ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

DFFMD A DEEPFAKE FACE MASK DATASET FOR INFECTIOUS DISEASE ERA WITH DEEPFAKE DETECTION ALGORITHMS

Dr Aluri Brahmareddy *Associate professor, Department of CSE, Marri laxman reddy institute of technology and management.* brahmareddy475@gmail.com

Dr. Arun Kumar Arigela, *Professor & Head, Department of CSIT Marri Laxman Reddy Institute of Technology and Management (MLRITM), Hyderabad-500043,Telangana, India (A UGC Autonomous Institute).* arun.arigala@mlritm.ac.in

Dr M Nagalakshmi , *Department of Computer Science and Engineering, Marri Laxman Reddy Institute of Technology and Management, Hyderabad, Dundigal -500043, nagalakshmi1706@gmail.com*

Abstract

Deepfake technology, capable of producing counterfeit images and videos by convincingly replacing or fabricating faces, has raised significant societal concerns. Among the dangers posed by this phenomenon are the deliberate creation of fake political news, dissemination of misleading information, fabrication of electronic evidence, and the perpetuation of digital harassment and fraud. The widespread use of face masks during the COVID-19 pandemic has further complicated the detection and generation of deepfakes. This study introduces a novel Deepfake Face Mask Dataset (DFFMD) based on Inception ResNet-v2. It incorporates preprocessing stages, feature-based analysis, residual connections, and batch normalization to address this evolving threat. The findings demonstrate superior accuracy in detecting deepfake videos featuring face masks compared to state-of-the-art methods like InceptionResNetV2 and VGG19. Additionally, the research highlights the effectiveness of combining Convolutional Neural Networks (CNNs) with an extended version of Xception for enhanced deepfake detection. Emphasizing the need for robust techniques to combat the growing sophistication of deepfakes, the study suggests that future work should prioritize iterative experimentation to further improve detection accuracy in an ever-evolving technological landscape.

Keywords: Deepfake, deep learning, CNN, generation, detection, fake videos, neural network, mask, face mask.

Introduction

Blending and altering media content has become easier than ever due to advancements in computer-generated editing systems. This has significantly increased the spread of false information through *deepfakes*, a technology that creates fake videos, modifies existing ones, or even replicates someone's voice using deep learning. With freely available tools such as DFaker, DeepFaceLab, FaceSwap, and FaceSwap-GAN, it has become difficult to distinguish real media from fake. This accessibility highlights the urgent need for AI-powered digital forensics to detect and counter deepfakes effectively.

Existing deepfake detection systems primarily rely on analyzing video frames and their temporal relationships through two-stream Deep Neural Networks (DNNs). One stream focuses on the frame level, dynamically pruning the network to avoid overfitting caused by compression noise. The other examines temporal correlations across video frames. Additionally, a Convolutional Vision Transformer (ViT-CNN) combines Convolutional Neural Networks (CNNs) for feature extraction and Vision

ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

Transformers (ViTs) for classification using attention mechanisms. However, these systems have notable limitations. They are computationally complex, resulting in high training times, and the ViT-CNN approach has a high rate of false positives. Furthermore, the lack of preprocessing steps such as residual connections, batch normalization, and data augmentation negatively impacts overall performance.

To address these challenges, the proposed system introduces an enhanced Inception ResNet-v2 model combined with preprocessing stages, feature-based analysis, residual connections, and batch normalization. It also leverages the newly created Deepfake Face Mask Dataset (DFFMD) to improve the detection of deepfake videos involving face masks, filling a critical gap left by traditional methods. The system evaluates multiple deep learning models, including VGG19, CNN, and an extended Xception architecture, to ensure versatility in model selection.

The proposed system offers several key advantages. First, the DFFMD provides a robust training dataset featuring diverse deepfake scenarios, enhancing real-world applicability. Second, the exploration of various deep learning models ensures scalability and adaptability to different contexts. Finally, the system's design allows it to evolve with emerging deepfake techniques, ensuring continuous innovation in detection methods. By addressing the shortcomings of existing systems and emphasizing adaptability, this approach establishes a strong foundation for reducing the negative impact of deepfakes in an era marked by rapidly evolving digital threats.

