iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61190

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Deep Neural Networks for Multimedia Forensics: Detection of Deepfake Content

Mrs. T.Ganga Bhavani[1] , D S Achyutha Sailendra[2], S D S K P Subrahmanyam[3], Gunnam T V S M Shyamal[4], Kakarla Mohana Krishna[5]

[1]*Assistant Professor* , [2, 3, 4, 5] *B.tech Students Department of Information Technology, Pragati Engineering College, Surampalem , Andhra Pradesh, India*

Abstract: ***"Deepfakes" are digital manipulation techniques that use deep learning to create false photos and movies. The most difficult component of obtaining the original is detecting deepfake photographs. Because deep fakes are becoming more widely known, it is critical to distinguish original photographs and videos in order to identify manipulated films. This project investigates and tests several methods for detecting between genuine and fake photographs and movies. Deep fakes were recognized using the Convolutional Neural Network (CNN) approach known as Inception Net. In this research, a comparative comparison of many convolutional networks was performed. This project takes use of a Kaggle dataset containing 3745 images generated during the augmentation process, as well as 401 videos of train samples. The accuracy and confusion matrix metrics were utilized to evaluate the outcomes. The proposed model exceeds the others in terms of accuracy, detecting deepfake photographs and videos with a 93% rate.***

Keywords: Deepfake, Inception net, CNN (Convolutional Neural Network), Vision Transformers

I. INTRODUCTION

Because of the prevalence of cell phones and social media platforms, deepfake videos have become readily available. These devices have produced fake news and films that are considered damaging to society. Terrorist groups also create misleading photographs and films in order to harm the government and disgrace the global people [1]. The world shrank as a result of growing globalization and virtualization, but it also brought nonstate threats to the country in the form of bogus videos, the radicalization of devotees of other religions, and agenda-setting. Many well-known people fell prey to this fraud and suffered a variety of consequences as a result of the bogus images and videos [2]. The most identifying feature of humans is their face. The security risk posed by face control is becoming increasingly significant as face blending innovation advances at a rapid pace. Human faces can frequently change depending on how someone looks at them. This is achievable since numerous computations use deep learning innovation to generate realistic and authentic human faces. A growing subgenre of counterfeit insights innovation enables any person's face to be recognized as the genuine face of another [3]. The twenty-first century has seen a faster-than-ever spread of deepfake content. Techniques for recognizing bogus videos masquerading as authentic are becoming increasingly important as the frequency of deepfakes grows. In this journal [4], we will look into more technologies for detecting deepfake pictures. The emergence of social networking sites and smartphone culture in recent decades has increased the appeal of digital photos and videos. This study examines various types of vision transformers for inception net performance. It is used to determine the accuracy percentage and the most appropriate and accurate method of discriminating between legitimate and deepfake videos [5].

II. LITERATURE SURVEY

A detailed study of the literature on deepfake detection models and ways for upgrading current strategies was conducted on the relevant papers. A review of the literature is undertaken on various data mining approaches. The connected papers reviewed in this study are discussed in the section that follows. Nishat Tasnim Roza et al. reported a comparison of the deepfake image detection algorithm using a convolutional neural network in 2021. They reported the following conclusions from their research. Human faces have many different characteristics in nature. Revolutionary AI subduals such as "deepfake videos" or "deepfake images" replace a person's face with another's. The deepfake images' pixels, skin tones, and facial features collapsed, resulting in false visual defects that were invisible to the naked eye. Deepfake can be used for sounds, photos, and videos. Advances in technology have rendered deepfake photographs practically indistinguishable from real ones. As a result, people all across the world face inevitable obstacles [1].

