

Survey On “Deepvision’s Human Eye Blink Pattern Analysis for Deepfake Detection”

Miss. Namita Survase¹, Miss. Sakshi Shrimandale², Mr. Gaurav Hande³, Prof. Pooja V. Baravkar⁴

**1.2.3 Last Year Student, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*

**4 Profecessor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India*

Abstract - Deepfake technology has rapidly evolved, enabling the creation of highly convincing synthetic media, including images, videos, and audio recordings. These maliciously manipulated digital artifacts can have severe consequences for privacy, security, and trust in digital content. Therefore, the development of effective deepfake detection methods is of paramount importance. This paper proposes a novel approach for deepfake detection based on the analysis of human eye blinking patterns. The human eye blink is a unique and subtle behavioral trait that is challenging to replicate accurately in deepfake videos. We leverage this inherent biometric feature to identify anomalies in video content and distinguish between genuine and synthetic videos.

Key Words: Eye Blink to Speech, Machine Learning.

1. INTRODUCTION

Deepfakes have raised alarming concerns due to their potential to deceive, manipulate, and spread misinformation. These AI-generated forgeries have become increasingly convincing, making them difficult to detect through conventional means. As a result, researchers are turning to human physiological and psychological indicators to tackle the problem of deepfake detection. One of the intriguing aspects of deepfake detection is the role of human eye blinking patterns. Blinking is a natural

and involuntary behavior that occurs frequently and rhythmically in humans. It serves multiple functions, including protecting the eye, moisturizing the cornea, and regulating visual input.

It becomes very important to spot the difference between the deepfake and pristine video. We are using AI to fight AI. Deepfakes are created using tools like Face App and Face Swap, which use pre-trained neural networks like GAN or Autoencoders for these deepfakes creation. Our method uses a LSTM based artificial neural network to process the sequential temporal analysis of the video frames and pre-trained Res-Next CNN to extract the frame level features. ResNext Convolution neural network extracts the frame-level features and these features are further used to train the Long Short Term Memory based artificial Recurrent Neural Network to classify the video as Deepfake or real. To simulate real-world conditions and enhance the model's performance on real-time data, we conducted extensive training using a diverse and balanced combination of various datasets, including Face Forensic++, the Deepfake Detection Challenge dataset, and Celeb-DF.

Further to make the ready to use for the customers, we have developed a frontend application where the user will upload the video. The video will be processed by the model and the output will be rendered back to the user with the classification of the video as deepfake or real and confidence of the model

2. LITERATURE SURVEY

Face Warping Artifacts [15] used the approach to detect artifacts by comparing the generated face areas and their surrounding regions with a dedicated Convolutional Neural Network model. In this study, two distinct categories of facial artifacts were identified. The research approach was rooted in the observation that contemporary deepfake algorithms can exclusively produce images with constrained resolutions. Subsequently, these images necessitate additional modifications to align with the desired criteria. Detection by Eye Blinking describes a new method for detecting the deep fakes by the eye blinking as a crucial parameter leading to classification of the videos as deepfake or pristine. The Long-term Recurrent Convolution Network (LRCN) was used for temporal analysis of the cropped frames of eye blinking. In today's landscape, the capabilities of deepfake generation algorithms have reached such a level of sophistication that relying solely on the absence of eye blinking is no longer a sufficient indicator for the detection of deepfakes. There must be certain other parameters must be considered for the detection of deep fakes like teeth enchantment, wrinkles on faces, wrong placement of eyebrows etc.

Some already exist deepfake detection web & Android application's are following :

[1]. Paper Name : Multidimensional Feature Optimization Based Eye Blink Detection Under Epileptiform Discharges

Author : Meng Wang, Jianhui Wang, Xiaonan Cui, Tianlei Wang

Publish Date : April 2022.

