International Journal of Engineering Sciences & Emerging Technologies, May 2024.
ISSN: 22316604 Volume 11, Issue 3, pp: 614-618 ©IJESET

DEEPFAKE WITH AI

Anurag Malik[1], Abhishek[2], Aseem Gupta[3], Gaurang Gupta[4], Iram Rafi[5]

[1,2,3,4,5] Department of Computer Science & Engineering, Moradabad Institute of Technology, Moradabad, India.

[1]Associate Professor. anurag_malik@rediffmail.com
[2] Btech Scholar. abhishekrajput4528@gmail.com
[3] Btech Scholar. aseemg786@gmail.com
[4] Btech Scholar. gauranggupta07@gmail.com
[5] Btech Scholar. iramrafi862002@gmail.com

ABSTRACT

Employing a pre-trained generative adversarial network, it's turning into easier to substitute the face of 1 person during a video with the face of another (GAN). Recent public scandals, equivalent to celebrity face swapping in erotica movies, have prompted the event of machine-controlled ways to notice deepfake videos. to assist within the development of such systems, we discharged the primary in public on the market batch of Deepfake movies generated from VidTIMIT videos during this studio. The deepfakes were created exploitation ASCII text file computer code supported GAN, and that we highlight that the coaching and commixture parameters have a considerable impact on the standard of the ultimate videos. To demonstrate the effect, we have a tendency to created low Associate in Nursingd high-visual-quality movies (320 videos each) exploitation parameter settings that were changed differently. we've shown that progressive biometric identification systems supported VGG and face internet neural networks are sensitive to faux movies, with false acceptance rates of 84.72% and 96.58% (for high-quality versions), respectively, that emphasizes the implicit need for approaches to notice deepfake videos, which means the necessity for deepfake video detection approaches. we have a tendency to found that an audio-visual technique based on lip synchronisation inconsistency detection couldn't distinguish deepfake movies when analysing many benchmark approaches. For high-quality deepfakes, the very best playacting technique, that relies on visual quality measures and is usually employed in the presentation attack detection industry, came back a similar error rate of 8.97 percent. Our findings show that GAN generated deepfake movies are difficult to spot exploitation existing biometric identification systems and detection approaches, and thanks to the advance in face-swapping technologies, it'll be even tougher to defeat.

KEYWORDS

Deepfake video detection, convolutional neural network (CNN), recurrent neural network (RNN), generative antagonistic network (GAN), XG BOOST.

1. INTRODUCTION

Recent advances in machine-controlled video and audio written material tools, generative adversarial networks (GANs), and social media create it potential to quickly produce and distribute high-quality doctored video content. As a results of such content, deliberate misinformation, known as "fake news", has emerged poignant the political landscape of assorted countries. A spate of recent films, several vulgar, during which one face is substituted for one more employing a neural network, referred to as deepfakes, has sparked widespread outrage. an oversized variety of synthetically generated deepfake videos occur on social media and within the news as a result of ASCII text file computer code and applications for such face swapping, making a considerable technical downside for the detection and

filtering of such content. As a result, making effective systems which will mechanically notice these face swap videos is critical. till recently, most analysis has centred on up face-swapping technologies. Scientists and engineers are starting to work on the information and recognition approach, exploitation the image and video knowledge generated with an older face swapping methodology known as Face2Face or movies nonheritable with the Snapchat app, in response to demand. public to detect face-swapping technologies. it's conjointly crucial to know however dangerous Deepfake movies are to biometric identification algorithms. as a result of if these systems aren't fooled by deepfakes, there's no want for a separate methodology to spot deepfakes. we have a tendency to tested 2 progressive neural network-based systems VGG Associate in Nursingd Face net on raw and face-swapped videos to envision however vulnerable biometric identification is to deepfake movies. we have a tendency to initial U.S.A.e an audiovisual approach to sleuthing deepfakes, that appearance for inconsistencies between visual lip movements and audio speech. It permits us to work out how well the generated Deepfakes will mimic mouth movement and whether or not lips are in adjust with speech.

2. LITERATURE SURVEY

To alter recognition, Pavel Korshunov and Sébastien Marcel [1] have projected a replacement threat. By treating deepfake videos as digital presentation attacks, we've conjointly applied many elementary ways that represent the domain of attack detection, equivalent to (IQM) Associate in Nursingd Support Vector Machines (SVM). we have a tendency to create the information of deepfake videos face recognition, and deepfake detection systems with acceptable ratings on the market as an ASCII text file Python package for researchers to review, reproduce, and extend our work.

Akhtar, Z.; Dasgupta, D.; Banerjee[2]. Face-swapping deepfake techniques are currently wide used, leading to an oversized variety of extremely realistic faux videos that endanger people' and countries' privacy. identifying between real and deepfake videos has become a crucial issue thanks to the devastating impact they're having on the world. This paper introduces a replacement deepfake detection methodology: Convolutional Neural Network - Extreme Gradient Boosting - you merely look once (YOLO-CNN-XGBoost).

