FACE CHANGER USING DEEP FAKE IN PYTHON

Sankeerth Reddy Jakkidi¹,Ajoji Aravind Kumar², Boompagul Pranay Kumar³, Dr M V Kamal⁴ ^{1,2,3}B. Tech Student, Department of CSE (Cyber Security), Malla Reddy College of Engineering and Technology, Hyderabad,India. ⁴Professor and HoD,Department of CSE Emerging Technologies,Malla Reddy College of Engineering and Technology,Hyderabad,India.

To Cite this Article

Sankeerth Reddy Jakkidi, Ajoji Aravind Kumar, Boompagul Pranay Kumar, Dr M V Kamal, **"FACE CHANGER USING DEEP FAKE IN PYTHON"** Journal of Science and Technology, Vol. 08, Issue 12,- Dec 2023, pp7-16

Article Info

Received: 12-11-2023 Revised: 22-11-2023 Accepted: 02-12-2023 Published: 12-12-2023

ABSTRACT:

The "Face Changer using Deep Fake in Python" project introduces an innovative application of deep learning techniques for facial manipulation. Leveraging deep neural networks, this project aims to create a Python-based tool that enables users to easily and ethically alter facial features in images and videos. It relies on high-quality face datasets for training and employs advanced deep learning models, such as Generative Adversarial Networks (GANs) or Variational Autoencoders (VAEs), to generate highly realistic facial transformations. A user-friendly Python interface is developed to simplify the process, enabling users to upload media and select desired transformations, including changes to identity, expression, or age. Moreover, this project strives to achieve real-time processing capabilities, making it possible to apply facial alterations within live video streams. Recognizing the ethical concerns surrounding deep fake technology, the project addresses these issues by including disclaimers and safeguards, as well as educating users on responsible usage. Quality and performance are paramount, with a focus on creating visually convincing deep fakes while optimizing processing speed. Additionally, measures are implemented to ensure security and privacy, such as watermarking the output and preventing unauthorized manipulation. This project's diverse applications span entertainment, identity protection, education, and creative art, empowering users to explore new avenues of expression and safeguard their digital identities. In summary, the "Face Changer using Deep Fake in Python" project combines cutting-edge deep learning technology with ethical considerations to provide a versatile and responsible tool for facial manipulation in the digital age.

I INTRODUCTION

In an era defined by rapid advancements in artificial intelligence

and computer vision, the convergence of deep learning techniques and real-time video manipulation has given rise to an innovative technology known as DeepFace Live.Face Changer is an innovative project that harnesses the power of cutting-edge deep learning techniques to explore the fascinating domain of facial image transformation. This endeavor goes beyond conventional facial recognition and expression analysis, delving into the realm of artistic, creative, and abstract face alteration.

This paper presents an approach for changing the facial coordinates of a person in the video as per the given input image. To get the desired outcome we use many machine learning and deep learning algorithms like Generative adversarial network and auto encoders to manipulate the video facial expressions. It stands out as a pivotal feature, where we intend to develop a robust algorithm capable of seamlessly replacing one individual's face with another while preserving the original image's lighting conditions, facial expressions, and overall realism. This feature has vast potential for fun and entertainment, as well as applications in the film and advertising industries.

This is mainly used to do some funny things and fancy computer tricks to do cool stuff with people'sfaces in pictures and videos. Additionally, our project aims to delve into the realm of emotion recognition. By harnessing state-of-the-art deep learning techniques, we plan to build a facial emotion recognition system that can accurately detect and analyze emotions displayed on human faces. This could have profound implicationsin psychology, enabling researchers to gain insights into emotional responses, and also benefit market research by gauging consumer reactions to products or advertisements.

In an era defined by rapid advancements in artificial intelligence and computer vision, the convergence of deep learning techniques and real-time video manipulation has given rise to an innovative technology known as DeepFace Live. This groundbreaking concept represents a new frontier in visual media manipulation, enabling the seamless and dynamic alteration of facial expressions, features, and even entire identities. Deepfake methods normally require a large amount of image and video data to train models to create photo-realistic images and videos.