Information : Detecting eye blink artifacts in scalp electroencephalogram (EEG) recordings of epilepsy patients poses a significant challenge due to their waveform similarities with epileptiform discharges. Developing an accurate detection method is of utmost importance and urgency. In this paper, we introduce an innovative approach for eye blink artifact detection in EEGs containing abundant epileptiform discharges, centered on multi-dimensional feature optimization. We propose an unsupervised clustering algorithm based on smoothed nonlinear energy operator (SNEO) and variational mode extraction

(VME) to identify epileptiform discharges in the frontal leads. Subsequently, we extract multi-dimensional time/frequency EEG features from the forehead electrodes (FP1 and FP2 channels) and combine them with the improved VME (IVME) threshold to represent the EEG data.

[2]. Paper Name Eye-Blink Detection System for Virtual Keyboard

Author : . Naila Hashmi¹, Jyoti Kavar², Shweta Kavar

Publish date : November 2021.

Information : In today's world, virtually every task necessitates the use of a computer, making computer access an essential requirement in our society. Human-Computer Interaction (HCI) has become a fundamental skill for everyone, enhancing computer literacy. HCI specifically concentrates on the interface and interaction between individuals and computers, aiming to design technology that enables unique ways for people to interact with computer systems. This becomes particularly valuable for individuals with physical disabilities, enabling them to navigate and access the internet. In this system, the use of eye blinks allows users to input special characters and alphanumeric characters, much like manual keyboard input. It empowers individuals to explore and engage with various websites using just a simple eye blink.

[3]. Paper Name : A Real-Time Blinking Reminder Supportive System for Eye Care of Computer Gamers

Author : S. M. Fahim Faisal, Asiful Haque Joarder

Publish Date : December 2021.

Information : One of the most prevalent issues afflicting people today is ocular diseases, with approximately 75% of individuals requiring eyeglasses to address vision problems. The excessive use of electronic devices is a primary contributor to this concern. When using these devices, individuals often neglect to blink their eyes regularly, especially while engrossed in activities like gaming or official work that demand prolonged screen viewing. The proposed system offers a potential solution to this issue, particularly concerning the diminished blink rates observed among computer gamers during gameplay. This study conducts a survey to establish the extent of eye blinking among computer gamers. To identify human eyes and detect eye blinks, the

system employs a Haar feature-based classifier capable of recognizing both human faces and eye positions.

[4]. Paper Name : Non-contact, real-time eye blink detection with capacitive sensing

Author : Mengxi Liu, Sizhen Bian, Paul Lukowicz

Publish Date : December 2022

Information : This research introduces an innovative non-contact, wearable, and real-time eye blink detection system utilizing capacitive sensing technology. A cost-effective, low-power capacitive sensing prototype was designed and integrated into a regular pair of eyeglasses, with a copper electrode affixed to the frame. The act of blinking the eye induces a change in capacitance between the electrode and the eyelid. By continuously monitoring the oscillating frequency shift signal resulting from this capacitance variation, eye blinks can be identified through a straightforward comparison of the raw frequency signal with a predefined threshold.

[5]. Paper Name : DEEPFAKE DETECTION USING BIOLOGICAL FEATURES: A SURVEY

Author : Kundan Patil, Shrushti Kale

Publish Date : January 2023.

Information : The emergence of deep learning techniques, particularly the deepfake technology, has significantly simplified the process of altering and manipulating images and videos. Visual evidence plays a crucial role in investigations and legal proceedings, but advancements in technology, notably deepfake, have raised concerns about the authenticity of such evidence. Edited photos and videos now appear remarkably realistic, making it challenging to distinguish them from unaltered originals. Deepfakes have been exploited for various nefarious purposes, including blackmail, planning of terrorist activities, spreading false information, character assassination, and inciting political unrest. Our study delves into the history of deepfakes to provide a comprehensive insight into this technology. Additionally, our research places emphasis on the evolution of deepfake technology and the challenges associated with its detection, particularly through physiological measurements. We elucidate the use of biological cues such as eyebrow recognition, eye blink detection, eye movement tracking, ear and mouth identification, and even heartbeat

detection, offering a promising direction for further exploration in this field.

