International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Deepfake Video Detection Using Eye Movement,Ear Variance and Blink Pattern Analysis

Dr.Radhika K R
Professor
Dept.Of Computer Networking B.M.S College of Engineering, Bangalore, India

Nikhil A M
Dept.Of Computer Networking
B.M.S College of Engineering
Bangalore, India

***Abstract*—The emergence of the digital media has enabled manipulated information like deepfakes to be more prevalent and difficult to identify. Such fake but realistic videos and images are of great concern to such aspects as security, privacy, and misinformation. The project aims at the creation of an effective and trustworthy deepfake detection framework based on machine learning and analysis based on the biometric.The algorithm is a combination of learning algorithms and the facial feature extraction to determine the presence of subtle inconsistencies, which would otherwise be unseen by the human eye. The system is also trained to differentiate between original and manipulated content by studying them based on the patterns of facial movements, irregularity of texture and inconsistency of space. The model is constructed with the help of a systematic dataset and tested in terms of accuracy and performance indicators.The importance of this work is that it has relevance in practice. Rather, the project employs available and not a complex or highly specialized approach to undertaking the project, but techniques that can be adopted and enhanced in the future. The findings indicate that meaningful detection performance could be obtained even when a relatively simple setup is involved.In sum, the given project demonstrates the ability of machine learning to be used to address practical issues such as deepfake detection. It also leaves the possibility to make future advances, like larger datasets and more complex models to make it more accurate and robust.**

Keywords*—Deepfake Detection, Machine Learning, Facial biometrics, Convolutional Neural Network (CNN), Image Processing, Feature Extraction, Computer Vision, Digital Forensics, Face Recognition, Deep Learning.

I. INTRODUCTION

Digital content has been of invaluable importance to the lives of people in the past few years; however, this is in the realms of social media and entertainment rather than education and communication. Coupled with this growth have also been a further growth in false media, mostly in deepfakes. Deepfakes are the kind of videos and images are produced or edited and appear very realistic and no one can distinguish what is exactly on the video and what is fake. Despite the positive purpose of the deepfakes technology in such areas of our life as filmmaking and VR, the technology does raise certain very serious questions about the security, privacy, and information misrepresentation. The greatest issue of deepfakes is that they are so believable. Simple inspection or simple analysis are the traditional methods of identifying the fake media, which is no longer adequate. As a result, there is an increased demand to have automated systems that have the ability to detect manipulated content. It is here that machine learning, and biometric analysis enter in. It is through such methods that systems can obtain patterns and detect minor differences in faces, expressions, and movements which are difficult to discover by humans.

The objective of the project is to develop a deep fake detector project according to machine learning models and face biometric features. The idea is to analyze the visual data such as facial features, details in texture and consistency of movements as a way of assuming the authenticity of a video or an image or the fact that it is a counterfeit one. The system is also trained on a sample of genuine and fake samples in terms of which the system learns to recognize the contents with an improved accuracy.

The concept of this work is to come up with an effective and practical solution that can be transferred into the actual life scenario. The project will not involve very complex methods, rather emphasis will be laid on simplicity vis-a- vis performance which will be easier to understand, implement and develop.

Overall, the specified project might be regarded as one of the solutions to the eradication of the growing menace of deepfakes, yet the manifestation of the application of machine learning as the tool of addressing the modern problem related to the verification of digital media.

II. RELATED WORK

The subject of detecting deepfakes has become the focus of much discussion in the past several years due to the explosive popularity of the generative models category and the growing use of synthetic media. In order to manage this problem, scientists have explored a wide range of techniques, both the classical machine learning techniques and more recent deep learning techniques.

These techniques were grounded on the characteristics that were hand-made such as texture irregularities, color incompatibilities, and unnatural movements of the faces. They have given some initial success, however, they often fail to perform well when using high-quality deepfakes, since current generation techniques have been increasingly refined.

The advent of deep learning has now made convolutional neural networks (CNNs) a widely used method of detecting deepfakes. A series of experiments has demonstrated the CNN-based models can be used to acquire complex patterns and distinguish between actual and fake images with the help of spatial features analysis. Other works have involved utilizing temporal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

information of videos to record inconsistencies in the facial expression and movement across frames as well. These methods are more accurate in detection but normally require enormous inputs of data and calculations.

Subsequently, other researchers have studied the use of physiological correlates of detection and face recognition. These techniques look at finer details of the blinking pattern of the eyes, head movement, and facial landmarks, which can not be reproduced well in the manipulated content. This has enabled researchers to get better results when biometric features are combined with machine learning classifiers, especially in detecting high-quality deepfakes.