In today's digital era, the realm of image and video manipulation has witnessed a remarkable evolution, thanks to the advent of deep learning techniques. Among the most intriguing and, at times, controversial innovations in this field is the concept of deep fakes. These sophisticated neural networks have the power to seamlessly alter the faces of individuals in images and videos, ushering in a new era of creative expression, entertainment, and, simultaneously, raising critical ethical considerations.

The "Face Changer using Deep Fake in Python" project is a fascinating exploration of this groundbreaking technology, offering a practical and responsible tool for facial transformation. This project harnesses the potential of deep learning, typically employing advanced models like Generative Adversarial Networks (GANs) or Variational Autoencoders (VAEs), to achieve realistic and convincing facial alterations. With a focus on high-quality data preparation, the model is trained on diverse datasets encompassing various facial expressions, lighting conditions, and angles, ensuring robust performance.

What sets this project apart is its commitment to user-friendliness. Through a Python-based interface, users can effortlessly upload images or videos and select their desired facial transformations, such as altering identity, expression, or age. Real-time processing capabilities further enhance the user experience, making it possible to apply facial changes within live video streams.

Nevertheless, the ethical implications of deep fake technology are not taken lightly. The project places a strong emphasis on ethical considerations, including the potential for misuse. It includes safeguards and disclaimers to promote responsible usage and user education. The pursuit of quality and performance is paramount, with ongoing efforts to fine-tune the model and optimize processing speed. Security and privacy are also fundamental aspects of the project, with measures in place to prevent unauthorized manipulation and protect individuals from misuse.

II LITERATURE SURVEY

Based on the observation that temporal coherence is not enforced effectively in the synthesis process of deep- fakes, Sabir et al. [103] leveraged the use of spatiotemporal features of video streams to detect deepfakes. Video manipulation is carried out on a frame-by-frame basis so that low level artifacts produced by face manipulations are believed to further manifest themselves as temporal artifacts with inconsistencies across frames. A recurrent convolutional model (RCN) was proposed based on the integration of the convolutional network DenseNet and the gated recurrent unit cells [1] to exploit temporal discrepancies across frames. The proposed method is tested on the FaceForensics++ dataset, which includes 1,000 videos, and shows promising results.

"FaceApp: About us". FaceApp.com. 2022-02-28. Retrieved 2022-02-28. en:Artificial_intelligence, oldid 916393721[circular reference] Stark, Harold (25 April 2017). "Introducing FaceApp: The Year Of The Weird Selfies". Forbes. Retrieved 13 June 2017.

Vincent, James (27 May 2019). "This app uses neural networks to put a smile on anybody's face". The Verge. Retrieved 13 June 2017. Vincent, James (15 February 2017). "Android users can now harness the power of neural networks to alter faces". The Verge. Retrieved 13 June 2017. Tan, Yvette (15 February 2017). "Viral selfiemorphing FaceApp launches on Android after huge iOS success". Mashable. Retrieved 13 June 2017.

Karner, Jen (2019-07-18). "Try out all of the different filters on FaceApp". Android Central.

Retrieved 2019-07-18. Cracker, Miz (5 May 2017). "The Magnetic and Emotionally Complex Power of FaceApp's Gender Filter". Slate. Retrieved 13 June 2017. Manning, Allee (1 May 2017). "FaceApp's gender swap is playing mind games with trans users". The Daily Dot. Retrieved 13 June 2017. "AI photo editor FaceApp goes viral again on iOS, raises questions about photo library access". TechCrunch. 17 July 2019. Archived from the original on 2020-06-16. Retrieved 2019-07-17.

Likewise, G[•]uera and Delp [2] highlighted that deepfake videos contain intraframe inconsistencies and temporal inconsistencies between frames. They then proposed the temporal-aware pipeline method that uses CNN and long short term memory (LSTM) to detect deepfake videos. CNN is employed to extract frame- level features, which are then fed into the LSTM to create a temporal sequence descriptor. A fully-connected network is finally used for classifying doctored videos from real ones based on the sequence descriptor as illustrated. An accuracy of greater than 97% was obtained using a dataset of 600 videos, including 300 deepfake videos collected from multiple video hosting websites and 300 pristine videos randomly selected from the Hollywood human actions dataset.

www.jst.org.in

III WORKING

The working methodology of a "Face Changer using Deep Fake in Python" project involves several key steps, from data preparation and model training to user interface design and ethical considerations. Below is a detailed breakdown of the working methodology for such a project:

Data Collection and Preparation:

Gather a diverse and high-quality dataset of faces. This dataset should include various individuals, facial expressions, lighting conditions, and angles. Annotate the dataset to identify key facial landmarks and attributes, which will be used for training the model.