[6]. Paper Name : The Deepfake Detection Challenge (DFDC) Preview Dataset

Author : Brian Dolhansky, Russ Howes, Ben Pflaum, Nicole Baram, Cristian Canton Ferrer

Publish Date : October 2019

Information : A sneak peek into the Deepfakes Detection Challenge (DFDC) dataset reveals the presence of 5,000 videos that showcase the effects of two distinct facial modification algorithms. This extensive dataset was curated through a meticulous data collection campaign, with participating actors willingly agreeing to the use and manipulation of their likenesses for dataset creation. The dataset prioritizes diversity on multiple fronts, encompassing various factors such as gender, skin tone, and age, ensuring a broad representation. Furthermore, actors recorded videos against a backdrop of their choice, adding an extra layer of visual diversity to the dataset. To facilitate the assessment of performance, a set of specific metrics has been established, and two established models for deepfake detection have been employed to establish a reference performance baseline.

[7]. Paper Name : Face X-ray for More General Face Forgery Detection

Author : Lingzhi Li, Jianmin Bao, Ting Zhang, Hao Yang, Dong Chen, Fang Wen, Baining Guo

Publish Date : December 2019

Information : The concept of a "Face X-ray" for an input face image involves the creation of a grayscale representation that serves to unveil whether the input image can be deconstructed into a fusion of two distinct source images. It accomplishes this by delineating the boundary of blending in the case of a manipulated or forged image, while also highlighting the absence of blending in genuine images. Notably, it has been observed that a significant number of existing face manipulation techniques consistently involve a common procedure: the integration of an altered face into an existing background image. In light of this observation, the Face X-ray technique emerges as a potent means for detecting forgery

resulting from most prevalent face manipulation algorithms. The strength of Face X-ray lies in its generality, as it solely assumes the presence of a blending step, without relying on any prior knowledge of the specific artifacts associated with a particular face manipulation technique.

[8]. Paper Name Deepfake Detection: A Systematic Literature Review.

Author : Md Shohel Rana, Mohammad Nur Nobil, Beddhu Murali, Andrew H. Sung

Publish Date : January 2022

Information : The term "Deepfake" is a fusion of "Deep Learning (DL)" and "Fake," and it denotes the creation of highly realistic video or image content through the application of deep learning techniques. This term was coined in late 2017 by an anonymous Reddit user who leveraged deep learning methods to replace a person's face in explicit videos with the face of another individual, resulting in the production of astonishingly lifelike counterfeit videos. The process of generating these deceptive videos involves the use of two neural networks: (i) a generative network and (ii) a discriminative network, employing a FaceSwap technique. The generative network is responsible for generating fabricated images through the utilization of an encoder and a decoder, while the discriminative network assesses the authenticity of the newly produced content. The amalgamation of these two networks is collectively referred to as Generative Adversarial Networks (GANs), a concept initially proposed by Ian Goodfellow.

[9]. Paper Name : Deep Learning for Deepfakes Creation and Detection: A Survey

Author : Thanh Thi Nguyen, Quoc Viet Hung Nguyen, Dung Tien Nguyen, Duc Thanh Nguyen, Thien Huynh-The, Saeid Nahavandi, Thanh Tam Nguyen, Quoc-Viet Pham, Cuong M. Nguyen

Publish Date : August 2022

Information : Deep learning has undeniably found success in addressing a myriad of intricate challenges, spanning domains as diverse as big data analytics, computer vision, and even achieving human-level control in various applications. However, the very advancements in deep learning that have

yielded these achievements have also been harnessed to develop software solutions that hold the potential to jeopardize individual privacy, democratic processes, and national security. Among the latest applications to emerge from deep learning technologies, deepfakes have emerged as a particularly noteworthy and concerning development.

