Deep Fakes Generator

Rahul Sharma[1], Sonal Choudhary[2], and Sanskar Singhal[3]

[1] **Guided By Mr. Deepak Moud**
[2]Ass. Professor
[3]Poornima Institute Of Engineering And Technology,Jaipur
[4]Affi. By Rajasthan Technical University, Kota

Abstract -
Technological evaluation puts us at a really advanced stage nowadays. Over the last few decades, we have become increasingly reliant on machines. With the development of machine learning and artificial intelligence, machines have become smarter and can perform a greater variety of actions. There are synthetic media, such as photographs, videos, and audio files, that are used for a variety of reasons. In the past, media manipulation has always involved humans and been heavily reliant on their needs. Deep-Fakes are mainly refers to the face swapping or making fake appearance of facial features of any human being. Recent developments in machine learning, deep learning, and artificial intelligence (AI) enable users to swap the faces and voices of other people in images, videos,films to make it appear as though they did something or are saying anything they want to refers to audio files manipulation. This technology is known as "deep-fake," which allows media manipulation using machine learning and AI.

index Terms - Media copyright, advertisement, Deep-Fake, Convolutional Neu-ral Network(CNN), Deep Neural Networks (DNN),Deep Convolutional Neural Network(DCCGAN),Recurrant Neural Netowrk(RNN), Generative Adversarial Networks (GANs).

Introduction

Online services, such as social and professional networking sites, get an estimated 1.8 billion photographs and videos daily . However, between 40 to 50 percent of these photos and videos seem to have been altered. either neutral goals (such as photos that have been altered for magazine covers) or antagonistic ones (such as propaganda or deception operations). Since faces are crucial to human interactions and biometrics-based person identification, human face image/video manipulation is a critical problem that jeopardises the accuracy of information on the Internet and face recognition systems. Therefore, realistic face sample manipulations have the potential to seriously undermine public confidence in digital security and communications applications (such as law enforcement). Deep-fakes are widely used today thanks to the accessibility of the internet to all forms of media and the strong demand they experience owing to their increased accuracy. Machine learning is a subset of artificial intelligence, which is the reproduction of the human brain in computers to enable machines to think like humans. Deep learning is a more focused kind of AI learning that creates artificial neurons that are similar to those in humans and helps computers do more complex computations. By introducing a collection of algorithms and a network of neurons, machine learning and deep learning tackle problems involving data. The DEEP-FAKE process, which combines deep learning and artificial intelligence generates fake content, involves changing a person's face in a video to that of a tar- get person, making the target person's face express itself correspondingly, and acting as if the target person is speaking the words that were actually said by somebody else. Deepfake techniques are defined as "face swapping," especially on pictures and videos, or the modification of facial expressions. Deep fakes also provide audio manipulation, which enables one to match an audio's frequency to another audio's while maintaining the same frequency. The audio manipulation may be attached to a movie or used alone as a message. The human senses have a very difficult time picking up on these visual or aural abnormalities unless they are carefully calculated. These so-called AI-synthesized media, often known as "deep fakes," can be divided into three groups: (1) Face-swapping, which involves automatically swapping out one person's face with another in a video, this technique is used for inserting the face of renown actors or personalities into a clip or entire movie in that they never appeared, Using this technique, non-consensual pornography is produced by swapping out one person's likeness for another person in an original video. (2) Lip-sync, in which a video source is altered so the mouth areas are consistent with an audio recording, for instance, actor Jordan Peele produced an example of such a method that altered a video of President Obama during his campaign. ,(3) puppet masters, who act out what they want their puppet to say and do while animating an audience member (head motions, eye movements, facial expressions).

Supplementary Note 1: History Of Deep Fakes

The development of GANs came about somewhat unexpectedly. Ian Goodfellow, a well-known AI researcher at the time and a Ph.D. fellow at the University of Montreal, came up with the concept while debating the shortcomings of previous generative algorithms with his pals at a friend's farewell party. After the party, he returned home full of optimism and put his plan into action. Surprisingly, the first attempt [5] went exactly as he had intended, and he was able to produce the Generative Adversarial Networks (more commonly known as GANs). The head of AI research at Facebook and professor at New York University Yann Lecun believes that GANs are "the most interesting idea in machine learning in the last 10 years."

Generation Of Fake

Visual material may be altered in a diverse range of ways, and new techniques are always being suggested. The most popular and promising of them will be briefly reviewed in this section. The addition is a rather typical process.

Visual material may be altered in a diverse range of ways, and new techniques are always being suggested. The most popular and promising of them will be briefly reviewed in this section. The addition is a rather typical process.