Literature survey

The collection of abstracts provides insights into cutting-edge advancements in generative adversarial networks (GANs) and image manipulation detection. The DeeperForensics1.0 dataset introduces a large-scale benchmark for face forgery detection, containing 60,000 videos and 17.6 million frames, making it significantly larger than previous datasets. Generated through an advanced face-swapping framework, the dataset features a secret test set with highly deceptive videos, offering a robust evaluation of five baseline detection methods. StarGAN addresses the challenge of image-to-image translation across multiple domains by using a single unified model, enabling dynamic transformations between diverse datasets and outperforming existing models in terms of translation quality. In contrast, Progressive Growing of GANs introduces a training method that gradually increases image resolution, enhancing stability and image quality while producing high-resolution images such as CelebA at 1024^2 resolution. StyleGAN proposes a novel generator architecture inspired by style transfer literature, enabling unsupervised separation of high-level features like pose and identity, resulting in superior interpolation and image quality. Finally, the First Order Motion Model for image animation presents a framework that animates objects based on motion extracted from driving videos, utilizing learned keypoints and local transformations to synthesize complex movements without prior annotations, achieving success across various object categories and benchmarks. Together, these works demonstrate significant progress in GAN architecture, image translation, and forgery detection.

Methodlogy

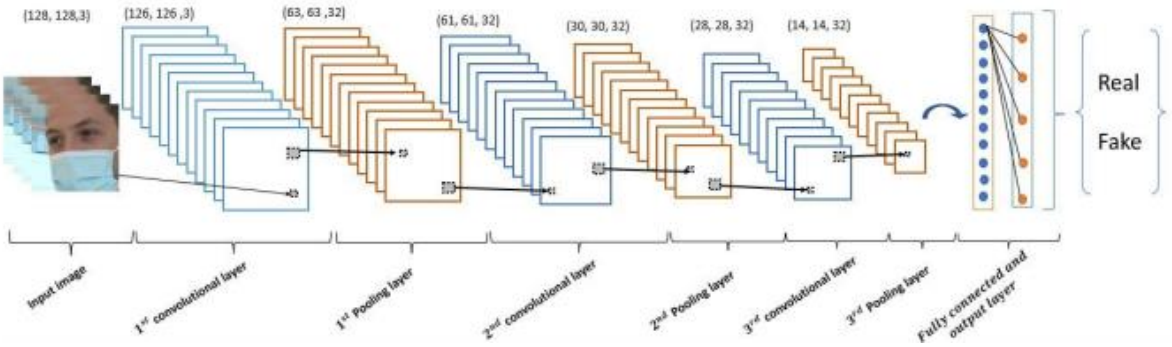
Framework configuration is the most common way of determining the design, parts, and connections inside a framework to fulfill given needs successfully. It includes coordinating, planning, and determining the parts of the framework and their cooperations to give expected usefulness and execution.

System Architecture

Utilizing a total procedure, the proposed Deep fake Face Mask Detection System (DFMDS) design productively distinguishes and decreases the risks related with deep fake recordings showing individuals wearing facial coverings. Based on the Origin ResNet-v2 brain network design, known for extraordinary picture grouping position execution, is the framework Picture normalizing and increase are essential for preprocessing stages intended to work on model strength.

Involving lingering associations for improved slope stream and to limit evaporating angle issues, the design utilizes include based examination to recognize minute examples reminiscent of deep fake control. Speeding up and settling preparing is achieved through cluster normalizing. Extraction of various leveled highlights is for the most part subject to the "Convolutional Neural Network (CNN)", which is additionally fundamental for separating genuine face feelings from deep fake changes. Besides included is an augmentation in view of Xception engineering, taking utilization of its profundity wise distinct convolutions for further developed highlight learning.