[10]. Paper Name : DeepFake Detection: Current Challenges and Next Steps

Author : Siwei Lyu

Publish Date : March 2020

Information : While DeepFake videos can undoubtedly offer intriguing and imaginative applications, their potential for misuse is a significant concern. Given the strong connection between faces and individual identity, these sophisticated fabrications can be weaponized with dire consequences. Meticulously crafted DeepFake videos can craft illusions of a person's presence and actions that never occurred in reality, giving rise to grave political, social, financial, and legal ramifications. The spectrum of potential threats spans from vengeful creation of pornographic content by synthesizing a victim's face, to convincingly lifelike videos of state leaders making false, incendiary statements, high-level executives manipulating global stock markets with fabricated corporate comments, or online predators posing as family members or friends during video chats.

3. CONCLUSION

In conclusion, using human eye blinking patterns for deepfake detection is a promising but challenging approach. While it offers several advantages, such as being a non-intrusive and interpretable feature, there are also significant limitations to consider. Blinking pattern analysis is just one piece of the puzzle in the broader field of deepfake detection. While this research represents a significant advancement in deepfake detection, it is important to acknowledge that deepfake technology continues to evolve. Therefore, further research and development are essential to stay ahead of malicious actors. Future work in this field may involve expanding the dataset, optimizing the model for real-time applications, and addressing emerging challenges.

4. FUTURE SCOPE

Deepfakes are a growing concern in the digital world, and detecting them is a challenging task. Deepfake detection using human eye blinking patterns holds significant promise in enhancing security and trust in digital content. Leveraging this unique biometric feature has the potential to provide an added layer of defense against the growing threat of deepfake technology. As deepfakes become increasingly sophisticated, novel approaches like blink pattern analysis offer a promising means to differentiate between real and synthetic content. This technology may find applications in diverse fields, from user authentication and access control to content verification on social media platforms and even in health monitoring. The key lies in further research and development to improve the accuracy and reliability of blink pattern detection, address privacy and ethical concerns, and ensure compliance with regulatory standards. With advancements in machine learning and computer vision, the integration of blink pattern analysis into various devices and applications may play a crucial role in countering the challenges posed by deepfakes while offering a non-intrusive and user-friendly experience.

5. REFERENCES

- [1]. Kristen Grauman, Margrit Betke, James Gips, Gary R. Bradski "Communication via Eye Blinks - Detection and Duration Analysis in Real Time" IEEE Conference, December 2001.
- [2]. A. Kerr, B. Durward, and K. M. Kerr, "Defining phases for the sit-to-walk movement," Clin Biomech (Bristol, Avon), vol. 19, no. 4, pp. 385–390, May 2004, doi: 10.1016/j.clinbiomech.2003.12.012.
- [3]. A. Magnan, B. J. McFadyen, and G. St-Vincent, "Modification of the sit-to-stand task with the addition of gait initiation," Gait & Posture, vol. 4, no. 3, pp. 232–241, May 1996, doi: 10.1016/0966-6362(95)01048-3
- [4]. Kunal Bhalgat, Sayali Desai, Rajeshri Kumar N, Kohlbechers, Schneider E "A Novel Approach to Videobased Pupil Tracking" IEEE Int. Conf. on San Antonio, pp. 1255-1262, 14 October 2009.
- [5]. K. Abe, Shoich Ohi, M. Ohyama "Eye Gaze Detection by Image Analysis Under Natural Light" Springer - verlag Berlin Heidelberg, pp. 176-184, 2011.
- [6]. Naresh E, Praveen Kumar P "Eye Blink Controlled Human Computer Interface for Physically Challenged People" in International Conference on Computer Science and Information Technology, 2012.
- [7]. Naresh E, Sandeep Kumar Kalaskar "A Novel Testing Methodology to Improve the Quality of Testing a GUI Application" MSRJETR, Vol.1 No.1, Page no 41-46, July 2013.
- [8]. Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, Matthias Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images" in arXiv:1901.08971.
- [9]. Deepfake detection challenge dataset : <https://www.kaggle.com/c/deepfake-detection-challenge/data> Accessed on 26 March, 2020.
- [10]. Yuezun Li, Xin Yang, Pu Sun, Honggang Qi and Siwei Lyu "Celeb-DF: A Large-scale Challenging Dataset for DeepFake Forensics" in arXiv:1909.12962.