INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1106-1110

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

DEEPFAKE FACE DETECTION USING Machine Learning

Miss. Khushi Vipin Chaudhari[1], Dr. Shrikant V. Sonekar[2]

[1]Department of Master of Computer Application, J D College of Engineering and Management Khandala, Borgaon Phata , Kalmeshwar Road, Nagpur, India-441501
khushichaudhari0406@gmail.com

[2]Department of Master of Computer Application, J D College of Engineering and Management Khandala, Borgaon Phata , Kalmeshwar Road, Nagpur, India-441501
shrikantsonekar@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS39851

ABSTRACT

As the prevalence of deepfake videos continues to escalate, there is an urgent need for robust and efficient detection methods to mitigate the potential consequences of misinformation and manipulation. This abstract explores the application of Long Short-Term Memory (LSTM) networks in the realm of deepfake video detection. LSTM, a type of recurrent neural network (RNN), has proven to be adept at capturing temporal dependencies in sequential data, making it a promising candidate for analyzing the dynamic nature of videos. The research delves into the intricacies of utilizing LSTM architectures for the detection of deepfake videos, emphasizing the significance of understanding temporal patterns inherent in manipulated content.

The proposed methodology involves preprocessing of video data, including the creation of high-quality training datasets and the application of data augmentation techniques to enhance model generalization. The training process and optimization strategies specific to LSTM networks are explored to achieve optimal performance in deepfake detection. Evaluation metrics such as accuracy, precision, recall, and F1 score are employed to assess the model's effectiveness in distinguishing between genuine and manipulated content.

The abstract also addresses challenges and limitations inherent in deepfake detection, including mitigating false positives and negatives, and discusses potential avenues for future research to enhance the robustness of LSTM-based detection systems. The findings of this research have implications for real-world applications, particularly in the context of social media platforms and video hosting services, where the integration of LSTM-based deepfake detection can contribute to a safer and more secure online environment.

Keywords: Deepfakes, Deep Learning, Fake Detection, Social Media, Machine Learning , artificial intelligence, Videos, LSTM

1. INTRODUCTION

Deepfake technology leverages machine learning (ML) to generate realistic but manipulated images or videos of individuals, often replacing one person's face with another's. Deepfake face detection using conventional neural networks

Deepfakes, Generated by sophisticated artificial intelligence algorithms, have the ability to seamlessly replace faces and manipulate audio, blurring the lines between truth and friction. As the technology behind deepfakes advances at an unprecedented pace, the implications for misinformation, identity theft, and malicious content creation become increasingly profound. Machine learning-based deepfake detection focuses on distinguishing real faces from synthetic ones by identifying subtle inconsistencies or artifacts unique to deepfakes. Techniques often rely on convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to analyze video frames for unnatural blinking patterns, unnatural skin textures, or discrepancies in lighting and shadows. Additionally, deepfake detection models use forensic analysis to identify telltale signs like inconsistent eye movements, irregular facial expressions, or abnormal head motions, which can reveal synthetic content. By training these detection models on large datasets of real and fake images or videos, researchers aim to improve accuracy and robustness in detecting sophisticated deepfakes

2. OBJECTIVE

As the prevalence of deepfake videos continues to escalate there is an unguent need for robust and efficient detection methods to mitigate the potential consequences of misinformation and manipulation. This applicaton of long short term memory networks in the realm of deepfake video detection. The objectives of deepfake face detection are multifaceted, primarily aimed at combating the growing threats posed by manipulated media. The primary goal is to accurately detect deepfake videos and images that have been altered or generated using artificial intelligence techniques. This includes distinguishing between real and fake content to prevent misinformation. Deepfakes can be used to spread false information, engage in identity theft, or create harmful narratives. Detecting deepfakes helps mitigate these risks by identifying and flagging manipulated content before it spreads.

