Artificial Intelligence for Deepfake Creation and Detection

Dr. Padmapani P. Tribhuvan

Assistant Professor, Department of Computer Science and Engineering

Deogiri Institute of Engineering and Management Studies, Aurangabad (MH), India

padmapanitribhuvan@dietms.org

Amrapali P. Tribhuvan

Research Scholar, Department of Computer Science and IT

Dr. Babasaheb Ambedkar Marathwada University,

Aurangabad (MH), India

amrapaliprakash512@gmail.com

**ABSTRACT**

Advances in artificial intelligence have led to the emergence of deep fake technologies. A deep fake that can manipulate images, sounds, and video content to represent an event that did not happen. This paper provides an overview of deepfake, benefits of deepfake technology with deepfake examples and deepfake challenges. the paper will explore AI based deepfake creation and detection apps and website.

Keywords—Deepfake, Artificial Intelligence, Deepfake creation, Deepfake Detection

1. **INTRODUCTION**

Deepfakes are videos or images that have been altered by artificial intelligence to look different from their original form. The first development of this technology met the requirements for creating synthetic videos in the entertainment industry. In animated films and influential science fiction films, depth-faking can produce realistic results. As further developments are made in this field, applications are developed that allow people to use this face-swapping feature for humorous purposes. Such applications were available to everyone and did not give very authentic results. The same technology combined with deep learning has proven to be a huge success. With the help of artificial intelligence, deep fakes are the most realistic captured images and videos.

Big tech companies like Facebook and Google have recruited researchers through competitions to help detect deep fakes and build massive data for them. Google worked with paying and consenting operators to capture hundreds of videos over the course of a year to create a massive data set and create thousands of deep fakes. This kind of videos that use open-source methods to create deep fakes. With limited problems and simple devices like smartphones, many new devices online have made it easier than ever to create practical "deep fake" texts. Recent advances in the development of deep falsification algorithms that produce distorted information have negatively affected anonymity, security, and mass communication. Every day technical people work with new technologies. Artificial intelligence is becoming so powerful that every industry uses it in some way. Deep-fake images can also be harmful to facial recognition systems, as they interpret and manipulate a person's facial expressions based on someone else's image. Since their debut in late 2017, many open-source deep parody generation strategies have emerged, resulting in a growing number of synthesized media.

Deepfakes is a new emerging technology that develops convincing images and videos created by artificial intelligence. For example, a video where the face of a real person is changed to someone else, giving the impression that the original person is doing and saying fictitious things. Such fake videos can be used to compromise a person's identity. Deepfake videos are now so popular that several political parties are using the tool to create fake images of the leader of the opposing party to incite hatred against them. Fake political videos that say or do things that never happened threaten election campaigns. These images are a major source of fake media controversies and spread misleading news. To reveal the fake in an extremely detailed way, such details are examined frame by frame in the production of a deep fake image.

1. **Benefits of Deepfake Technology**

Deepfake technology also has positive uses in many industries, including film, educational media and digital communication, gaming and entertainment, social media and healthcare, material science and various business areas such as fashion and online shopping.

The film industry can benefit from deep rigging technology in several ways. For example, it can help make digital voices for actors who have lost their voice due to illness, or update a film frame instead of re-filming it. Filmmakers can recreate classic scenes in movies, create new movies with long-dead actors, use special effects and advanced facial processing in post-production and enhance amateur videos in professional quality. Deepfake technology also enables automatic and realistic audio dubbing in any language for movies, which allows different audiences to better enjoy movies and educational media.

Global 2019 Malaria Awareness Campaign Featuring David Beckham Breaks Language Barriers with Educational Ads Using Visual and Audio Transformation Technology to make him appear multilingual. Similarly, deepfake technology can break the language barrier in video conference calls by translating speech while changing facial and mouth movements to improve eye contact and make it appear that everyone is speaking the same language.

In an ad campaign for chocolate maker Cadbury, Indian film superstar Shah Rukh Khan wishes everyone a Happy Diwali while naming thousands of small businesses. This was made possible by creating a fake version of Khan that seamlessly adds the names of small businesses across the country chosen by Indian residents, allowing each business to create their own personalized version of the ad that they can then share online. For this machine learning used to recreate Shahrukh khan’s face and voice.

Deep fakes and AI-generated characters can be educational. During the Shanghai lockdown, associate professor Jiang Fei noticed her students' attention spans dwindled during online classes. To help them focus better, he used an anime version of himself to teach. Jiang Fei said, "Students' enthusiasm in class and improvement in the quality of homework have made clear progress."

