International Journal Trendy Research in Engineering and Technology
Volume 8 Proceedings of NCCDS-24
ISSN NO 2582-0958

DEEPFAKE DETECTION USING MACHINE LEARNING

Manumitha G P(4PM20IS023)[1], Pragathi V(4PM20IS030)[1], Shreya S S(4PM20IS041)[1],
Swetha B T(4PM20IS046)[1], Mr. Rudresh N C[2],
[1]Students, [2]Asst Professor. *Dept of Information Science & Engineering,*
PES Institute of Technology and Management Shivamogga, Karnataka, India
'Corresponding Author Rudreshnc@pestrust.edu.in'

ABSTRACT

This study focuses on using machine learning to spot deepfake content, which are manipulative videos or images often created with malicious intent. We employ advanced computer algorithms that deepfake detection system using Convolutional Neural Networks (CNNs) using a collection of fictitious photos and videos is a critical endeavor in the face of increasing concerns about manipulated media content. To identify subtle differences in deepfakes that set them apart from real media, like unnatural facial movements or audio inconsistencies. Through extensive training and testing, our method proves effective at accurately detecting these deceptive creations, offering a valuable defense against the spreadof misleading or harmful digital content. For example: Sometimes people make videos that look real, but they are not. We taught computers to see the mistakes in these fakes, like weirdfaces or voices. Our method works well at finding these tricky fakes, which helps keep the digital world truthful and safe.

Keywords – Deepfake, Convolutional Neural Network (CNN), Manipulative images, Trans Net, Recurrent Neural Network (RNN)

I. INTRODUCTION:

Convolutional Neural Networks (CNNs) serve as the foundational component in thecomplex and critical domain of deepfake detection. In the specific context of detecting deepfake content within images and video frames, CNNs assume an important part in the categorization and analysis of media data. In today's digital world, where the lines between reality and deception have blurred, the rise of deepfake technology poses a significant challenge. Deepfakes are highly convincing takes videos or images, often created with malicious intent. To combat this growing threat, we turn to the power of machine learning. Using advanced computer algorithms, we teach computers to become digital detectives, discerning between genuine content and these skillfully crafted illusions. This introduction explores the cutting-edge field of deepfake detection,

where technology becomes our companion in preserving the integrity of digital media in an increasingly deceptive world.

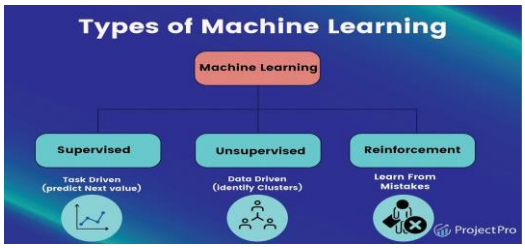

Fig 1: Types of Machine Learning

Deep fake is a human image generation technique that utilizes neural network techniques such as CNN (Convolutional Neural Network). These technologies use deep learning to superimpose target pictures onto source movies, producing a realistic-looking deepfake video. It is hard to recognize differences with the unaided eye in these deeply simulated videos because they are so lifelike. We present a novel deep learning approach in this study that can successfully discriminate between artificial intelligence (AI)-generated phony videos and actual videos. One of the most effective ways we have found to differentiate between pristine and deep fake videos is to take advantage of the limitations of the equipment used to create them. Despite the fact that currently available deep fake creation gadgets may not be obvious to humans, they leave behind some distinct artifacts in the frames that trained neural networks may detect during the fabrication process. We demonstrate that Convolution Neural Networks can effectively capture the distinctive artefacts

generated in the Deep Fake videos produced by Deepfake generation techniques. Our approach extracts frame-level characteristics using a Res-Next Convolution Neural Network. After that, a based convolution Neural Network (CNN) is trained using these features to figure out whether or not the video has been altered, or if it is a deepfake or authentic video. We indicated testing our approach on a sizable collection of deepfake motion pictures gathered from several online video portals. We made an effort to improve the performance of the deep fake detection model using real-time data. We used a variety of accessible datasets to train our model in order to accomplish this. in order for our model to acquire the features from various types of photos.

II. METHODOLOGY:

- When utilizing machine learning to detect deepfakes, models are usually trained on big datasets of both natural and manipulated material.
- These models acquire the ability to identify patterns and characteristics that set real content apart from counterfeits.
- The techniques, like convolutional neural networks (CNNs), is commonly used toanalyze image and video in the dataset.
- Researchers are seeking ways to improve deepfake detection's accuracy and efficiency by iteratively upgrading these models.