System requirement

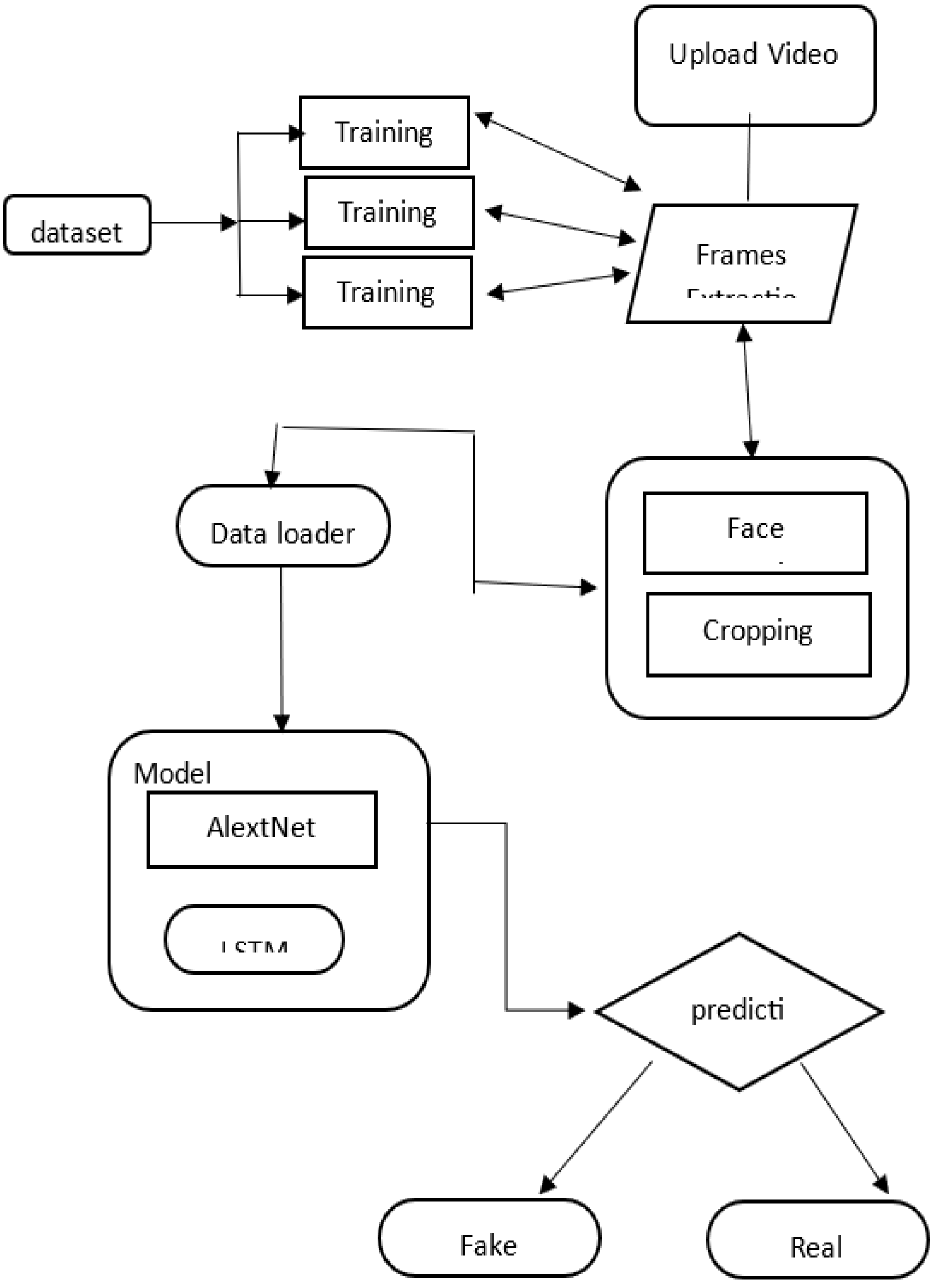
1) Software requirement

- Operating system
- Deep learning Frameworks
- Coding languages:-
  Backend:- python 3.10.9
  Frontend:- html, css, js
  Farmework:- flask
- Web framework