**B. Deepfake Challenges**

Deepfakes affect the world because people around the world use deepfakes for various reasons, including changing faces, creating pornographic videos of someone's face or body, and creating and spreading fake news. Deep fakes increasingly affect democracy, privacy, security, religion and human cultures. The number of deep fakes increases from time to time, but there is no standard for evaluating deep fake detection techniques. The number of deepfake videos and photos found online has almost doubled since 2018. The Massachusetts Institute of Technology (MIT) analysed 126,000 news stories shared by 3,000,000 users over 10 years. Finally, they concluded that fake news spreads 1500 people 6 times faster than real news.

Deepfake creates fake news, images, videos, and terrorist events. Deepfake undermines people's trust in the media and leads to social and financial fraud. Deepfake influences religions, organizations, politicians, artists, and voters. With the proliferation of fake videos and photos on social media, people ignore to believe the truth. The authors analysed profound fakes that can harm individuals and societies.

The use of deep fakes to harm others is still widely seen, including pranks to embarrass a co-worker, identity theft or even incitement to violence, porn videos to satisfy someone, etc. Deepfakes are also used to fake terrorist events, blackmail, defame individuals and create political anxiety. While no one is immune to deep fakes, some people are more vulnerable than others. With minimal data and computing power, someone can create a video of a country's leader saying something that leads to civil conflict.

Deep fakes have a negative impact on the target, increase fake news and hate speech, create political tension, harass the public or start a war. For example, a person can manipulate the content of a video and the people in the video to spread fake news that could lead to war between nations; especially a country with various peoples and nationalities. Deep fakes are on the rise and social media is quickly spreading these deep fake photos and videos.

1. **DEEPFAKE CREATION APPS AND WEBSITES**

Over the years, the use of the best deep fake apps has grown tremendously. We live in a time where it is not easy to believe what you see on the Internet. Real videos and photos make it even harder to tell the truth from a fake. The technology used to create such fraudulent videos and images is readily available and is known as deepfake apps.

1. **Lensa AI**

Lensa AI is the latest app that has become popular for creating AI portraits of yourself or someone else. It's not exactly a deep fake in the sense of putting your face on other people's bodies or videos. However, Lensa's AI has the insane ability to create its own photorealistic portraits from a few selfies. Additionally, the program creates portraits in a variety of styles, including superheroes, anime, and more.

1. **Deepfake Web**

Deepfake Web is a service that allows you to create Deepfake videos online. It uses deep learning to absorb the complexity of facial data. Deepfakes Web can take up to hours to learn and practice based on video and images, while swapping faces with a trained model takes another 30 minutes. The free version sends a deep fake video in about five hours, while the premium version spits out a video in just an hour.

1. **Reface**

The Dublicate developers renamed the Reface app to Reface after Reface AI. Reface AI is a generative adversarial network (GAN) behind the scenes. All you have to do to use the app is take your photo and then select the GIF you want to use. After a few seconds, the app will add a GIF of your face. It doesn't work perfectly, and face overlap depends on the symmetry of your face and the GIF you're using. But there are so many gifs on the internet that you always have a choice. This can be your personal GIF app to impress your friends.

1. **Myheritage Deepfake App**

The app's Deep Nostalgia feature has gained popularity among social media users as it allows you to animate old photos. To use the service, you just need to upload a picture and press the animation button. In a few seconds, you'll have an animated version of the image with the face, eyes and mouth moving as if straight out of Harry Potter's The Daily Prophet.

1. **DeepFackLab**

DeepFaceLab is a Windows program that allows you to create deep face fake videos. It is primarily intended for computer vision researchers and students. However, if you want to learn about deepfaking videos, you can definitely try this tool. It uses machine learning and human image synthesis to replace faces in videos.

1. **FaceMagic**

Another AI-based face-swapping app is FaceMagic. FaceMagic allows you to use faces of your choice in videos and photos. The app's in-app feed offers face swap invitations, but you also have the option to use your own photos and images as the main face swap theme.

1. **FaceApp deepfake App**

FaceApp is a popular app and is actually one of the first apps that really popularized and democratized deep fakes and AI-generated face manipulation on smartphones. With FaceApp, you can simply upload your photo to the app and see what you look like in your old age, smile and much more. As mentioned above, the program uses artificial intelligence to edit images to make them look quite realistic.

1. **Avatarify**

An AI facial animator that uses facial cues and then adds them to images. Avatarify has large collection to boot. It ranges from classic sound effects to more complex head movements synchronized to international and even regional tunes. You can even use different memes for deep fake effects.

1. **DeepBrain**

DeepBrain is a deepfake software that stands out for its ability to create highly authentic and visually stunning fake videos. Using advanced AI techniques, DeepBrain has become a popular choice for users who want to create authentic deep-fake video content with professional quality. It also has an effortless and reliable face change feature. DeepBrain offers an intuitive interface that allows both beginners and experienced users to explore its countless features to create amazing fake videos.