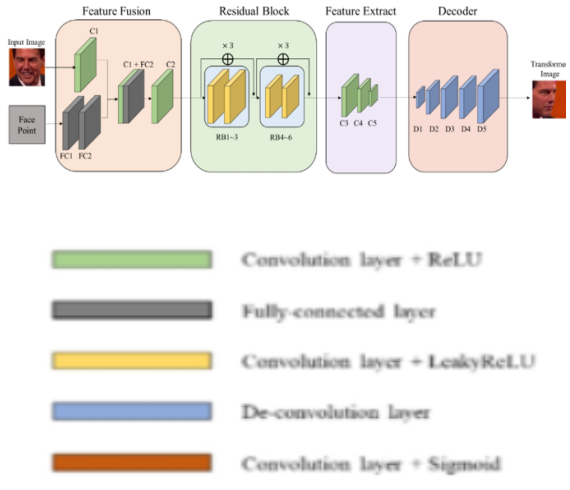

Fig:2 Methodology

The research paper suggests an efficient architecture In order to boost angle conversion and face replacement. With angled switching of faces in face de-identification, there is visual distortion that this ATFS framework seeks to correct. Using generative adversarial networks as a the basis, TransNet and SWGAN were presented for the ATFS framework. TransNet incorporates the anticipated face points in its neural network reconstruction of pictures. Transnet can therefore identify the target's face characteristics and produce multi-angle influenced shots in order to accomplish angle transformation. To extract characteristics from the input picture and replace the input image's face area with the target image to achieve face de-identification, the SWGAN uses a complex neural network that includes self-attention modules with residual operations. To correctly expedite the training process and train the neural network, TransNet and SWGAN both use discriminators and different loss functions. The findings of the experiment indicate that, in contrast to earlier suggested techniques, the suggested method may preserve high-quality photos and prevent image distortion when face swapping is done for image angle adjustment.

III. PROPOSED METHODOLOGY:

- **Data collection:** It involves gathering a diverse dataset of both real and fake media samples, including images, videos where the Real content is sourced from various sources
- **Data preprocessing:** It is essential to standardize formats, align facial landmarks, and remove inconsistencies, ensuring the dataset is well-prepared for training.
- **Model training:** Training takes place on the prepared dataset using the chosen deep learning model, which is usually a Convolutional Neural Network (CNN). Data augmentation techniques are applied to enhance the dataset's diversity and the model's robustness. This phase is critical for teaching the model to recognize patterns and anomalies associated with deepfake content.
- **Performance evaluation:** Using known metrics like accuracy, precision, and recall, the model's performance is assessed once it has been trained. These metrics give us information about how well the algorithm works to differentiate between real and deepfake content. The goal is to maximize the accuracy of detection while minimizing false positives and false negatives.

IV. OBSERVATIONS:

To apply the techniques to accurately identify and mitigate the harmful effects of deepfake media.

To create a deep learning model that can effectively discern between a genuine video and a deepfake.

V. RESULTS:

- The deepfake detection enhances ability to identify manipulated content withinimages and videos

- It serves as a crucial defender of media authenticity, helping to safeguard the publicagainst the dissemination of misinformation, fake news and deceptive narratives.

VI. CONCLUSION:

Deepfake has grown in widespread acceptance with so many photos and videos readily available on social media. This is especially critical given that deepfake creation tools are getting easier to obtain and social media platforms make it simple for users to share and disseminate these kinds of phony materials. In several fields, deep learning techniques have drawn a lot of attention. To effectively detect phony photos and videos, a number of deep learning-based techniques have been put out recently. In these days, deepfake detection is essential and requires sophisticated detection algorithms since it will get harder to identify deepfakes in the future. Deepfakes can have a significant influence on society and politics, hence efforts to identify them should be continually improved.

REFERENCES:

- Asad Malik, Minoru Kuribayashi, Sani M, Ahmad Neyaz Khan″ Deepfake Detection for Human Face Image and Videos: A survey", IEEE,2022.
- Yogesh Patel, Sudeep Tanwar, Rajesh Gupta, Pronaya Bhattacharya, Srinivas Aluvala, Vrince Vimal."Deepfake Generation and Detection: Case Study and Challenges",IEEE,2022.
- Barni, Mauro, et al. "CNN Detection of Gan-Generated Face Images Based on Cross BandCo-Occurrences Analysis." IEEE Workshop on Information Forensics and Security, 2 Oct. 2020. https://arxiv.org/abs/2007.12909
- International Journal of Advanced Trends in Computer Science and Engineering

"Deepfake Video Detection Using Convolutional Neural Network" Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhidkar, Saurabh Agrawal Shri Ramdeobaba College of

- Engineering and Management, Nagpur, Maharashtra, India
- Karen Simonyan and Andrew Zisserman, "Very Deep Convolutional Networks for Large –Scale Image Recognition", ICLR 2015, arXiv:1409.1556v6 [cs.CV] 10 Apr 2015.
- Younus, M. A. and Hasan, T. M. (2020). Effective and fast deepfake detection method based on haar wavelet transform, pp. 186–190.
- S.-Y. Wang, O. Wang, R. Zhang, A. owens and A. A. Efros, "CNN-generated images are surprisingly easy to spot… for now", Proceedings of the IEEE/CVF Conferenceon Computer Vision and Pattern Recognition, pp. 8695-8704, 2020.
- N. Bonettini, E. D. Cannas, S. Mandelli, L. Bondi, P. Bestagini and S. Tubaro, "Video face manipulation detection through ensemble of cnns", 2020 25th International Conference on Pattern Recognition (ICPR), pp. 5012-5019, 2021.
- S. Albawi, T. A. Mohammed and S. Al-Zawi, "Understanding of a convolutional neural network", 2017 International Conference on Engineering and Technology (ICET), pp. 1-6, 2017.