Deep Learning Model Selection:

Choose a deep learning architecture, often a Generative Adversarial Network (GAN) or Variational Autoencoder (VAE), as the basis for the model. Customize the model architecture to suit the specific requirements of the project, such as the desired level of realism and the types of facial transformations.

IV RESULTS EXPLANATION

Model Training:

Train the deep learning model using the prepared dataset. This involves feeding the model with pairs of input and target images. The model learns to generate realistic facial transformations by minimizing a specific loss function. For instance, it can minimize pixel-wise differences between generated and target images.

User Interface Development:

Create a user-friendly Python interface that allows users to interact with the deep fake system. Users should be able to upload images or videos and select the desired facial transformations, such as changing identity, expression, age, or other attributes.

Real-time Processing (Optional):

If the project aims to support real-time video processing, optimize the model and processing pipeline to achieve low-latency performance. Implement streaming capabilities that allow users to view the transformed video in real time.

At first the requirements are installed and it configure as the corresponding dependencies. After completion of installation of the requirements the system will get all the libraries that required for the face changing as per the given image to the video character.



Fig. Requirements installation

The system will resolve the facial coordinates of the image and video, recognizes the facial expressions of the face in the video.

The HTTP request is sent to the link that present in the requirements which redirects the training of face to its techniques and wait for the response. The image is trained under all the situations to give the accurate facial expressions as represented in the video which helps to fit the input image into the video character

> Resolving tor-Jrs.huggingface.cs (odr-Jrs.huggingface.cs)... 10.155.68.128, 10.155.68.75, 10.155.68.44, ... Connecting to odr-Jrs.huggingface.co (odr-Jrs.huggingface.cs)(10.155.68.128):443..., connected. HTTP request sert, maiting response... 200 D1 Length: 554155681 (S100) [finaryloctet-stream] Saving to: 'insusper_110.com.' insusper_110.com. 1005[insussessessesses] Saving to: 'insusper_110.com.' 1023-10-00 10:11:06 (M41 M0(4) - 'insusper_110.com.' saved [S14255681/554155481]

Fig: Training the image

The system takes the input image and video and manipulate the facial expressions in the character present in the video by training the image with lot of data like expressions similar to the video character so that the face will get trained by the expressions so that it will be fit into the video and the facial coordinates will be changed.

In the above code we have give the path of the image with .jpg or .jpeg extensions so that machine will recognize that it is the image and starts training it.

The video path also required for the processing where the extension of the video also very much required which must be in .mp4 format so that the system starts analyzing the faces in the video and facial expressions in the video and train the image as per the expressions and change the video with the input image and give to us. So we need to download the video which will be displayed in files in the swapped.mp4 format. After downloading the video you can play it with external player in the system.

This is mainly happens with the gan networks. The Generator Model generates new images by taking a fixed size random noise as an input. Generated images are then fed to the Discriminator Model. The main goal of the Generator is to fool the Discriminator by generating images that look like real images and thus makes it harder for the Discriminator to classify images as real or fake.

The Discriminator Model takes an image as an input (generated and real) and classifies it as real or fake.Generated images come from the Generator and the real images come from the training data.The discriminator model is the simple binary classification model.

The Generator Model G takes a random input vector z as an input and generates the images G(z). These generated images along with the real images x from training data are then fed to the Discriminator Model D. The Discriminator Model then classifies the images as real or fake. Then, we have to measure the loss and this loss has to be back propagated to update the weights of the Generator and the Discriminator.When we are training the Discriminator, we have to freeze the Generator and back propagate errors to only update the Discriminator.

The following character has been changed as per the given srk image with character in the video. Finally the changed image will be displayed in the files so that image can be download from the files.