Despite these being made, there still are several challenges. The existing majority of existing models are not effective in the generalization when applied to unseen data or when applied to other variants of methods of deepfaking. Moreover, some of the techniques are too complex and their implementation is not easily achieved in an actual situation where limited resources exist.

In this respect, the proposed work will develop a more efficient and convenient deepfake detector by combining facial biometric recognition with machine learning approaches. It is based on the achievement of the accuracy and simplicity balance and part of the constraints experienced in the current approaches is addressed.

III. Proposed Methodology

The proposed system is focused on determining the images and videos of deepfakes through the fusion of the facial biometrics and machine learning algorithms. The overall approach is to be simple, effective and workable and still capable of tracking out the small inconsistencies that transpire in a manipulated text.

It begins with the input information that is the collection of the actual and fake pictures or video frames that are recalled in an organized arrangement. Any raw data tends to contain certain noise and fluctuation and therefore preprocessing stage is undertaken to improve quality and consistency. It includes scaled down pictures, equalization of pixel values and a division of video details into distinct frames where necessary. These steps help in ensuring that the data is of appropriate type and that can also be analyzed further.

Face detection comes after the preprocessing so that the system can isolate the region of interest. It is also a drastic step, considering that the facial components are largely influenced by deepfake manipulation. The face is detected and the significant face features and landmarks such as mouth, nose and eyes are extracted. These are biometrical indications that are highly used in detecting anomalies that can be employed to indicate manipulation.

The processed data then enters a machine learning model after extraction of the features. In this project, a learning based strategy is used to train the model on actual- and fake-samples. Patterns which the model is trained to recognize are texture anomalies, unnatural motions of the face, and spatial deformities. It will eventually be able to identify the real content and deepfakes more efficiently in the long term.

The training phase may be regarded as the one that performs the task of feeding the model on the labeled data and adjusting the parameters to minimize the number of classification errors. Test data is used to test the model to evaluate its performance upon training. Measures such as accuracy are used to find how far the system is capable of making predictions on, previously unknown, inputs.

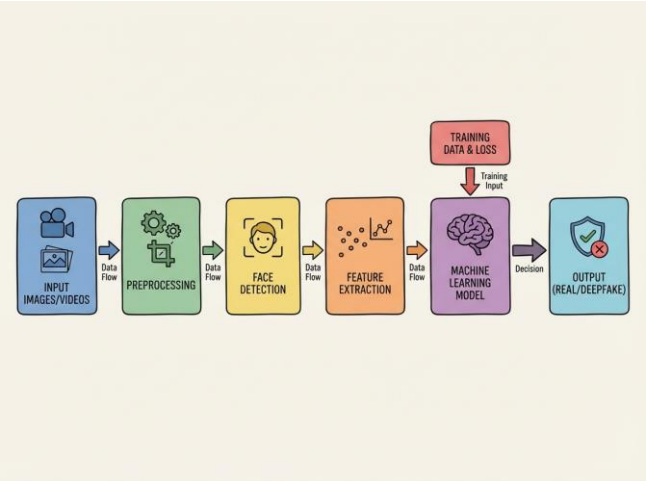

Fig 1.Architecture Diagram

A. Algorithm: Deepfake Detection Framework

Input:
Dataset of images/videos X={x1,x2,...,xn}

Output:
Trained Deepfake Detection Model *M*

1. **Initialize** face detector F_d, feature extractor F_e, and model M
2. **PreprocessData:**
   For each $x_i \in X$:
   - Detect face $f_i = F_d(x_i)$
   - Normalize and resize image
3. **Extract Features:**
   $z_i = F_e(f_i)$
4. **Train Model:**
   - Predict $\hat{y}_i = M(z_i)$
   - Compute loss:

$$L = -[y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)]$$

- Update model parameters

5. **EvaluateModel:**
   Compute accuracy, precision, recall, F1-score
6. **Prediction:**
   For new input x_t, classify as **Real or Fake**

Finally, the system produces an output indicating the authenticity of the presented input or not. These modules are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

expected to constitute the entire workflow, and in the future, more complex models can be incorporated or more data can be added.

Overall, the suggested methodology is rooted in a mediocre compromise - to combine both the biometric and machine learning and create a robust and scalable deepfake detection system.

IV. Dataset and Pre-processing

The quality and preparation of the data to be used in the training and evaluation is the most crucial aspect of this work. In this project, a set of both genuine and fake images (video frames, in case it is a video) is used to ensure that a model would effectively learn to distinguish between original content and manipulated one. The data is clumped in two large categories; real and fake that allow guided learning in the learning phase.

