gets started been utilized at its early stage and without prior knowledge which further leads to rising concerns over

it. Hence, we will explore all the fields where deepfake can be used and will categorize it as positive and negative based on the effects it has on public.[12]

- Education – Deepfake has positive potential to be used in education and can revolutionize the way the subjects are taught. For instance, history subject with long theory can be taught with interactivity using deepfake. It can be used for creating deepfakes of history figures which can help in visualizing the era or situations of the past. And as we know learning by visuals is stored in our memory for a longer time then reading it from book, so it will have positive impact on public and will also change the way deepfake technology is being seen leading to the generation of more innovative ideas for the usage of this technology. For example, CereProc, a company that resuscitate JFK's voice. The deepfake created made it possible to hear the late president's speech he would have delivered, if were alive.
- Terminating language barriers –Deepfake possess the power of replicating people's voices and creating a new video with them. It might be possible with deepfake to use actor's original voice in a translated version of a movie. When using deepfake for translation in different language lip syncing can be done smoothly. If, used, it might end or reduce language barriers and will help in sharing of thoughts across a large group of people. This can lead to a crucial step towards united humankind. For instance, the video of actor David Beckham who used the technology for spreading awareness about malaria in nine different languages for the campaign Malaria Must Die.
- Entertainment – A vast field for deepfake where it can be used in different innovative ideas and will also help film or video creators in saving cost and time. It might also help in recreating a memory for a deceased actor or actress if one has their visual dataset comprising of their facial expression, voice, physical behavior. It may also be used for aging and de-aging of actors.

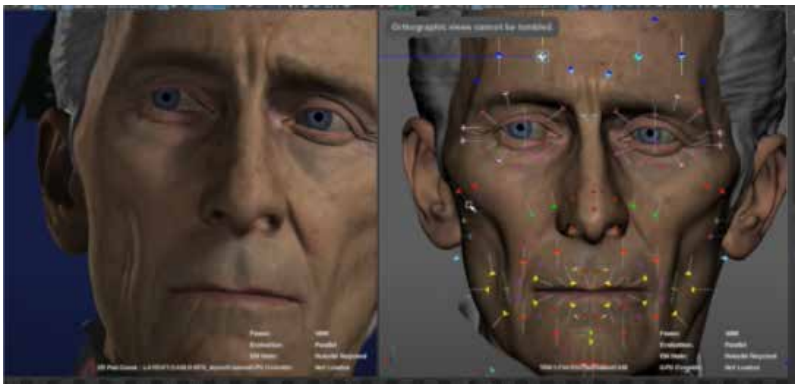

Figure 8: Image showing an actor face being recreated using deepfake.

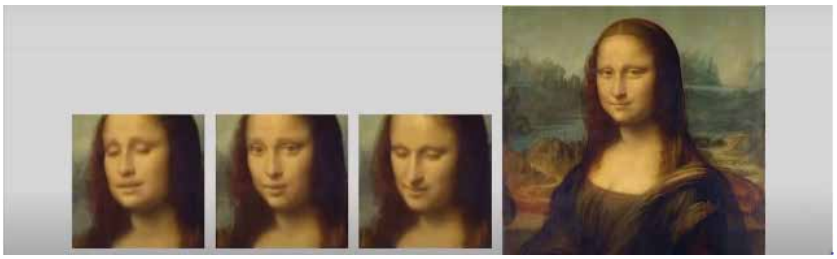

Figure 9: Image showing Mona Lisa moving her head and lips made by Samsung's AI using deepfake.

Art – Deepfakes have been seen making their place in art world also. Dalí Museum in St. Petersburg created an exhibition called Dalí lives, using deepfakes for visitors to interact and take a selfie with surrealist painter Salvador Dalí. Hence, it can be used for creating virtual museums enabling people to have access to the famous masterpieces, and realistic deepfake artwork. Samsung's AI research brought such art to life by making Mona Lisa to act with her head, mouth and eyes.

Medicine – Deepfakes might prove the most beneficial in healthcare sector. By advancing the technology, hospitals might be able create true-to-life deepfake patients for testing and experimenting saving a real patient life from risk. This creates an opportunity to test new diagnosis practices and training other AI with medical decision making.

Training – AI based models requires large datasets to train them and colleting such a huge dataset is still complex and time consuming. If used wisely we can create pure synthetic but useful datasets for training purposes and will relieve people from their data privacy concerns. It can be used in fashion designing to train models and designers by visualizing their design, customer service training by creating synthetic voices of people asking for services.

Corporate Level Fraud – Deepfake wrong utilization is leaving people concerned and stressed. A new way to do corporate level monetary fraud is by making calls to transfer

money in CEO voice. Such cases are been registered and a few companies have also seen losses of millions.[13]

Extorting Money from Businesses or Individuals – AI doctored videos, images and voices are being used to blackmail people for money by threatening to send the video to press agencies or posting it on internet.