There are a number of ways you can generate fake media at your fingertips without having any technical knowledge. In this section, we will briefly discuss the types of fake media and the generational methods proposed. Fake me- dia content generation is not limited just to generating face-swapping images or videos, rather also common operations are adding, replication, or removing objects. It is possibleto add a new item by copying it from another picture (splic- ing) or from the same image (copy-move). A well-known example of exemplar-based in-painting involves expanding the backdrop to include an existing item (in-painting). There is also some post-processing, such as resizing, rotation, and color adjustment. Well, all that operation can be accomplished by widespread image editing tools. However, in recent years, deep learning and sophisticated computer graphics (CG) technologies have been used to achieve the same outcomes with improved semantic consistency. Artificial intelligence (AI) manipulations that do not require complex tools are frequently referred to as "shallow fakes" or "cheap fakes." Ironically, the deep-fake generations are often less expensive. Furthermore, they can have a significant influence on how reality is distorted. For instance, changing the meaning of a film entirely by deleting, adding, or copying entire sets of frames. Apart from the "classical" manipulation, including the specific areas of image or video facial swap, deep learning and artificial intelligence offer a large num- ber of synthesized media starting from zero. Autoencoders and generative adversarial networks aid in the development of complete solutions for facial synthesization, allowing for extremely high photo realism. Nowadays, image synthesis is also done based on a text description or an audio sequence.

Deep-fake Generation

Although these are primarily referred to as face-swapping techniques employing artificial intelligence, deep fakes are produced using artificial intelligence and deep learning. Deep fakes are used to create a facial synthesis between a source and a target, or, to put it another way, the source media may be altered to provide the desired outcomes depending on the target media. Deep-fake creation using two key elements 1. Generative adversarial network (GANs): GANs develop media files for sources and destinations where media is created using deep learning and artificial intelligence. 2. Autoencoder: This encoder searches for material that may be used for the encoding or other modification with a target, combining created media with the source to get the desired results. With this improvement in technology, it is now quite simple to produce deep fakes in a matter of minutes. There are several free web programs that may be used to manipulate photographs and videos. List of a few Deep-fake generating tools:

FaceApp:A smartphone application with face-swapping tools for deep-fake videos and AI picture editing.

DeepFaceLab: You may swap faces with this open-source tool, which can also be utilized for research.

DeepFaceWeb: It’s a web platform that enables the user to create face-swapped videos.

FacesSwap: An application that allows for deep fakes driven by AI that conducts the process using Tensorflow and Keras.

REFACE: Another AI-based tool to create face swaps in GIFs and images.

OpenAILabs: it is a very different tool in AI image processing that enables users to perform multiple Image operations such as out-painting, Alignment research etc.

Replicate: Advanced ai image models that allow you to manipulate the pictures with removal, addition, or generation based on just a text description.

DeepNude:It was an offered app that might be deleted. Remove Clothing from women in images may make them look nude, and it was taken down just three days after it was published.

FirstOrderMotionModel: it is an open-source available model for generating deep-fakes by yourself and can get you desired results.

StyleGAN It is developed by NVidia for facial features which allows to generate high resolution faces of people that do not exist in real world.

Image Generating Model

This idea of correctly creating the deep false pictures is not new in the present study activity. While there are other ways to implement these characteristics, our strategy avoids the usage of extremely powerful hardware by creating deep fakes with less resources. This strategy only relies on employing cloud resources and models that may be applied to a website’s web page using the supplied input. The models employed in this project are entirely reference-based models that integrate and provide an aggregated result based on various learning and outputs from these models.

Loss Functions :- In order to begin, we first create a Binary Crossentropy object using the tf.keras.losses module. The from logits argument is also set to True. We build the object and then populate it with unique generator and discriminator loss functions. Combining (i) the discriminator’s predictions on created pictures to an array of zeros and (ii) its predictions on real images yields our discriminator loss formula. The effectiveness of our generator’s ability to fool the discriminator is used to determine its loss. Consequently, we must contrast the discriminator’s judgements about the produced pictures with an array of 1s. Optimizer:- Additionally, we independently put up two optimizers for generator and discriminator networks. The Adam optimizer object is available in the tf.keras.optimizers module. generator-optimizer Adam(1.5e-4,0.5) discriminator-optimizer Adam(1.5e-4,0.5)

Models

These GANs should need to be trained on a good dataset in order to develop a good image synthesis model. In order to do this, a model was created and originally trained on the MNIST dataset. This allowed us to create accurate and high-quality handwritten digit pictures. The following is a later picture with face characteristics. Images from CelebA The high-quality celebrity face photos in this image collection. More than 10,000 photos, with a variety of face expressions and traits, are included. This data set from Kaggle FAce Image contains low quality photos of over 11500 online photographs with various facial expressions.