1. **AI BASED DEEPFAKE DETECTION TOOLS AND TECHNIQUES:**
2. **Sentiel**

Sentinel is a leading AI-based security platform that helps democratic governments, Defence agencies and enterprises stop the threat of deep counterfeiting. Sentinel technology is used by leading organizations in Europe. The system works by allowing users to upload digital media through their website or API, which is then automatically analysed for AI fakes. It uses advanced artificial intelligence algorithms to analysed the system determines whether the media is a deep fake or not and shows the visualization of the manipulation.

1. **FakeCatcher**

Intel launched a real-time deep fake detector called FakeCatcher. This technology detects fake videos with 96° accuracy and returns results in milliseconds. The detector uses Intel hardware and software that runs on a server and connects via a web-based platform. FakeCatcher looks for real clues in real videos and appreciates what makes us human - the subtle "blood flow" in video pixels.

1. **WeVerify**

WeVerify is a project that aims to develop intelligent methods and tools for in-the-loop content verification and disinformation analysis. The project focuses on analyzing and contextualizing social media and web content within the wider internet ecosystem to discover the content produced. This is achieved through multifaceted content verification, social network analysis, micro-targeted exposure and a blockchain-based public database of known fakes.

1. **Microsoft's Video Authenticator tool**

Microsoft's Video Authenticator tool is a powerful tool that can analysed an image or video and provide a trust score that indicates whether the media has been tampered with. It detects the blend boundary of deep fakes and subtle grayscale elements that cannot be detected by the human eye. It also provides this reliability in real time, enabling immediate detection of deep fakes. This Video Authenticator Tool uses advanced artificial intelligence algorithms to analysed media and detect signs of manipulation.

1. **The Phoneme-Viseme Mismatch**

The Phoneme-Viseme Mismatch technology uses advanced artificial intelligence algorithms to analysed video and identify mismatches. It compares mouth movements (viseme) to spoken words (phonemes) and looks for possible inconsistencies. If a discrepancy is detected, it is a strong indication that the video is a deep fake.

1. **CONCLUSION**

Deepfake is Artificial technology is incredibly advanced and can easily fool humans. The research we have discussed deepfake, benefits of deepfake technology and its challenges. In this paper we have provide AI based Deepfake creation and detection tools and techniques. This research concludes there are both Positive and Dangerous Applications of Deepfake Technology.

**REFERENCES**

1. Abu-Ein, Ashraf A., et al. "Analysis of the current state of deepfake techniques-creation and detection methods." *Indonesian Journal of Electrical Engineering and Computer Science* 28.3 (2022): 1659-1667.
2. Akhtar, Zahid. "Deepfakes Generation and Detection: A Short Survey." *Journal of Imaging* 9.1 (2023): 18.
3. Botha, Johnny, and Heloise Pieterse. "Fake news and deepfakes: A dangerous threat for 21st century information security." *ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited*. 2020.
4. Chadha, Anupama, et al. "Deepfake: an overview." *Proceedings of Second International Conference on* Computing, Communications, and Cyber-Security: IC4S 2020. Springer Singapore, 2021.
5. Fletcher, John. "Deepfakes, artificial intelligence, and some kind of dystopia: The new faces of online post-fact performance." *Theatre Journal* 70.4 (2018): 455-471.
6. Gaur, Loveleen, ed. *DeepFakes: Creation, Detection, and Impact*. CRC Press, 2022.
7. Guarnera, Luca, et al. "The face deepfake detection challenge." *Journal of Imaging* 8.10 (2022): 263.
8. Khder, Moaiad Ahmed, et al. "Artificial Intelligence into Multimedia Deepfakes Creation and Detection." *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*. IEEE, 2023.
9. Lee, Gihun, and Mihui Kim. "Deepfake detection using the rate of change between frames based on computer vision." *Sensors* 21.21 (2021): 7367.
10. Lin, Yuru, and Krishnaveni Parvataneni. "Deepfake Generation, Detection, and Use Cases: A Review Paper." *International Journal of Computational and Biological Intelligent Systems* 3.2 (2021).
11. Maras, Marie-Helen, and Alex Alexandrou. "Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos." *The International Journal of Evidence & Proof* 23.3 (2019): 255-262.
12. Mirsky, Yisroel, and Wenke Lee. "The creation and detection of deepfakes: A survey." *ACM Computing Surveys (CSUR)* 54.1 (2021): 1-41.
13. Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection: A survey." *Computer Vision and Image Understanding* 223 (2022): 103525.
14. Rahman, Ashifur, et al. "A qualitative survey on deep learning based deep fake video creation and detection method." *Aust. J. Eng. Innov. Technol* 4.1 (2022): 13-26.
15. Swathi, P., and Saritha Sk. "Deepfake creation and detection: A survey." *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*. IEEE, 2021.
16. Zhang, Tao. "Deepfake generation and detection, a survey." *Multimedia Tools and Applications* 81.5 (2022): 6259-6276.