2) Hardware specification

- Processor(CPU)
- Graphics processing unit(GPU)
- Memeoy(RAM)
- Storage
- network

flowchart



related work:-

Sr. no	Paper Name	author	year	Focus of study, design, objective, method used and sample size	Findings of the study and their conclusions	limitations
01	FaceForensics ++: Learning to Detect Manipulated Facial Images	Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, ChristianRis, JustusThies, Matthias Niebner	2019	The rapid progress in synthetic image generation and manipulation has now come to a point where it raises significant concerns for the implications towards society. At best, this leads to a loss of trust in digital content, but could potentially cause further harm by spreading false information or fake news.	This paper examines the realism of state-of-the-art image manipulations, and how difficult it is to detect them, either automatically or by humans	Lack of large-scale, high-quality datasets Limited generalization Evaluation across different manipulation techniques
02	The Deep Fake Detection Challenge (DFDC) Dataset	Brian Dolhansky J. Andonian R. Howes M. Pflaum J. Bitton	2020	Deepfake techniques, which present realistic AI-generated videos of people doing and	Identifying manipulated media is a technically demanding and rapidly evolving challenge that requires collaboratio	Need for Diversity in Fake Video Creation Techniques Limited Availability of Large-Scale

Sr. no	Paper Name	author	year	Focus of study, design, objective, method used and sample size	Findings of the study and their conclusions	limitations
				saying fictional things, have the potential to have a significant impact on how people determine the legitimacy of information presented online.	ns across the entire tech industry and beyond.	Public Datasets
03	Explaining Deepfake Detection by Analysing Image Matching .	Andreas rossler Florian jug Mathias niebner	2022	The process of identifying deep fake content involves a thorough analysis of image matching techniques. By examining the similarities and differences between the original and manipulated images, researchers can develop algorithms that can detect the	This analysis typically involves comparing pixel values, color gradients, and other visual features to determine if an image has been digitally altered	Limitation focus on local image features.

Sr. no	Paper Name	author	year	Focus of study, design, objective, method used and sample size	Findings of the study and their conclusions	limitations
				subtle alterations made in deep fake videos.		

3. CONCLUSION

This article offers a comprehensive survey of a new and prominent technology, namely, DeepFake. It communicates the basics, benefits and threats associated with DeepFake, GAN-based DeepFake applications. In addition, DeepFake detection models are also discussed. The inability to transfer and generalize is common in most existing deep learning-based detection methods, which implies that multimedia forensics has not yet reached its zenith. Much interest has been shown by different important organizations and experts that are contributing to the improvement of applied techniques. However, much effort is still needed to ensure data integrity, hence the need for other protection methods. Furthermore, experts are anticipating a new wave of DeepFake propaganda in AI against AI encounters where none of the sides has an edge over the other.

4. REFERENCES

[1] Zhiqing Guo, Gaobo Yang, Jiyou Chen, Xingming Sun (2021) "Fake face detection via adaptive manipulation traces extraction network" in Computer Vision and image Understanding-Volume 204.

[2] Belhassen Bayar and Matthew C. Stamm (2016) "A Deep Learning Approcen to Universal Image Manipulation Detection Using a New Convolutional Layer in IH & MM Sec 16: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security.

[3] Richard Zhang et al, (2018), "Making Convolutional Neural Networks Shift-Invariant Again" in ICML 2019.

[4] Sheng-Yu Wang, Oliver Wang, Richard Zhang, Andrew Owens, and Alexei A Efros. CNN- generated images are surprisingly easy to spot for now. In IEEE Conference on Computer Vision and Pattern Recognition, 2020.

[5] Carlini, N. and Farid, H. (2020) "Evading deep-fake-image detectors with white-and black-box attacks" in IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops.

[6] Narayan, Kartik, et al. (2023). DF-Platter: Multi-Face Heterogeneous Deepfake Dataset. Conference on Computer Vision and Pattern Recognition (CVPR).

[7] Almutairi, Z. Elgibreen (2022). Review of Modern Audio Deepfake Detection Methods. Algorithms, Vol 15, Issue 5. Academic Journal.

[8] Ilyas, Hafsa, Ali Javed, and Khalid Mahmood Malik (2023).AVFakeNet: A unified end-to-end Dense Swin Transformer deep learning model for audio–visualdeepfakes detection. arXiv:2305.01979v