Using MTCN, Kaipeng Zhang et al. (2016) proposed cooperative face detection and alignment. They reported the following conclusions from their research. Many face systems, like face reputation and facial feature analysis, rely on the detection and alignment of phony faces. However, the huge visible face versions, with their occlusions, large pose versions, and unduly intense lighting, create extreme demands on those jobs in real-world global systems. The cascade face detector suggested AdaBoost and Haar-Like functions for training cascaded classifiers, resulting in genuine overall performance and real-time efficacy. Nonetheless, some research suggest that even with improved functions and classifiers, this detector could worsen dramatically in real-world global programs with large visible versions of human faces. To obtain optimal overall performance, combine deformable element models (DPM) for face identification with the cascade structure. However, they demand high estimating rates and may necessitate costly annotation during the training phase. Convolutional neural networks have lately made significant progress in a variety of computer vision tasks, including picture categorization and facial recognition. Many CNN-based face identification approaches have recently been released, driven by the network's excellent performance in computer vision tasks.

Yang et al. train deep convolution neural networks to learn facial reputation features that generate excessive reactivity in face regions, which results in candidate home windows for faces. However, because of its complex CNN structure, this strategy takes time to implement in practice. Li et al. use cascaded CNN for face identification; however, they ignore the fundamental link between bounding regression and facial landmark localization, necessitating bounding field calibration from face detection at a higher estimation rate [3].

In 2015, Christian Szegedy et al. proposed Going Deeper with Convolutions. They reported the following conclusions from their research. They claimed that in the last three years, developments in deep learning had resulted in considerable improvements in their item classification and detection abilities. Increasing improvement in statistics is not always the product of larger data sets, more powerful equipment, or more stylish designs; rather, it is mostly the outcome of cutting-edge concepts, algorithms, and improved community architectures. For example, no new statistical statements have been made based on the top entries in the competition, with the exception of the same class of competition for identification. According to their findings, Google Net has to be given with 10 times fewer parameters than the Krizhevsky structure that won years ago while remaining much more accurate. In terms of item detection, the highest profits come not from larger networks and more utilities, but from deep architectures and older laptops, similar to the CNN set of rules via Girshick. Along with the ongoing cellular and calculated embedded issues, there is another outstanding one: the algorithm's performance, notably its strength and memory, pays dividends. The primary causes of concern are the deeply structured layout provided on the note covered issue rather than the maximum in the trial, and the designs created to maintain estimation finance by 1.6 multiplication of billions that provide by correct time, so that it is now used and will no longer be limited to educational curiosity but will be used for real-world applications worldwide, even on large data files, at a reasonable cost.

This statement highlights green neural, a deeper community structure in laptop vision that Lin et al. mentioned in a community paper, as well as the well-known deeper net meme that they hope to disseminate. In their context, the term "deep" has several meanings: first, it alludes to both the experience of a brand-new business stage and the more direct experience of a multiplied community [2]. As a result, the majority of the literature study focuses on methods for gathering data from news articles and Twitter, structuring it appropriately, and performing operations to establish the user's purpose. They have not, however, focused on the method used to categorize the content of the news tweets.

III. SYSTEM ANALYSIS

A. Existing System

Deepfake detection methods frequently use convolutional neural networks (CNNs), which may include pre-trained InceptionNet models. Wide-ranging datasets are required for system development, including training and testing. Some systems include temporal consistency checks, audio analysis, and facial landmarks to improve detection accuracy. These applications commonly use open-source frameworks and libraries such as TensorFlow and PyTorch. Using the model in a video processing pipeline enables the detection of deepfakes in real time. Because deepfake-generating algorithms are always evolving, continuing research and development is required. The system's performance can be upgraded and improved by leveraging existing resources and collaborating with subject matter experts.

DISADVANTAGES OF THE EXISTING SYSTEM

1) *Adversarial Attacks:* Deepfake creators constantly adapt their strategies to evade detection, creating a game of cat and mouse. Current systems may struggle to keep up with emerging approaches for making deepfakes.

2) *Generalization:* If the training dataset is insufficiently diverse, deepfake detection models may fail to effectively detect innovative and previously unknown varieties of deepfakes.
3) *Computational Intensity:* Deepfake detection can need a significant amount of processing power, making it challenging to deploy in real time on devices with minimal resources.