Fig: results of face changer

The output screen in a face changer project typically displays the transformed or altered facial images or videos. This screen showcases the primary result of the project, which can include a wide range of modifications to the original face. These alterations may involve swapping faces with another person, changing facial expressions to convey different emotions, applying virtual makeup, adding accessories like glasses or hats, or even morphing the face to create artistic or humorous effects. The key to a successful output screen lies in the realism and quality of the modifications, ensuring that they seamlessly integrate with the original footage, creating convincing and visually engaging transformations. Users can evaluate the effectiveness of the face changer application based on the content displayed on this screen.

The program, and the post, will be divided into three sections. The first one deals with the extraction of the faces from the two videos and the construction of standard face datasets. The second part uses the datasets together with a neural network to learn how to represent a face in some latent space and reconstruct an image of a face from this representation. The last part uses the neural network to create a face as in the source video but with the expression of the person in the destination video for each frame of the video. Then the original face is replaced by the fake one, and the new frame is saved into the new fake video.

V CONCLUSION

As technology continues to advance, face changer projects are likely to become more sophisticated, offering even more realistic and engaging transformations. However, striking a balance between innovation and responsible use will remain a critical challenge for developers and users alike. Therefore, ongoing research, ethical considerations, and safeguards against misuse are essential components of the future of face changer projects. In conclusion, a face changer project represents a fascinating intersection of technology and creativity, offering a range of possibilities for altering and enhancing facial features in images and videos. This project's outcome typically depends on the quality of the algorithms and techniques used to modify faces, the realism of the results, and the overall user experience. While face changer projects have numerous entertaining and artistic applications, they also raise significant ethical and privacy concerns. The ability to manipulate and impersonate individuals in digital media underscores the importance of responsible use and regulation in this field.

VI REFERENCES

- 1) Shruti Agarwal, Hany Farid, Yuming Gu, Mingming He, Koki Nagano, and Hao Li. Protecting world leaders against deep fakes. In Computer Vision and Pattern Recognition Workshops, volume 1, pages 38–45, 2019.
- Pascal Vincent, Hugo Larochelle, Yoshua Bengio, and PierreAntoine Manzagol. Extracting and composing robust featureswith denoising autoencoders. In Proceedings of the 25th International Conference on Machine learning, pages 1096–1103, 2008.
- 3) Diederik P Kingma and Max Welling. Autoencoding variational Bayes. arXiv preprint arXiv:1312.6114, 2013.
- 4) Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. Advances in Neural Information Processing Systems, 27:2672– 2680, 2014.
- 5) Alireza Makhzani, Jonathon Shlens, Navdeep Jaitly, Ian Goodfellow, and Brendan Frey. Adversarial autoencoders. arXiv preprint arXiv:1511.05644, 2015.
- 6) Ayush Tewari, Michael Zollhoefer, Florian Bernard, Pablo Garrido, Hyeongwoo Kim, Patrick Perez, and Christian Theobalt. High-fidelity monocular face reconstruction based on an unsupervised model-based face autoencoder. IEEE Transactions on Pattern Analysis and Machine Intelligence, 42 (2):357–370, 2018.
- 7) Jiacheng Lin, Yang Li, and Guanci Yang. FPGAN: Face deidentification method with generative adversarial networks for social robots. Neural Networks, 133:132–147, 2021.
- 8) Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, and Arun Mallya. Generative adversarial networks for image and video synthesis: Algorithms and applications. Proceedings of the IEEE, 109(5):839–862, 2021.
- 9) Siwei Lyu. Detecting 'deepfake' videos in the blink of an eye. http://theconversation.com/detecting-deepfake videos - in- the - blink - of- an - eye - 101072, August 2018.
- 10) Bloomberg. How faking videos became easy and why that's so scary. https://fortune.com/2018/09/11/deepfakesoamavideo/, September 2018.
- 11) Robert Chesney and Danielle Citron. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs, 98:147, 2019.
- 12) Nataraj, L., et al. (2019) Detecting GAN Generated Fake Images Using Co-Occurrence Matrices. Electronic Imaging,2019,532-1-532-7.https://doi.org/10.2352/ISSN.24701173.2019.5.MWSF-532.