Vezzetti, .; Marcolin, .; Tornincasa[3] This paper proposes a unique method for mechanically locating eleven landmarks in facial RGB images. identifying between real and deepfake videos has become a crucial issue thanks to the devastating impact they're having on the world.

Zhang; Zhang W; Liu[4]. this text describes a time period system read of a real-time system for multi-view facial feature localization in RGB-D pictures. The biometric identification localization downside is developed as a regression framework that estimates each the cause of the top and therefore the position of the popularity mark. To handle high-dimensional regression output, we have a tendency to propose a coarse-tofine approach during this framework.

Viola, P.; Jones[5] This paper describes a machine learning approach for visual beholding capable of process images with high recognition rates whereas processing images at a high rate. This work is characterised by 3 key contributions. the primary is that the introduction of a replacement image illustration referred to as "Integral Image" that permits for quick calculation of the features utilized by our detector.

Bazarevsky, V.; Kartynnik, Y.; Vakunov[6] The projected model, acting on the total image or a video frame, is used because the initiative in nearly any face-related pc vision application, equivalent to B, 2D/3D facial key points, contour or surface pure mathematics estimation, face expression or expression classification and facial region segmentation. As a result, the task that follows within the computer vision pipeline can be outlined in terms of acceptable facial detail. once combined with BlazeFace' few facial keypoint estimates, this crop can be turned to center the face on the inside, normalize to scale, and have a near-zero roll angle.

Zhang, K.; Zhang [7] during this article, we recommend a extremely cascaded multitask structure that produces use of the intrinsical association among them to enhance their performance. Our framework adopts a cascaded structure with 3 phases of exquisitely designed deep convolution internetworks that coarse-to-finely predict the position of faces and landmarks.

Tan, M.; Le. economical net [8] Convolutional neural networks (ConvNets) are usually designed with a rigid resource budget and are scaled for larger exactness as a lot of resources are deployed. during this paper, we have a tendency to examine the model scaling in-depth and realize that the careful equalisation of width, resolution, and network depth will improve performance.

Rossler, A.; Cozzolino, D.; Verdoliva [9] This paper check-up on the fact of circumstances of the art of image alternation and the way difficult it's to catch them either manually or automatically. This paper recommended an automatic customary for facial manipulation detection to normalize the assessment of identification methods.

3. PROBLEM STATEMENT

There are multiple instances of faux videos that includes well-known politicians and celebrities. These fraud videos are terribly onerous to spot with the oculus and have become a vital social issue. thus far, it has been discovered that Deepfake videos simply go microorganism on varied social media platforms like YouTube, Twitter, and Facebook. These platforms are operating terribly onerous to resolve this problem. Facebook is creating an enormous investment of ten million bucks to mend it, and totally different social media platforms equivalent to Google and Twitter are working to fix this problem. Deepfake identification is consequently a troublesome job. during this project, we are going to see however we are able to distinguish between fauxs and real ones. Breaking down videos into images, distinctive faces in fake and real videos, cropping them and analysing them are some of them. Figure.1 represents the simple architecture of the proposed system and Figure.2 represents Video Splitting.

4. PROPOSED SOLUTION

4.1. By exploitation XGBoost

The proposed theme includes a robust methodology for sleuthing deepfakes in videos. The system architecture of the proposed deepfake video noticeion scheme could be a YOLO face detector to detect faces from video frames. The InceptionResNetV2 CNN model is employed to extract discriminating visual-spatial options. These features facilitate within the exploration of visual artifacts in video frames, that are then fed to the XGBoost classifier to differentiate between real and deepfake videos. The projected theme is explained thoroughly below.

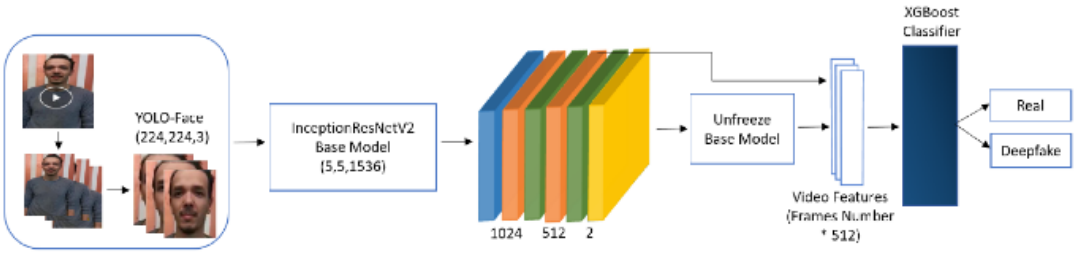


Figure 3. Deepfake videos detection system architecture of the proposed model

4.2.1. Pre-Processing Stage

The frames were taken from videos. Faces are important in today' manipulation methods; thus, etymologizing the face space options ought to be a serious function. The YOLO face observeor

is employed to detect faces in video frames. as a result of the YOLO detector is trained to detect tight bounding boxes, the face' size is accrued by 22% relative to its region.