The data has been compiled up to the publicly available sources and grouped in such a way that there is a balance between the two classes. Such balance is required to prevent biases within the model such that the model is not discriminating a particular one of the classes. In case there is video data, the videos are decomposed into individual frames making videos to be treated as individual input samples.

Several preprocessing operations are then performed on the data prior to inputting into the model in order to optimize consistency and feature extraction. Firstly, every picture is resized to a standard image size in order to make the data set homogenous. This helps this model to prevent size variation when processing inputs. Normalization of the pixel values follows which is normally normalized to a standard range to stabilize the training process and to make it faster.

Face detection is then applied on the pictures or frames so as to detect the face part of the picture only. This action can remove redundant information about the background and ensure that the model is interested in the most topical sphere where deepfake manipulations are likely to occur. After detecting the face we crop and align it so as to make it uniform in terms of orientation.

In addition to these, basic data cleaning is performed to remove contaminated or of poor quality samples that may have a negative effect on the performance of a model. As an alternative, data might be augmented by rotation, flipping and increasing/decreasing the brightness which will increase the generalization capability of the model.

Overall, the preparation and preprocessing stages of data mean a lot in the context of ensuring that the system is more reliable. The model will tend to form meaningful patterns and achieve the correct deepfake detection through ensuring that the input data are clean, balanced, and well-structured.

V. Feature Extraction and Model Design

In this project, the feature extraction shall come in handy in helping the system to identify the minute differences between the real and deep fake contents. Considering the fact that raw pictures are not necessarily adequate, the process will be entailed in extraction of meaningful facial biometric features that denote discrepancies that have been brought about during the process of manipulation.

This begins with the face detection as seen in fig 2. which is then followed by the isolation of the facial region of the input image or frame. Among this part, some of the facial features are identified, and they are eyes, nose, mouth, and jaw. Such marks help to determine the anatomy and form of the face. Overall, the deepfake content typically introduces slight misrepresentations in the following aspects, and they might not be detected by the human eye yet can be revealed through computational analysis.

The landmarks are not the only features considered, the features founded on texture are also considered. These include pixel-based patterns, skin texture and the lighting of the face uniformity. In other instances, deepfake models do not perfectly emulate natural textures and form mini holes. Based on these patterns, the system can pick up some indications that would qualify the content to be manipulated.

Once the features are extracted, they are inputted into the model and they are classified. The machine learning process is used to train the model, where the model is trained to differentiate between genuine and counterfeit samples with respect to the extracted features. The given step can be conducted by means of a Convolutional Neural Network (CNN), which is particularly efficient at the extraction of the spatial pattern and visual detail in pictures. The network will consist of multiple layers, each of which will consist of convolutional ones that will acquire features, followed by pooling layers that will make the dimensions smaller and finally fully connected layers that will be used to perform final classification.

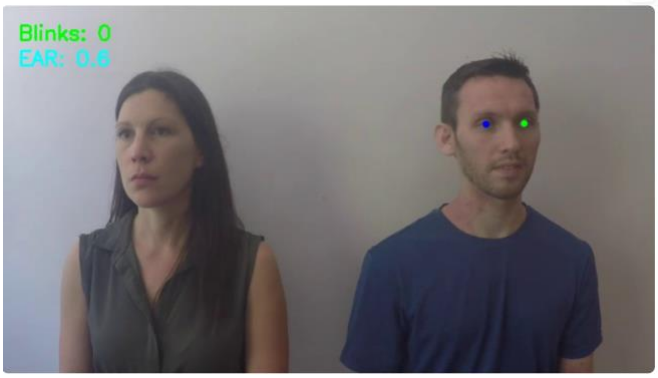

Fig 2.Feature Extraction

During training, the model is trained to follow specific patterns of features either over the real or the fake labels. This can easily identify even slight inconsistency that cannot be identified manually with time. Regularization methods and sufficient parameter adjustment are applied in the process of avoiding overfitting and improving generalization.

The overall structure of the model is kept at relatively simple level in order to make the model effective and computationally efficient. This makes it easy to implement the system and it can be applied to the practical use without compromising on the good detection performance of the system.

VI. Experimental Result and Discussion

In order to analyze the effectiveness of the proposed system of deepfake detection, a set of experiments was performed based on the prepared data. The data set was split into training and testing in order to make sure that the model could be tested using unknown data. This is useful in terms of knowing the extent to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

which the system can be extrapolated out of the data it was trained on.

In the training process, the model was trained to differentiate between the real and the fake samples based on the patterns of the facial features and textures. Following the required training, the model was evaluated with the help of the test dataset, and its performance was assessed with the help of conventional evaluation measures, which include accuracy, precision, recall, and F1-score.