Broad testing shows that the framework is more powerful than acknowledged methods like InceptionResNetV2 and VGG19 by goodness of extraordinary accuracy. The mix of CNN and Xception stresses how the two of them influence deep fake identification. Steady improvement and evaluation of the proposed engineering ought to be given first concern in continuous examination projects accordingly ensuring transformation to new deep fake approaches in the powerful mechanical scene. This solid component helps the nonstop battle against advanced control and bogus data in the time of irresistible illnesses.



ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

“Fig.1.System Architecture”

ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

UML Diagrams

Data Flow Diagram

An “Data Flow Diagram (DFD)” offers a graphical portrayal of the framework's information stream. It shows how information passes across numerous frameworks, stockpiling, and outside associations. The chart contains processes that convert input information into yield, data stores where data is kept, information stream ways showing the exchange of information among parts, and outside substances signifying sources or objections of information. DFD saidin makes muddled frameworks more agreeable for examination, plan, and cognizance by displaying the connection between many pieces and representing the overall information handling inside the framework, consequently appreciating the utilitarian highlights of the framework. Figure 2 shows the information stream chart for the recognizing driver drowsiness. Shows graphically the way that information streams all through the framework.

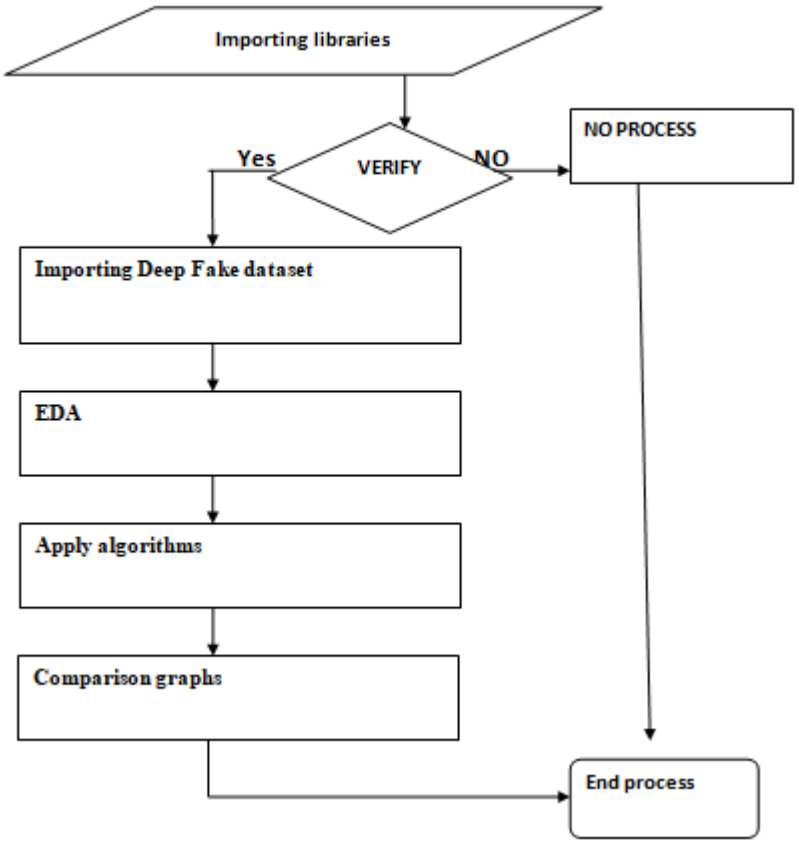
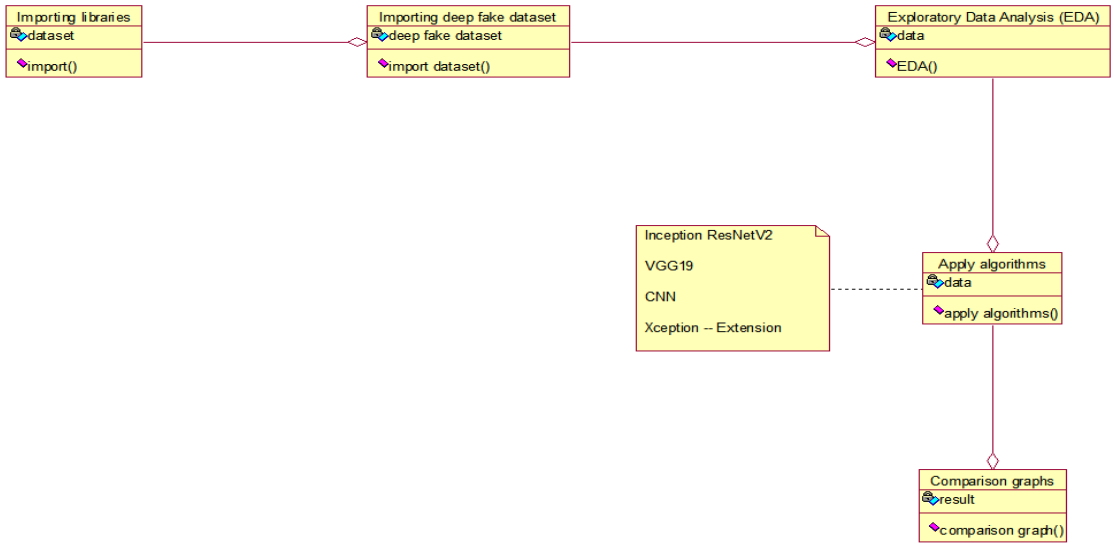