In computer vision-supervised learning applications, CNNs have been extensively utilized. Unsupervised picking up utilizing CNNs, interestingly, has gotten less attention. We hope to close the achievement gap between CNNs for supervised and unsupervised learning with this study. We demonstrate that the type of CNN known as deep convolutional generative ad- adversarial networks (DCGANs), which have some architectural restrictions, is an excellent choice for unsupervised learning. Through training on multiple picture datasets, we demonstrate convincingly that our deep convolution adversarial pair learns a hierarchy of representations in both the generator and discriminator, ranging from object parts to scenes. We additionally apply the learned attributes to shiny new undertakings to show how flexible they are as nonexclusive picture portrayals.

What Are use Of Deep-Fakes

Recent developments have made deep-fakes development more approachable and easy, rather than being restricted to experts and technical workers. Today, the vast majority of people have access to AI development, which is utilized for both commercial and non-commercial objectives, including entertainment and business. Deep fakes are employed to create exceptional art, hold audiences' attention, and provide them with distinctive experiences. Technology is currently being used to create copies of great works of art, such as a film created utilizing a famous Monalisa piece. By us- ing Deepfake technology's editing capabilities rather than reshooting videos, the film industry can save a ton of money and time. There are several other positive examples, including the renowned footballer David Beckham, who spoke in nine different languages to promote a campaign against malaria. Deep-Fake also has wide use in the educational sector. Generative Adversarial Networks may be utilized in many other fields to provide realistic experiences, such as the retail industry, where it would be feasible to physically view the genuine thing that we see in a store. Recently, Reuters and AI firm Synthesis worked together to create the first-ever synthesized news presenter. This was accomplished using the same AI techniques as Deep-fakes, and it will be useful for providing customized news to specific people. Deep generative modeling has also demonstrated excellent potential for growth in the healthcare sector. Instead of exchanging genuine data from patients and research projects, this technology might be used to create fake data. Additionally, by creating videos of well-known people requesting assistance or funding for innovative projects, this technology has great potential for fundraising and raising awareness.

How Deep Fakes Are Being Used

Entertainment And Media Industries. Over the past few decades, the entertainment industry has grown significantly, and deep fakes in the sector help to create effective scenes faster. Tom Hanks' encounter with President John F. Kennedy in the film Forrest Gump required months of preparation from talented actors. after 30 years, now that can be replicated within seconds using the advanced computers.

A subsidiary of the UK firm Synthesia requested the same advertisement after the company's two advertisements featuring the rapper Snoop Dogg were so popular. Instead of reshooting, Synthesia altered Snoop Dogg's lip gestures to match the name of the subsidiary in the new advertisement using deep fake technology.

With the help of his own company, Metaphysic, which enables anyone to create a synthetic avatar of themselves, the creator of the popular Tom Cruise deepfakes on TikTok found such widespread success.

The recent Season 2 finale of The Mandolorian used synthetic media production to make actor Mark Hamill resemble a younger Luke Skywalker.

Artificial intelligence can be used to create devices that can hear, see, and soon think with increasing precision. Thank you, Artificial General Intelligence (AGI). Computerized reasoning produced engineered media can likewise give people more office. It gives them independence by making accessibility tools that are more intelligent, less expensive, and individualized. Deep-fakes can help a teacher create engaging lessons. They would likewise rise above past customary vi-sual and media mediums.

In the classroom, artificial intelligence-generated synthetic media can bring historical figures to life. As a result, lessons become more interesting and dynamic. A fake film of reenactments or a voice-over film of a historical figure will have a greater impact. It could support cooperation and make for a superior learning device.

Video Gaming Industry. Games that were created just us-ing programming languages and graphical tools in the past did not appear to hold the audience's attention very well. The gaming business has experienced tremendous growth along with the advancement of technology. The graphics and visuals used in today's games are more lifelike, which appeals to the eye and makes the action more interesting. Characters in the games aren't just randomly generated faces; instead, deep-fakes are used to make them appear like actual people, which connects players to the game. GOD OF WAR: very well-known gaming franchise has gained enormous popularity since it was first launched. In 2018, a new edition of the game was released that allowed gamers to view the protagonist, ' Kratos ', in incredibly realistic visuals where the face of Christopher Judge was used.