B. *Proposed System*

Our system proposal, titled "Deepfake Face Detection Using Deep InceptionNet Learning Algorithm," seeks to solve the drawbacks of current techniques. We intend to employ an upgraded deep learning technique that integrates several cutting-edge CNN architectures with InceptionNet. To improve generalization, we will curate a diverse collection of both actual and deepfake content. To boost detection accuracy, our system will employ multimodal analysis, which will include auditory and facial landmarks. Priority will be given to real-time processing capabilities, which will enable the speedy detection of deepfake data in video streams. To decrease biases, we will focus on the model's explainability and fairness. While respecting privacy and ethical considerations, our system's effectiveness against evolving deepfake techniques will be ensured through periodic improvements and close collaboration with the research community.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

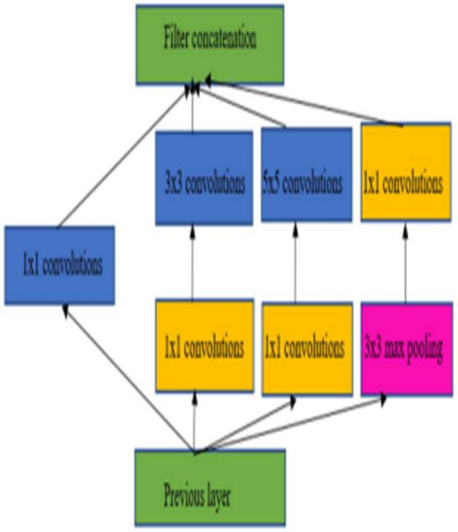


Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

MODULES

1) *Data Preprocessing*

Collecting and structuring a wide range of real and deepfake content.
Data augmentation aims to increase the dataset's diversity.
Preparing images and videos in preparation, including downsizing and normalization.
Feature extraction is performed using deep learning architectures such as InceptionNet and other CNN models.
Obtaining auditory and facial landmarks to increase detection accuracy.

2) *Model Training*

Train the deepfake detection model on the preprocessed dataset.
Optimizing and modifying the selected CNN architectures.
verifying that the model is applicable to various deepfake scenarios.

3) Real-time analysis

Implementing a pipeline for evaluating videos in real time in order to detect deepfakes.

Creating a natural user experience for real-time communication.

Fairness and ethical considerations include implementing bias detection technologies to ensure equitable performance for all demographic groups.

addressing privacy concerns while also considering the ethical implications of deepfake detection.

VI . RESULTS AND DISCUSSION

The datasets utilized in this paper are the Deepfake Detection Challenge (DFDC) and the Face Forensics dataset. This dataset contains 30 GB of movies (5000 total) for the face forensics dataset and 470 GB of films (124000 total) for the DFDC dataset. Each stage generates a separate version of the dataset. Face forensics++ was also used to conduct tests that involved comparing different generated photographs from various data sources. Aside from Deep Fakes, the employed architecture outperforms traditional architectures when applied to several sub-datasets of Face Forensic++. This is likely owing to the network's increased ability to generalize about extremely particular deepfakes.