The findings indicate that the proposed system can be used to differentiate between genuine and deepfake content, as the accuracy of the classification is good. Facial biometric features were also used in the detection and this helped in detection particularly where there was slight difference in appearance. The model could match irregularities of the face structure and texture, which frequently occur in edited media.

The system performed reliable results on the majority of the test samples in terms of performance. It was however noted that in some cases the model would handle deepfakes which were extremely realistic, as the manipulation was very high. Herein lies one of the most significant problems of deepfake detection, namely the ongoing advancement of generation methods.

Compared to the current methods, it would be reasonable to assume that some of the more sophisticated models can be a bit more accurate, but this is usually accompanied by more complexity and higher computational cost. On the contrary, the proposed approach provides the compromise between the two, as it is reasonably accurate, yet rather simple and efficient to achieve.

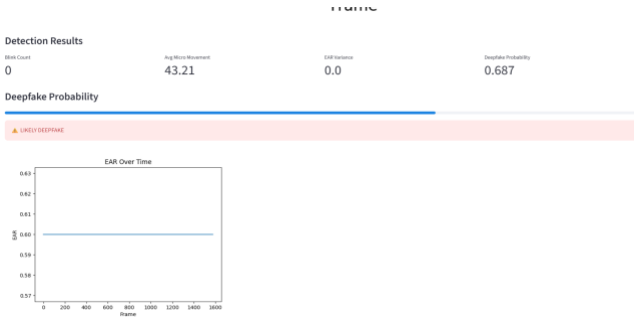

Fig 3.Result

The other critical finding is that the dataset quality and diversity have a great influence on performance. When trained on more diverse datasets, the models are likely to generalize and work well on the data that was not proceeded. This implies that it can still be improved by adding more data and introducing other varieties of deepfake methods.

On the whole, the experimental findings show that the suggested system can be successfully used to identify deepfakes when a set of biometric features is combined with machine learning. It is a good starting point to the future work in the field because the discussion identifies the strengths of the approach and the areas, which can be improved further.

VII. Conclusion and Future Work

The given work is an attempt to make deepfakes detection practical through the integration of facial biometric detection and machine learning. The system is aimed at detecting minor deviations in the structure of the faces, texture, and spatial patterns, which are often fed during manipulation. The suggested approach can successfully categorize material into real and fake with the help of preprocessing, extraction of features, and a learning-based model.

The experiment outcomes indicate that the system can obtain the good performance and it is capable of detecting deepfakes with a reasonable level of accuracy. The simplicity and effectiveness of this approach balanced with each other is one of its major advantages. Rather than using overly complicated architectures, the model has been created to be efficient and less difficult to implement and is therefore appropriate in practical applications.

But, similar to most of the current-day techniques, the system is challenged with the highly realistic deepfakes. With the ever advancing generation techniques, the content becomes harder to detect. Also, the size and diversity of the dataset that is used in training affect performance of the model.

In perspective, the directions that can be improved in the future are several. The system can be improved by adding bigger and more varied datasets, and this would contribute to better generalization. Determining the optimal model or a combination of more advanced deep learning models may help further boost the accuracy of detection. Another area that can be considered is real-time implementation particularly when dealing with social media monitoring, digital security applications.

To conclude, this project can illustrate how machine learning and biometric features can be successfully applied to the problem of deepfakes detection which increasingly becomes the challenge to be considered, as well as a basis to develop further in this direction.

References

[1] H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, “Multi-task learning for detecting and segmenting manipulated facial images and videos,” in *Proc. IEEE Int. Conf. Biometrics (ICB)*, 2019, pp. 1–8.

[2] A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, “FaceForensics++: Learning to detect manipulated facial images,” in *Proc. IEEE/CVF Int. Conf. Computer Vision (ICCV)*, 2019, pp. 1–11.

[3] Y. Li and S. Lyu, “Exposing deepfake videos by detecting face warping artifacts,” in *Proc. IEEE Conf. Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2019, pp. 46–52.

[4] D. Afchar, V. Nozick, J. Yamagishi, and I. Echizen, “MesoNet: a compact facial video forgery detection network,” in *Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS)*, 2018, pp. 1–7.

[5] T. Karras, S. Laine, and T. Aila, “A style-based generator architecture for generative adversarial networks,” in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4401–4410.

[6] P. Korshunov and S. Marcel, “Deepfakes: a new threat to face recognition? Assessment and detection,” *arXiv preprint arXiv:1812.08685*, 2018.

[7] F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 1251–1258.