Fig.2.DataFlow Diagram

Class Diagram

By showing classes, their qualities, strategies, and associations, a class outline assists with explaining the structure of a framework. It shows the classes' credits, connections, legacy, and conditions as well as the fixed viewofthesystem's article interactions. Figure 3 shows how a few parts of the driver sleepiness identification framework interface and cooperate outwardly.



"Fig.3. Class Diagram"

Use case Diagram

A utilization case graph shows the collaborations between clients (entertainers) and a framework, thusly representing the many elements or exercises the framework completes to fulfill client targets. It presents entertainers, use cases — functionalities — and their interactions. Figure 4 shows the utilization case graph making sense of the instrument of driver sluggishness identification.

The proposed procedure outlines the development and deployment of an advanced deep fake detection system tailored to scenarios involving face masks. The process begins with the creation of the Deep Fake Face Mask Dataset (DFFMD), ensuring a diverse collection of deep fake videos featuring varied facial expressions, mask styles, and lighting conditions, followed by partitioning the dataset into training and testing sets. Next, the model architecture incorporates preprocessing steps, feature analysis, and residual connections based on the

ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

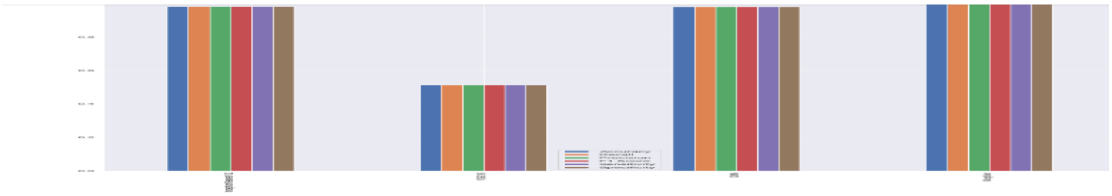
Inception-ResNet-v2 architecture, with enhancements from Xception to boost detection accuracy using CNNs.

During data preprocessing, video frames are refined to enhance facial attribute clarity, pixel values are normalized, and data augmentation techniques expand the training set. The model training phase involves optimizing the detection model using suitable loss functions and optimizers, adjusting parameters based on performance benchmarks. For evaluation, the trained model is tested on a dataset to measure its accuracy in detecting deep fakes with masks, comparing results to state-of-the-art techniques like VGG19 and Inception-ResNet-v2.