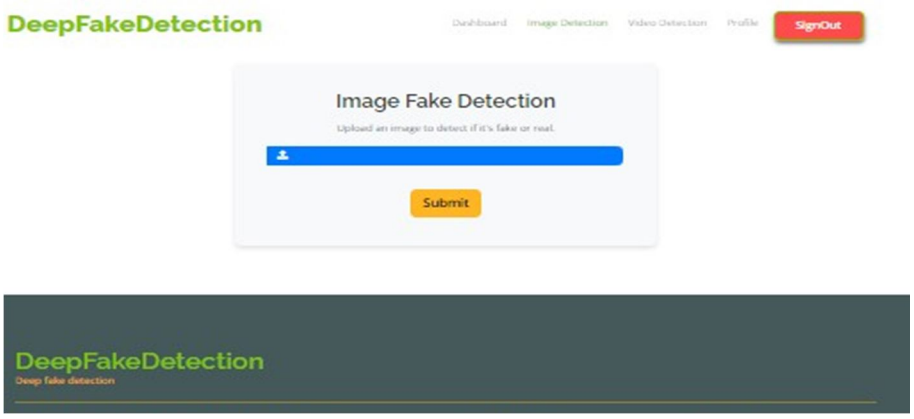


Fig 2.Image based Deep Fake Detection

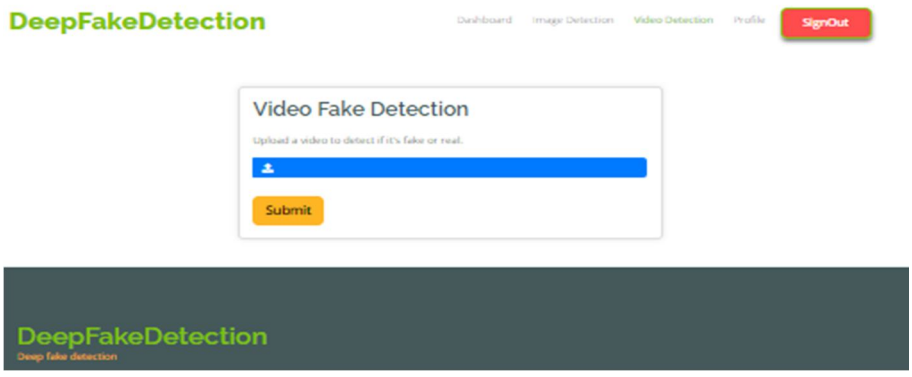


Fig 3.Video based Deep Fake Detection

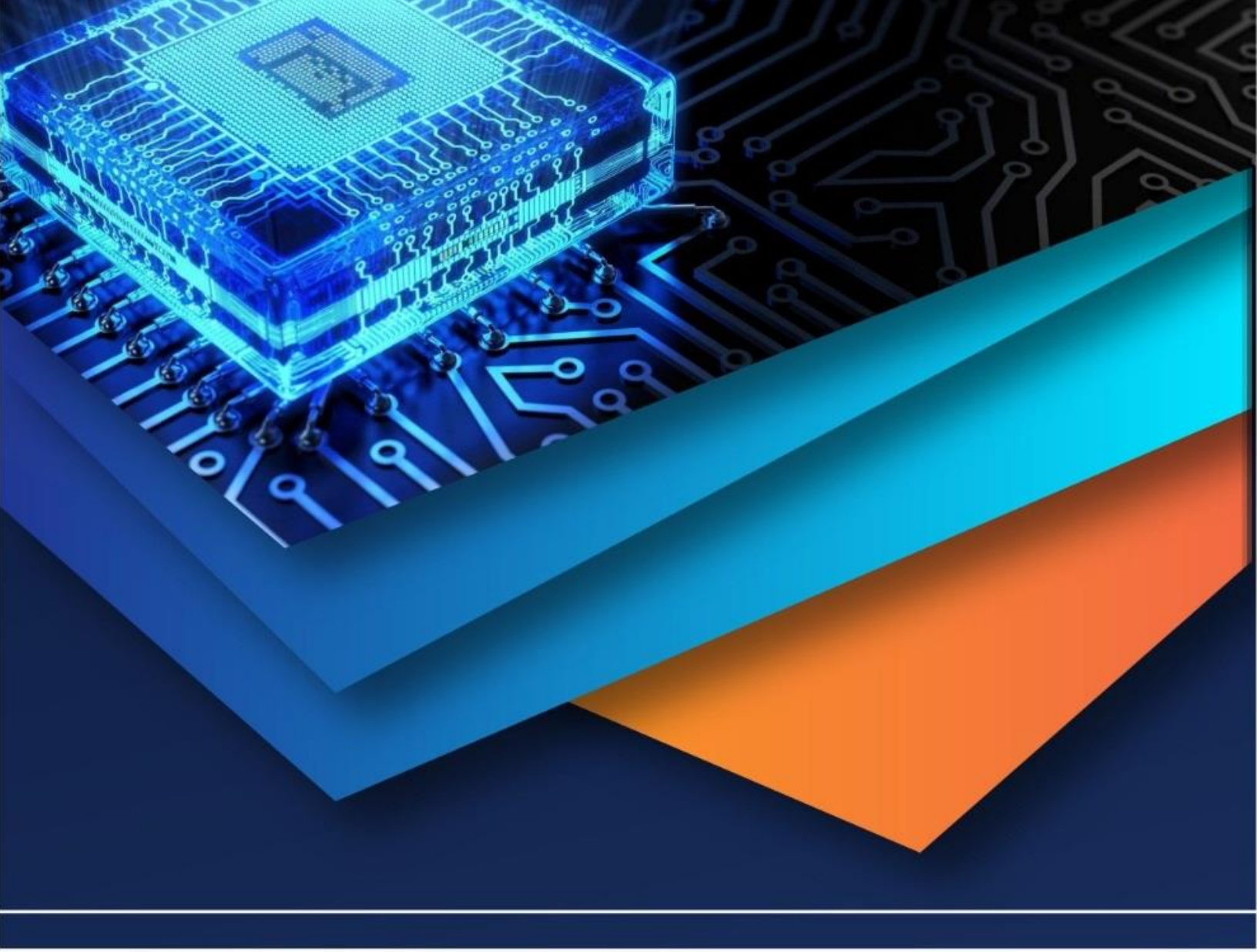
VI. CONCLUSION AD FUTURE WORK

The bogus faces in this study were detected using the Inception Net architecture. Various transition types in real images are used, together with test factors such as the number of key locations in the image, the comparison rate, and the amount of time required for each method to run. According to this report, the overall accuracy of the DFDC dataset is 93%. This work uses different convolutional layers to categorize deepfake recordings from various sources. As a result, the contributions of this research will surely help to reduce coercion and misleading records in our society. The suggested work was completed faster than the previous work, and it was quite effective at distinguishing between legitimate and fake photographs.

The suggested work's accuracy percentage in the DFDC dataset was 93%. It could eventually be expanded to identify deepfake face photographs using various classifiers and distance metric measurements.

REFERENCES

[1] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint face detection and alignment using multitask cascaded convolutional networks. IEEE signal processing letters, 23(10), 1499-1503.