Marvel's Avengers: Popular Hollywood studio Marvel has its own gaming universe as well known as Avengers. Which

is also, has the faces of their movies actor as gaming characters. Until Dawn: Bohemian Rhapsody's character was portrayed by acclaimed actor Rami Malek in the well-known horror video game series Until Dawn.
Batman- Arkham Series: In the well-known game, the Joker was played by the extremely well-known actor Mark Hammill.
Cyberpunk 2077: Keanu Reeves doesn't need to be introduced in public, he provided his face for the video game Cyberpunk 2077.

Facial Copyright

A new idea of facial copyright has emerged in the media business as a result of technological advancements. For as long as the contract is in effect, prominent studios have introduced the copyright of the faces of their iconic characters. Although it may sound unusual, studios have also used this technique in the film "Fast and the Furious," where star Paul Walker's untimely death forced them to re-shoot the scene with another actor before overlaying Walker's face and finishing the scene despite the difficulties.

Deep-Fake Detection

Deepfake contents are frequently difficult to recognize, and occasionally even impossible, to do so by a person with untrained eyes. Finding abnormalities in Deep fake films requires a high degree of knowledge. To tackle Deepfake,a number of strategies have been put out up to this point, including machine detection, forensics, authentication, and regulation. According to experts, since Deepfake videois produced by an algorithm as opposed to genuine video, which is produced by a real camera, Deepfake may be identified from existing cues and artifacts. Additionally, there are other abnormalities that might be used to identify Deepfake, such as inconsistent illumination, picture warping, smoothness in specific places, and strange pixel shapes.

Facial Movement Tracking. Tracking of facial movementsis proposed as an effective way of detecting deep fakes, as the videos are generated using overlapping and computer programs, there are very certain fixed movements on the facial expression of a person's video that can be tracked by using software of eyes.

Frame Based Detection. The major advancements of the various techniques revolve around the frame function extrac- tor. Numerous hand-crafted algorithms, deep learning algorithms, and more recently GAN-based methods are all be- ing researched. Distinguished between authentic and false photos using variations in the 3D head posture. The par- ticular light sensor noise pattern for each digital camera is called PRNU (Photo Response Non-Uniformity). Because it may be altered by any picture alteration, this local noise mode is frequently employed for counterfeit image identifi- cation. recommends modifying face identification by fusing RGB spatial information with two-stream CNN steganalysis features. This is a result of combining manual work with machine learning.

Clip/Segment Based. The fundamental distinctions be- tween the various approaches are the clips extractor and aggregator. Eye blinking and rPPG sought physiological signals as features, but they rapidly lost their efficacy when confronted with more training data and more sophisticated generation models. RNN was originally employed as an aggregator to determine the interval of time between frames. The duration of the segment is important for the aforementioned procedure, however, the length of the test video in real life is unpredictable. The action recognition technique served as the basis for 's primary notions. However, employing the action recognition technique directly is not advised owing to the distinction between action recognition and DeepFake detection. These techniques rely on to efficiently capture properties in temporal data.

Applications of Deep-fake Technology that can be Dangerous

Deep-fakes, which are hybrid or synthetic media, is a source of information on the internet or on social media. The most frequent threat is the dissemination of false information to the public as a result of data alteration in media files. False recordings of well-known people making statements they never said are another serious threat from deep fakes; one such video featuring the former US president Barack Obama was widely circulated online. Although it was quickly identified as phony despite having a lower accuracy score, one video that appeared to be extremely authentic may have a significant impact on world peace and spark another global war. Because one replaced face in such content can harma person's reputation in society, the culture of pornographic content is growing in the internet age, and this comes with the threat of fake promotion of the pornography of famous people or even regular people. These kinds of threats are frequently used to extort money from people.

.1. Corporate Level Fraud. The most common attack methods are deepfake-based ones. Fraudsters no longer attempt to convince an organization employee to send money through a fictitious email. By calling them pretending to be the CEO or CFO, they persuade them.

.2. Fake News/False Information. Over the entire course of time, counterfeit news has been utilized to instigate discord and division. It is still used today to deceive the public and thwart social, business, and political endeavors. Fake recordings that portray actual events or show real people talking and acting in ways they would never have, for example, can engender doubt and uncertainty. This is already being attempted by the false news industry.

.3. Fake Videos. Using the initial Deep-fake technology, a film was produced in which a Thai actor stood in for Presi- dent Trump. On social media, the warped video attracted a lot of attention and was shared globally. The original video's actress asserts that the President is genuine in other viral videos, but the President disputes her assertion.