Fake News and Videos – Fake news are being used to raise violence, confusion, division and doubt among people in nations. Fake videos are also been shared to gain wide coverage over that topic. Revenge pornography is one of the crucial examples of deepfake videos. Public is been misled by sharing misinformation and people in fake news and videos are been defamed. Such forgery things do affect the lives of people and their decision making.

CONCLUSION

Deepfake technology will keep advancing and evil-doers will continue to spread misinformation in every way possible. This is our responsibility to manage these deepfakes so as not to let the trust fade away that we have on things we see. It is the responsibility of governing bodies to make their citizen aware of deepfake technology and tech companies to manage all the deepfakes that are present on their platforms and that can have harmful impacts. Lastly the public should be aware and should stop reposting malicious deepfakes. The researchers are working hard to find an appropriate deepfake detection technique and will surely succeed in their goal and we have to support them by wisely using deepfake technology.

REFERENCES

[1]. Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared, https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/?sh=29ad4c627494

[2]. Artificial intelligence, deepfakes, and the uncertain future of truth, https://www.brookings.edu/blog/techtank/2019/02/14/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/

[3]. The biggest threat of deepfakes isn't the deepfakes themselves, 2019, https:// www.technologyreview.com/2019/10/10/132667/the-biggest-threat-of-deepfakes-isnt-the-deepfakes-themselves/

[4]. How to tell reality from a deepfake? , 2021, https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-deepfakes/

[5]. Deepfakes in India: Regulation and Privacy, 2020, https://blogs.lse.ac.uk/southasia/2020/05/21/deepfakes-in-india-regulation-and-privacy/

[6]. Tackling deepfakes in European policy, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[7]. CGI and Deepfake: How They Work and How to Do Them with Your Mobile, https://itigic.com/cgi-and-deepfake-how-they-work-with-your-mobile/

[8]. Deepfake, https://en.wikipedia.org/wiki/Deepfake

[9]. The Emergence of Deepfake Technology: A Review, 2019, https://timreview.ca/article/1282

[10]. China steps up efforts to ban deepfakes. Will it work? , https://restofworld.org/2022/china-steps-up-efforts-to-ban-deepfakes/

[11]. What are deepfakes – and how can you spot them? , https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

[12]. Yes, positive deepfake examples exist, https://www.thinkautomation.com/bots-and-ai/yes-positive-deepfake-examples-exist/

[13]. Living in A Deepfake World, https://amt-lab.org/blog/2021/10/living-in-a-deepfake-world

[14]. Why we need a better definition of 'deepfake', https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news

[15]. New Steps to Combat Disinformation, https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/

[16]. Discover 5 Top Startups Tackling Deepfakes, https://www.startus-insights.com/innovators-guide/5-top-startups-tackling-deepfakes/

[17]. Deepfake detection by analyzing convolutional traces, 2020, https://openaccess.thecvf.com/content_CVPRW_2020/papers/w39/Guarnera_DeepFake_Detection_by_Analyzing_Convolutional_Traces_CVPRW_2020_paper.pdf

[18]. Detecting Deep-Fake Videos from Phoneme-Viseme Mismatches, 2020, https://openaccess.thecvf.com/content_CVPRW_2020/papers/w39/Agarwal_Detecting_Deep-Fake_Videos_From_Phoneme-Viseme_Mismatches_CVPRW_2020_paper.pdf

[19]. Generalization of Audio Deepfake Detection, 2020, https://www.isca-speech.org/archive_v0/Odyssey_2020/pdfs/29.pdf

[20]. Deep Learning for Deepfakes Creation and Detection, https://www.researchgate.net/publication/336058980_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey#pf9

[21]. Deepfake Video Detection through Optical Flow based CNN, https://openaccess.thecvf.com/content_ICCVW_2019/papers/HBU/Amerini_Deepfake_Video_Detection_through_Optical_Flow_Based_CNN_ICCVW_2019_paper.pdf

[22]. Deepfake Video Detection Using Recurrent Neural Networks, https://engineering.purdue.edu/~dgueraco/content/deepfake.pdf

[23]. Exposing DeepFake Videos By Detecting Face Warping Artifacts, https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Li_Exposing_DeepFake_Videos_By_Detecting_Face_Warping_Artifacts_CVPRW_2019_paper.pdf

[24]. Automated Deepfake Detection, 2021, https://arxiv.org/pdf/2106.10705.pdf

[25]. Fighting Against Deepfake: Patch&Pair Convolutional Neural Networks (PPCNN), 2019, https://www.researchgate.net/publication/341128950_Fighting_Against_Deepfake_PatchPair_Convolutional_Neural_Networks_PPCNN