4.2.2 Spatial-Visual Feature Extraction Stage

one in every of the pre-trained CNN models, InceptionResNetV2, is used to derive the discriminant special features for every face photo. The InceptionResNetV2 is associate degree Inception-style network that produces use of residual connections rather than direct connections. Concatenation of filters is preferable. The Inception- ResNet block is formed from multiple convolution layers of varied sizes that are joined beside residual connections.

4.2.3. XGBoost Based Deepfake Detection Stage

The spatial-visual options are fed into the XGBoost recognizer, that uses them to differentiate between real and deepfake videos. The XGBoost rule may be a robust, expandable, and increased version of the gradient boosting algorithm that uses a additional precise guess to search out the foremost tree model. it's designed to be variable and efficient. It introduces parallel tree boosting, which solves a spread of knowledge science problems quickly and exactly [50,51]. The XGBoost contains a assortment of N classification and regression trees (CARTs).

4.2. By victimization GAN

Deepfakes are created using Generative Adversarial Networks (GANs), during which 2 machine learning models exit. One model trains on a group of data, then create pretend videos, whereas the opposite model tries to observe fake ones. The forger creates fakes till the other model can't detect the forgery. The larger the coaching dataset, the simpler it's for the forger to make likely deepfakes.

Figure 4: Original Video vs Deepfake video

5. CONCLUSION

By learning of these analysis articles, we've got gained data concerning the importance of detecting deepfake videos and why it's necessary today to understand additional in detail. a brand new deepfake detection methodologyology is introduced to stop deepfakes. coaching generative adversarial networks (GANs) and ensuant use of components of the generator and individual networks as feature extractors for supervised tasks is one method to make smart image presentations. GANs are a convincing various to most chance techniques. It includes mouldering videos into a frame, detective work faces from real and faux videos, cropping faces, and analyzing them.

ACKNOWLEDGEMENTS

we tend to give thanks to Mr. Anurag Malik, prof for help with [Data mining, Machine learning algorithms], and for comments that greatly improved the manuscript.

REFERENCES

[1] Pavel Korshunov, Sebastien Marcel (2018). DeepFakes: a New Threat? Assessment and Detection. https://arxiv.org/abs/1812.08685.

[2] Akhtar; Dasgupta, D.; Banerjee, B. Face Authenticity: Authenticity of face: An brief of face manipulation generation, detection, and recognition. In affairs of the International Convention on Communication and Information Processing, Chongqing(Municipality in China).

[3] Vezzetti, E.; Marcolin, F.; Tornincasa, S.; Maroso, P. Applying Figure to RGB Images for Facial Landmark Localization - A Primary Approach. Int. J. Biom. 2016, 8, 216–236. [CrossRef].

[4] Zhang; Liu; Tang Multiview facial corner localization in RGB-D images via hierarchical retrogression with double models. IEEE Trans. Circuits Syst. Video Technology. 2014, 24, 1475–1485.

[5] Viola, P.; Jones, M. Quick object discovery using a boosted cascade of simple features. In affairs of the 2001 Institute of Electrical and Electronics Engineers(IEEE) Computer Society.

[6] Bazarevsky, V.; Kartynnik, Y.; Vakunov, A.; Raveendran, K.; Grundmann, M. Blazeface: Sub-millisecond neural face discovery on mobile gpus. arXiv 2019, arXiv:1907.05047.

[7] Zhang; Li, Z.; Qiao, Y. Joint face discovery and alignment using multitask protruded convolutional networks. IEEE Signal Process. Lett. 2016, 23, 1499 – 1503.

[8] Tan; Le. Efficientnet Rethinking model spanning for convolutional neural networks. In affairs of the International Convention on ML, Long Beach, CA, USA, 10 – 15 June 2019; pp. 6105 – 6114.

[9] Rossler,A.; Cozzolino,D.; Verdoliva, L.; Riess, C.; Thies,J.; Nießner, M. Faceforensics Learning to descry manipulated facial images.

[10] Frame Photo, Kaggle DeepFake Discovery Preface.

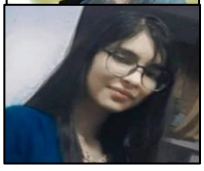
Authors

Anurag Malik[1] Over 20yrs of Teaching Experience . Presently working as an Associate Professor in Computer Science & Engineering department in Moradabad Institute of Technology, Moradabad, U.P. He have guided 5 M. Tech Thesis. and published two books. Area of research includes Data mining , machine Learning and image processing.

Abhishek[2] He had done their B.tech in computer science and engineering in (2018-22) from MIT, Moradabad & Have an experience in development and interest in Java and artificial intelligence.

Aseem Gupta[3] He had done their B.tech in computer science and engineering in (2018-22) from MIT, Moradabad & Have an experience in development and interest in C++,Python and Machine Learning.

Gaurang Gupta[4] He had done their B.tech in computer science and engineering in (2018-22) from MIT, Moradabad & Have an experience in development and interest in machine learning and Game Development.



Iram Rafi[5] She had done their B.tech in computer science and engineering in (2018-22) from MIT, Moradabad & Have an experience in development and interest in Python and artificial intelligence.