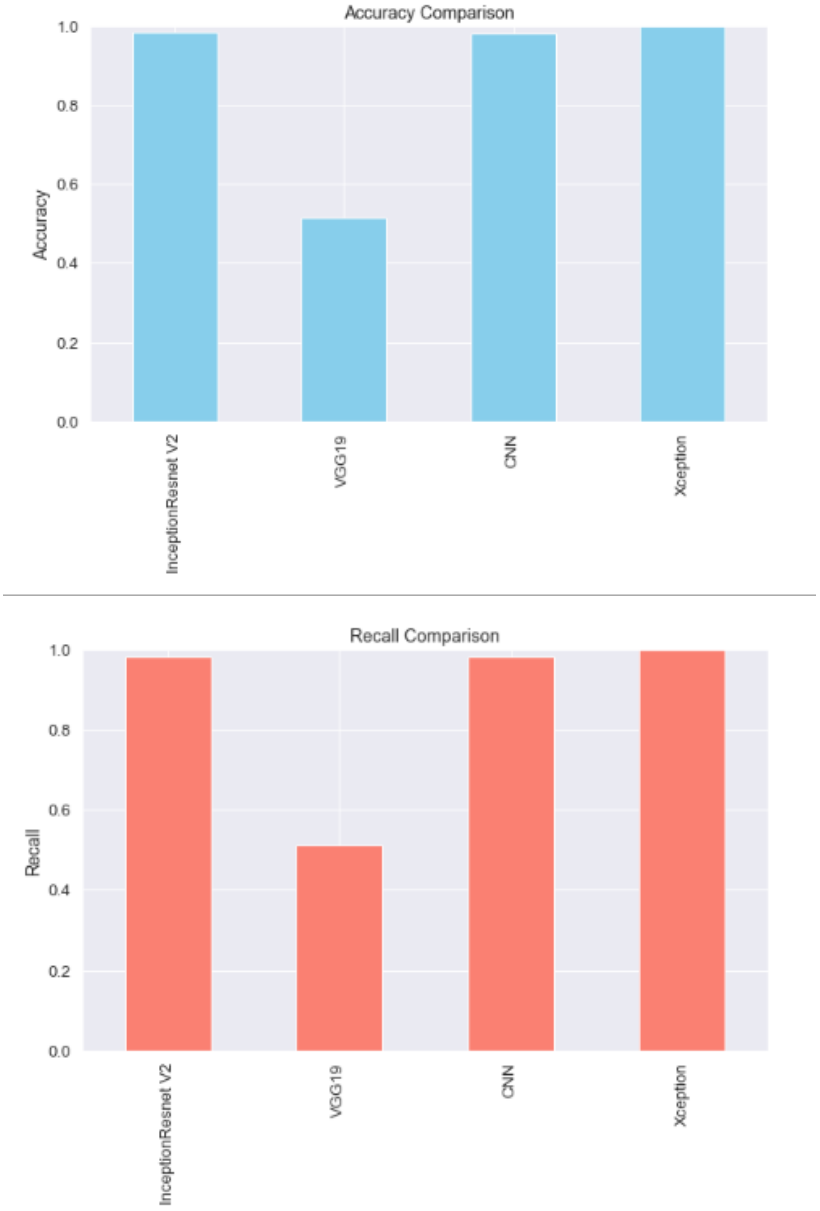
The system integrates CNN and Xception architectures, leveraging the strengths of both for improved performance. Performance metrics such as accuracy, precision, recall, and F1 score are used to assess effectiveness. Optimization and future work involve refining the model based on evaluation results and planning iterative improvements to address evolving deep fake challenges. Documentation covers all implementation details, including dataset sources, preprocessing steps, model architecture, training parameters, and evaluation outcomes. Finally, deployment options are considered for integrating the model into security systems, social media platforms, or content verification tools.

The approach employs advanced algorithms such as Inception-ResNet-v2, known for its 164-layer deep architecture and high accuracy in image classification, VGG19, a 19-layer deep CNN trained on the ImageNet dataset, CNNs for image recognition tasks, and Xception, a 71-layer deep network that excels in classifying diverse objects. Together, these components form a comprehensive framework for detecting deep fakes in masked face scenarios, emphasizing robustness, accuracy, and scalability.