[2] Mordvintsev, Alexander, Christopher Olah, and Mike Tyka. "Inceptionism: Going deeper into neural networks." (2015).
[3] Badale, Anuj, et al. "Deep fake detection using neural networks." 15th IEEE international conference on advanced video and signal-based surveillance (AVSS). 2018.
[4] Dosovitskiy, Alexey, et al. "An image is worth 16x16 words: Transformers for image recognition at scale." arXiv preprint arXiv:2010.11929 (2020).
[5] Bayar, Belhassen, and Matthew C. Stamm. "A deep learning approach to universal image manipulation detection using a new convolutional layer." Proceedings of the 4th ACM workshop on information hiding and multimedia security. 2016.
[6] Ioffe, S., & Szegedy, C. (2015, June). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In International conference on machine learning (pp. 448-456). PMLR.
[7] Chen, Chun-Fu Richard, Quanfu Fan, and Rameswar Panda. "Crossvit: Cross-attention multi-scale vision transformer for image classification." Proceedings of the IEEE/CVF international conference on computer vision. 2021.
[8] Heo, Young-Jin, et al. "Deepfake detection scheme based on vision transformer and distillation." arXiv preprint arXiv:2104.01353 (2021).
[9] Zhang, Kaipeng, et al. "Joint face detection and alignment using multitask cascaded convolutional networks." IEEE signal processing letters 23.10 (2016): 1499-1503.,



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY