# Deepfakes Detection Using Human Eye Blinking

[1]Umair Ansari, [2]Prithvi Kamble, [3]Apurva Shinde, [4]Mr.Subhash.G.Patil
[1,2,3]UG Student, [4]Assitance Professor, Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala, Pune, Maharashtra, India.
[1]ansariumair2402@gmail.com, [2]kambleprithvi2300@gmail.com, [3]shindeapurva138@gmail.com, [4]subhashpatil1902@gmail.com

*Abstract* - **Advanced deepfake technology enables the creation of highly realistic yet fabricated images and videos, posing significant challenges for detecting misinformation and maintaining trust in media content. One effective method for detecting deepfakes involves utilizing the natural human response of blinking. This paper presents a novel approach to deepfake detection by leveraging the physiological response of human eye blinking. Deepfakes, which manipulate facial features and expressions, often struggle to replicate the natural blinking patterns of real individuals. Our method utilizes computer vision techniques and machine learning algorithms to analyze eye blinking patterns from video clips and images. We extract key features such as blink frequency, duration, and synchronization with other facial movements.**

**To train and evaluate our method, we used an extensive dataset containing real and deepfake videos. The results demonstrate the effectiveness of our approach in distinguishing between real and deepfake videos. The human eye blinking-based detection approach achieved a high accuracy rate, accurately detecting deepfakes in seven out of eight types of videos (87.5% accuracy rate). This suggests that we can overcome the limitations of integrity verification algorithms based solely on pixel analysis.**

**Keywords: deep-fake, GANs, deep learning, Convolutional Neural Network (CNN), Python, Tensor Flow, SQL Lite.**

## I. INTRODUCTION

Detection of Deepfakes Using Human Eye Blinking" is an intriguing subject that intersects computer vision, deep learning, and cybersecurity. Deepfakes are realistic but fake videos or images created using AI techniques, particularly deep learning. These manipulated media can be used to alter content, impersonate individuals, or spread misinformation.

In recent years, Deepfakes have become a social issue due to their potential for misuse. Created using the generative adversarial network (GANs) model, Deepfakes involve iterating a data-based generation and verification task through two opposing deep learning models. This process allows for the synthesis of faces or specific body parts in videos or photos to artificially assume the appearance of other people. Initially, early Deepfakes could be identified by the naked eye due to pixel collapse phenomena, resulting in unnatural visual artifacts in skin tones or facial contours, or frequent visual artifacts. However, with technological advancements, Deepfakes have become increasingly indistinguishable from natural images.

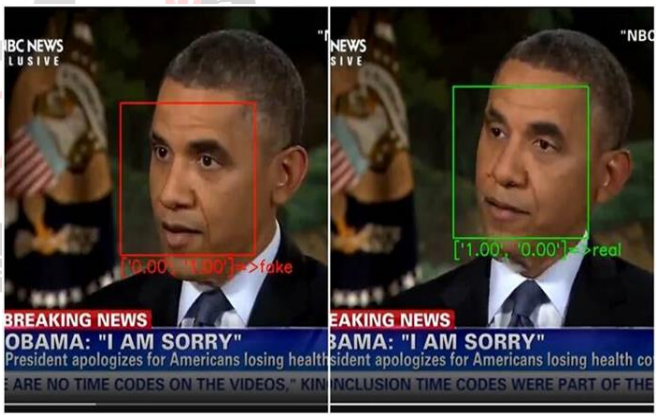


Image 1: Difference Between Real and Deepfake Image

As technology has advanced, there has been an increase in the improper use of Deepfakes. Numerous pornographic images of celebrities and politicians have been created to spread propaganda and fake news, leading to various social issues. According to the Washington Post, the victims of these Deepfake images now include the general public, with face photos and pornographic images being skillfully synthesized and distributed through social media without the consent of the individuals involved. Some companies specialize in providing such Deepfake services.

 DOI : 10.35291/2454-9150.2024.0160 

## II. LITERATURE REVIEW

Article Published In 2016, DCGAN (Deep Convolutional Generative Adversarial Networks) proposed by Alec Radford *et al.* made possible arithmetic operations with filters between images using latent vector by applying CNN (Convolutional Neural Network) models to GANs, emerging more clever forgeries.[1]

Article published in 2023, titled as "Pros and cons of comparing and combining hand-crafted and neural network based Deepfake detection based on eye blinking behavior" by Dennis Siegel and team suggest that, In this paper , a different approach is used, combining hand-crafted as well as neural network based components analyzing the same phenomenon to aim for explainability, and the impact of video duration on the classification result is evaluated empirically, so that a minimum duration threshold can be set to reasonably detect Deepfakes.[2]

Article published in 2022, titled as "Using cascade CNN-LSTM-FCNs to identify AI-altered video based on eye state sequence" by Muhammad Salihin Saealal and team suggest that, In this article, the authors presented a novel means of revealing fake face videos by cascading the convolution network with recurrent neural networks and fully connected network (FCN) models.[3]

Article published in 2023, titled as "Spatiotemporal Pyramidal CNN with Depth-Wise Separable Convolution for Eye Blinking Detection in the Wild" by Nguyen Chi Bach and team suggest that,

In this paper, the authors proposed to utilize up sampling and down sampling the input eye images to the same resolution as one potential solution for the first problem, then find out which interpolation method can result in the highest performance of the detection model.[4]

Article published in 2022, titled as "Eye Blink-Based Liveness Detection Using Odd Kernel Matrix in Convolutional Neural Networks" by N. Nanthini and team suggest that, in this paper, a new approach to detect face liveness based on eye-blinking status using deep learning has been implemented, which is called Odd Kernel Matrix Convolution Neural Network (OKM-CNN).[5]

Article published in 2021, titled as "Deepfake Creation and Detection: A Survey" by Swathi P and team suggest that, In this paper, the authors explore different algorithms used for Deepfake creation and detection; presenting a comprehensive overview of the techniques used and aimed at identifying their pros and cons, as well as identifying their advantages and disadvantages.[6]

## III. METHODOLOGY

The concept of using human eye blinking to detect deepfakes is an interesting one. Deepfakes are created using deep learning techniques to manipulate videos or images to make them appear as though they are real, even though the content is fake. One of the challenges with deepfakes is that they often lack natural human characteristics, such as blinking.

The idea behind using human eye blinking to detect deepfakes is that deepfake videos may not accurately mimic the natural blinking patterns of real humans. By analyzing the blinking patterns in a video, researchers can potentially identify inconsistencies that suggest the video is a deepfake.

This approach typically involves using computer vision and machine learning algorithms to track and analyze the blinking patterns in a video. These algorithms can be trained on a dataset of real and deepfake videos to learn the differences in blinking patterns between the two.

The detection of deepfakes using human eye blinking involves a multifaceted process that relies on the analysis of unique patterns and characteristics associated with natural eye movements. Here's a breakdown of the general workings involved:

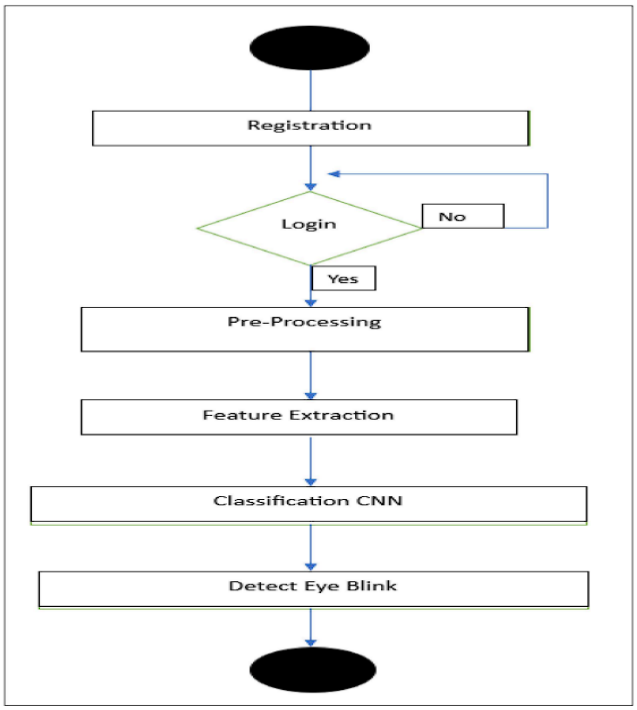


Fig 1: Work Flow

Data Collection and Analysis: Initially, a substantial dataset of authentic eye blink patterns is compiled. This dataset serves as the basis for training machine learning algorithms to recognize and differentiate between genuine and deepfake-generated eye movements. This dataset may encompass a wide range of individuals to capture the natural diversity in blinking patterns.

Feature Extraction: Machine learning models, particularly deep neural networks, are employed to extract distinct features from the eye blinking patterns observed in videos or images.

Comparison and Verification: Once trained the required data, these models are then utilized to analyze new or unknown video or image content. When encountering a video suspected of being a deepfake, the system examines the eye blink patterns within the given data, comparing them against the learned characteristics of genuine blinks.

 DOI : 10.35291/2454-9150.2024.0160 

Validation: The accuracy of the detection system is continually validated and refined through the ongoing collection of new data and the adjustment of algorithms to enhance their capacity to discern between real and manipulated eye blinking patterns.

Comparison and Verification: Once trained the required data, these models are then utilized to analyze new or unknown video or image content. When encountering a video suspected of being a deepfake, the system examines the eye blink patterns within the given data, comparing them against the learned characteristics of genuine blinks.

## IV. RESULT

1. User Interface (UI) of Application


Image 2: UI of Application

The user interface (UI) plays a crucial role in providing a seamless and intuitive experience for users interacting with the application. Here are some key aspects of the UI:

Registration: On the Home page of Application Registration Option is Given by Which User Can Register Our Self to the Application.

Login: If a User Account Already Exist on the server, then User can Directly Login to the application through their Account.

Exit: Also, an exit option are there to exit from the Application.

2. Registration Page


Image 3: Registration page

The Registration page allows users to create an account to access the application's features. Here are some key considerations for the Registration page:

User Information: The Registration page should collect necessary information from users, such as username, email address, and password. Consider including optional fields for additional information, such as user preferences or demographics.

Error Handling: Display error messages if there are issues with the registration process, such as duplicate usernames or email addresses.

Submit Button: Include a submit button for users to finalize their registration. Use JavaScript to handle form submission and send the registration data to the server.

Login Link: Provide a link to the Login page for users who already have an account and need to log in.

3. Main UI

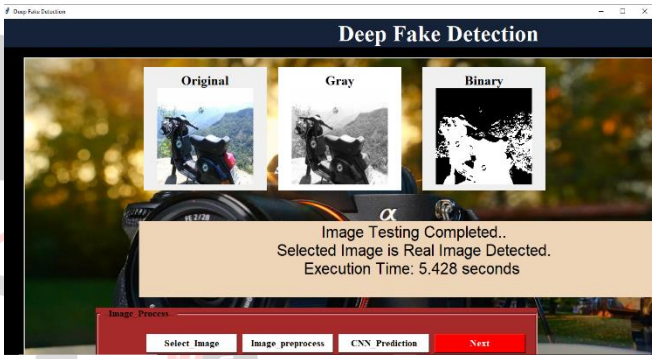


Image 4: Main Application UI

The Main UI of the Application is the most important thing in an application. In this project the main UI of Application consist of some options.

Like User can Select Trained Image or video from their local storage and after selecting an image or video application will process the image and analyze the give data.

Basis on the given data our Algorithm will predict the given input data is real or fake by analyzing pixels or frames of the given data. It can process only one data at a time. The before provide some data to algorithm we need to trained that data. The time required for training the data is very high because algorithm analyze each and every pixel or frames of data.

## V. SCOPE

The scope of employing human eye blinking for deepfake detection is a burgeoning field within the realm of biometric authentication and anti - deepfake technologies. By leveraging the unique, involuntary nature of human blinking patterns, researchers are exploring the use of blink dynamics and characteristics as a potential biometric identifier to differentiate between authentic and manipulated facial videos. This approach aims to analyze the natural blink frequency, duration, and intricacies of blinking patterns, detecting

 DOI : 10.35291/2454-9150.2024.0160 

discrepancies in deepfake videos where such patterns may be absent or inaccurately replicated. With the growing concerns surrounding deepfake proliferation and its potential consequences in various sectors, including misinformation and identity theft.

However, while utilizing eye blinking for deepfake detection presents a novel and potentially effective method, it faces challenges concerning accuracy, especially given the advancements in deepfake generation that continually strive to mimic natural human behavior. The scope of this approach may require extensive data sets and sophisticated machine learning models to accurately distinguish between authentic and manipulated content based on blink patterns.

## VI. CONCLUSION

Utilizing human eye blinking patterns for deepfake detection shows promise, yet it comes with notable challenges. While offering advantages like non-intrusiveness and interpretability, there are significant limitations. Blinking pattern analysis is just one component in the broader deepfake detection field. While this research marks progress, it's crucial to note that deepfake technology continues to advance. Therefore, ongoing research and development are vital to outpace malicious actors. Future work could involve dataset expansion, real-time model optimization, and addressing emerging challenges.

## VII. REFERENCES

[1] A. Radford, L. Metz, and S. Chintala, ‘‘Unsupervised representation learning with deep convolutional generative adversarial networks,’’ 2015, arXiv:1511.06434. [Online]. Available: http://arxiv.org/abs/1511.06434

[2] Siegel, Dennis, Stefan Seidlitz, Christian Krätzer and Jana Dittmann. “Pros and cons of comparing and combining hand-crafted and neural network based DeepFake detection based on eye blinking behavior.” *Media Watermarking, Security, and Forensics* (2023).

[3] Saealal MS, Ibrahim MZ, Mulvaney DJ, Shapiai MI, Fadilah N (2022) Using cascade CNN-LSTM-FCNs to identify AI-altered video based on eye state sequence. PLoS ONE 17(12): e0278989. https://doi.org/10.1371/journal.pone.0278989

[4] Nguy, L.A., Bach, N., Nguyen, T.T., Eiji, K., & Phan-Xuan, T. (2023). Spatiotemporal Pyramidal CNN with Depth-Wise Separable Convolution for Eye Blinking Detection in the Wild. *ArXiv, abs/2306.11287*.

[5] N., Nanthini., N., Puviarasan., P., Aruna. (2022). Eye Blink-Based Liveness Detection Using Odd Kernel Matrix in Convolutional Neural Networks. 473-483. Doi: 10.1007/978-981-16-2594-7_39

[6] Swathi, P., Saritha, Sk. (2021). Deepfake Creation and Detection: A Survey. doi: 10.1109/ICIRCA51532.2021.9544522

[7] https://user-images.githubusercontent.com/85504424/166109395-1dab98ae-f2f0-4c47-a80e-2a55e599c384.png

 DOI : 10.35291/2454-9150.2024.0160 