Results and discussion



ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024



CONCLUSION

At last, particularly comparable to facial covering upgraded circumstances during the Coronavirus pestilence, this review handles the dire social issues raised by deep fake innovation. Expanded by “Convolutional Neural Networks (CNN)” and Xception, the recommended “Deep fake Face Mask Dataset (DFFMD)” and the new Beginning ResNet-v2-based strategy show eminent advancement in recognizing modified films. The discoveries of the examination show more precision than traditional strategies, accordingly focusing on the model's adequacy in the troublesome occupation of spotting deep fakes with obstructed

ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

facial qualities. This study gives the establishment to continuous upgrades as innovation creates and underscores the need areas of strength for of to forestall the detestable utilization of deep fakes in our connected society driven by data.

Author publication date: 12-07-2024

ISSN: 0972-2750
Vol-14 Issue-03 No.04: 2024

REFERENCES

[1] F. H. Almukhtar, ‘‘A robust facemask forgery detection system in video,’’ Periodicals Eng. Natural Sci., vol. 10, no. 3, pp. 212–220, 2022.

[2] S. R. Ahmed, E. Sonuç, M. R. Ahmed, and A. D. Duru, ‘‘Analysis survey on deepfake detection and recognition with convolutional neural networks,’’ in Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robot. Appl. (HORA), Jun. 2022, pp. 1–7.

[3] J. Hu, X. Liao, W. Wang, and Z. Qin, ‘‘Detecting compressed deepfake videos in social networks using frame-temporality two-stream convolutional network,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 3, pp. 1089–1102, Mar. 2022.

[4] D. A. Coccomini, N. Messina, C. Gennaro, and F. Falchi, ‘‘Combining EfficientNet and vision transformers for video deepfake detection,’’ in Proc. Int. Conf. Image Anal. Process. Berlin, Germany: Springer, 2022, pp. 219–229.

[5] M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, ‘‘Deepfake detection: A systematic literature review,’’ IEEE Access, vol. 10, pp. 25494–25513, 2022.

[6] L. Jiang, R. Li, W. Wu, C. Qian, and C. C. Loy, ‘‘DeeperForensics1.0: A large-scale dataset for real-world face forgery detection,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020, pp. 2889–2898.

[7] Y. Choi, M. Choi, M. Kim, J.-W. Ha, S. Kim, and J. Choo, ‘‘StarGAN: Unified generative adversarial networks for multi-domain imageto-image translation,’’ in Proc. IEEE Conf. Comput. Vis. pattern Recognit., Jun. 2018, pp. 8789–8797.

[8] T. Karras, T. Aila, S. Laine, and J. Lehtinen, ‘‘Progressive growing of GANs for improved quality, stability, and variation,’’ 2017, arXiv:1710.10196.

[9] T. Karras, S. Laine, and T. Aila, ‘‘A style-based generator architecture for generative adversarial networks,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019, pp. 4401–4410.

[10] A. Siarohin, S. Lathuilière, S. Tulyakov, E. Ricci, and N. Sebe, "First order motion model for image animation," in Proc. Adv. Neural Inf. Process. Syst., vol. 32, 2019, pp. 1–11.

[11] A. S. Uçan, F. M. Buçak, M. A. H. Tutuk, H. İ. Aydin, E. Semiz, and S. Bahtiyar, "Deepfake and security of video conferences," in Proc. 6th Int. Conf. Comput. Sci. Eng. (UBMK), Sep. 2021, pp. 36–41.

[12] N. Graber-Mitchell, "Artificial illusions: Deepfakes as speech," Amherst College, MA, USA, Tech. Rep., 2020, vol. 14, no. 3.

[13] F. H. Almukhtar, "A robust facemask forgery detection system in video," Periodicals Eng. Natural Sci., vol. 10, no. 3, pp. 212–220, 2022.

[14] B. Dolhansky, R. Howes, B. Pflaum, N. Baram, and C. C. Ferrer, "The deepfake detection challenge (DFDC) preview dataset," 2019, arXiv:1910.08854.

[15] P. Yu, Z. Xia, J. Fei, and Y. Lu, "A survey on deepfake video detection," IET Biometrics, vol. 10, no. 6, pp. 607–624, Nov. 2021.