Conclusion

We have spoken about how to generate Deepfake films and images as well as how to identify them, as well as how to use Deepfakes for both good and bad. We also covered a number of Deepfake generation and detection technologies. Every day, a new aspect of technology is introduced to us, and technology is always improving. The development of the Deepfake generating method is making the detection process more challenging every day. The successful identification of Deepfake depends on improved detection techniques and an accurate dataset. According to our analysis, individuals are losing faith in online information daily as a result of Deep-fake technology. As the methods for creating Deep-fake contents advance daily, anybody with a powerful computer—rather than just someone with a basic understanding of technology—can produce Deep-fakes of any person for harmful intentions. Furthermore, the rapid distribution of Deep-fake films was made feasible by advancements in networking and the internet. This tactic could sway the judgments of world leaders and other influential people, which might be detrimental to international peace. On the other hand, there are advantages and disadvantages to technology. Deep fakes that allow for face-swapping are advantageous in the media sector and are also relatively affordable. Face-swapping techniques are advantageous for users because they allow them to enjoy high-definition graphics-only movies and games that don't endanger human life. Ai image and video tools assist users in doing post-processing operations over photos and videos without the need for technical expertise, and as a result, they have a large user base. A wonderful chance to improve our lives is provided by deepfakes. Synthetic media produced by artificial intelligence may be a potent facilitator. People can find a voice and a sense of purpose through deepfakes. New ideas and capacities for empowerment have come frommany facets of society, including business, accessibility, pub- lic safety, and the arts, expression, and accessibility. No mat-ter what their restrictions, deepfakes have the power to let anybody in. However, the risk of exploitation grows as synthetic media technology becomes more broadly accessible. Deepfakes have the power to deceive the public, manufacture evidence, and damage people's reputations. The public's trust in democratic institutions may be damaged.

Refernces

A Threat of Deep-fakes as a Weapon on Digital Platform and their Detection Methods - Manish Khichi, Dr, Rajesh Kumar Yadav - IEEE [2021]

Protecting World Leaders Against Deep Fakes Shruti Agarwal and Hany Farid - CVF[IEEE] University of California, Berkeley Berkeley CA, USA

David G¨uera and Edward J Delp. Deepfake video detection using recurrent neural networks. In IEEE International Conference on Advanced Video and Signal Based Surveillance, pages 1-6, 2018

Media Forensics and DeepFakes: An Overview Luisa Verdoliva , Senior Member, IEEE

The Emergence of Deepfake Technology: A Review MikaWesterlund

Deep Insights of Deepfake Technology : A Review Bahar Uddin Mahmud1* and Afsana Sharmin

Awareness to Deepfake: A resistance mechanism to Deepfake : Mohammad Faisal Bin Ahmed, M.Saef Ullah Milah , Abhijit Bhowmik , Junaida iti Sulaiman - IEEE [2021]

Combining Deep Learning and Super-Resolution Algorithms for Deep Fake Detection Nikita S. Ivanov1, Anton V. Arzhskov2, Vitaliy G. Ivanenko3 - IEEE 2020

Deepfake Detection Using SVM Harsh Agarwal1, Ankur Singh2, Rajeswari D3 -ICESC-2021

DEEPFAKE Image Synthesis for Data Augmentation : NAWAF WAQAS , SAIRUL IZWAN SAFIE ,KUSHSAIRY ABDUL KADIR , , (Senior Member, IEEE),SHEROZ KHAN, AND MUHAMMAD HARIS KAKA KHEL2 - IEEE

Image Animations on Driving Videos with DeepFakes and Detecting DeepFakes Generated Animations Yushaa Shafqat Malik, Nosheen Sabahat,Muhammad Osama Moazzam - IEEE 2020

Karras, T., Laine, S., Aila, T. (2019). A style-based generator architecture for generative adversarial networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., Morales, A., Ortega-Garcia, J. (2020). Deepfakes and Beyond: A Sur- vey of Face Manipulation and Fake Detection. arXiv preprint arXiv:2001

Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. In Proceedings of the IEEE conference on computer vision and pattern recognition

Choi, Y., Choi, M., Kim, M., Ha, J. W., Kim, S., Choo, J. (2018). Stargan: Unified generative adversarial networks for multi-domain image-to-image translation. In Proceedings of the IEEE conference on computer vision and pattern recognition

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... Bengio, Y. (2014). Generative adversarial nets. In Advances in neural information processing systems

Afchar, D., Nozick, V., Yamagishi, J., Echizen, I. (2018, December). Mesonet: a compact facial video forgery detection network. In 2018 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE.