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.2024.60970

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 fakes Detection Using Human Eye Blinking Pattern: Deep Vision

Gorde Siddharth[1], Gadhave Rohit[2], Gadhave Pankaj[3], Bhaskar Satyam[4], Prof. S. A. Shivarkar[5]
[1, 2, 3, 4, 5]*Department of Computer Engineering, Sanjivani College of Engineering, Kopargaon, Maharashtra, 423603, India*

Abstract: ***Deepfake technology is developing rapidly and has the ability to create fake videos that pose a threat to people. Modern depth detection methods often rely on facial disparity, but as technology advances these methods become obsolete. In this study, we propose a new method for deepfake detection based on observation of human eye blink patterns. Human eye blinking is a natural and involuntary action that is difficult to accurately replicate in deepfake video. In our study, we used the unique characteristics of individual blink patterns, which are influenced by many factors such as genetics, muscle tone and unconscious reflexes. We use computer vision and machine learning techniques to extract and identify these patterns from video clips. Our preliminary tests show good results in detecting deepfakes with high accuracy. We are focused on continuing to support the fight against the spread of fraud by focusing on a part of human behaviour that is difficult to replicate. This approach has the potential to improve existing tools for in-depth discovery and increase the overall security and reliability of multimedia content in the digital age. This research opens new avenues for the development of more robust, reliable and flexible deep recognition technologies. This represents a significant step forward in the ongoing fight against malicious misuse of electronic devices.***
Keywords: Deepfakes, Computer Vision, Eye Blinking Patterns, Eye Blinking Patterns

I. INTRODUCTION

The rise of deepfakes in today's digital age poses an increasing challenge to privacy, security and authenticity. Deepfakes involve the use of artificial intelligence to control audio and video content with the ability to deceive, deceive and manipulate people on a large scale. Recognizing and mitigating the impact of fraud is essential to maintaining trust and confidence in the digital world. It has become difficult to understand the truth and trust the information, which means a great disaster [6]. The rise of apps Keep content online and easy to access by quickly sharing it across platforms. At the same time, we are seeing major advances in machine learning and efficient (ML) and deep learning (DL) algorithms that can be used to make audiovisual content display false text and damage the reputation of people online [5].

There are some popular techniques that are widely used to manage photos/videos. Some are computer graphics based (like Photoshop, GIMP and Canva), while the rest are different content. Deepfake is a method based on deep learning and is a strong competitor in the context of video spoofing technology [4]. The ability to control videos can lead to data misuse, identity theft, and other cybercrimes. This situation has encouraged the increasing need for technology research to prevent the use of harmful technologies [3,4].

A new method for detecting deepfakes uses an algorithm called “deep vision” and a different network model to analyse the difference between blink patterns. Struggling is a goal without movement. The blinking pattern of the human eye has been shown to vary greatly depending on a person's physical health, work experience, biological makeup, and capital formation. Rithvika SanilM [6] this technique uses Long Term Recurrence CNN (LRCN) which is deep. Combining neural networks and CNNs, neural networks combine the body's experience to distinguish the open and closed state of the eye. Ruhsar Gazi1 [1, 2].

II. LITERATURE SURVEY

Research work by 7 different authors has been discussed on the basis of varied deep learning techniques and architectures adopted by them.

In their research, Ruksa Gazi and fellow researchers [1] employed a novel approach utilizing Long-term Recurrent CNN (LRCN), a deep neural network amalgamating recursive neural network and CNN architectures. Their methodology aimed to discern between open and closed states of the eye, integrating past temporal information. Typically, a blink lasts approximately 0.1 to 0.4 seconds per blink. In standard video recordings, the anticipated occurrence involves spontaneous blinks with the aforementioned frequency and duration

Rithvika SanilM and her team [2] propose a novel approach for detecting Deepfakes, leveraging an algorithm named Deep Vision alongside the generative adversarial network model. Their method focuses on analyzing significant disparities in blinking patterns. Blinking, often considered a reflexive and unconscious action, exhibits considerable variability based on an individual's overall physical health, cognitive abilities, biological characteristics, and cognitive workload. Factors such as gender, age, time of day, emotional responses, and level of alertness can all influence blinking patterns. Consequently, the detection of Deepfakes can be facilitated through the analysis of such data.

M. M. El Gayar and collaborators [3] introduce an innovative methodology that combines the strengths of Graph Neural Networks (GNN) and Convolutional Neural Networks (CNN). Their proposed model leverages GNN's capability to capture spatial-temporal information alongside CNN's proficiency in extracting visual features from individual frames. To bolster the model's resilience against adversarial attacks and mitigate overfitting, three distinct fusion strategies and a mini-batch technique are employed. This paper presents a novel and efficient model tailored to address these challenges, utilizing mini-batch GNNs (miniGNNs). Similar to CNNs, miniGNNs facilitate efficient network training for deep fake video detection by operating on downsampled graphs or topological structures in a minibatch fashion.[3]

In a study led by Alakananda Mitra and colleagues [4], the Convolutional Neural Network (CNN) module is employed to extract spatial features, with these feature vectors subsequently input into the classifier section. The resultant classification outcome is then obtained. In order to develop a model resilient to overfitting, average pooling and dropout layers are judiciously incorporated into the network architecture. The FF++ dataset, comprising videos at two distinct compression levels, is deemed suitable for experimentation purposes. In the case of the DFDC dataset, video compression is altered across three levels. Given the prevalent use of compressed data in social media, frame extraction is performed directly on the compressed videos, without prior decompression.

In their research, Rimsha Rafique and colleagues introduce a novel framework designed to detect and classify deep fake images with greater accuracy compared to many existing systems. The proposed method utilizes Error Level Analysis (ELA) to preprocess images, enabling the detection of pixel-level manipulations. These ELA-enhanced images are then input into Convolutional Neural Networks (CNNs) for feature extraction. The deep features extracted are subsequently classified using Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) algorithms. Notably, the proposed technique achieved an impressive accuracy of 89.5% by leveraging ResNet18's feature vector and an SVM classifier. These results underscore the robustness of the proposed method, enabling real-time detection of deep fake images. However, it's important to note that the proposed method is tailored for image-based data. In future research, the authors plan to explore various CNN architectures using video-based deep fake datasets. Additionally, they aim to collect real-life deep fake datasets from their community and utilize machine learning and deep learning techniques to distinguish between deep fake and regular images, thereby enhancing the utility and robustness of the system [5].

In their study, Arash Heidari and her collaborators [6] highlight the predominant evaluation criteria for publications centered on qualitative characteristics, emphasizing metrics such as accuracy, Area Under the Curve (AUC), latency, robustness, and complexity. Notably, functions like security and delay are often overlooked in these assessments. The analysis reveals a diverse range of programming language libraries employed for method analysis and implementation, with Keras constituting a significant portion, approximately 24%. Moreover, the report indicates that 40% of applications prioritize the recognition of video deepfakes. The researchers envision their work as a valuable reference for future investigations into Deep Learning (DL) and deepfake applications, emphasizing the time and collaborative effort required to effectively apply DL in deepfake detection. They advocate for a collaborative approach involving government, business, and academia to enhance overall classification performance in the ongoing fight against deepfakes [6].

In the study led by MD SHOEL RANA and colleagues [7], a novel approach is explored, emphasizing the utilization of eye-blinking patterns as a distinctive and intricate biometric feature for deepfake detection. The primary aim of this research is to devise a system that is both robust and dependable for the detection of deepfakes by [7].

III. PROPOSED METHODOLOGY

Detecting deepfakes is commonly approached as a binary classification problem, where classifiers are utilized to differentiate between authentic and manipulated videos (Singh et al., 2021). This method necessitates a substantial dataset comprising both genuine and fraudulent videos to effectively train classification models. However, despite the increasing prevalence of deceptive videos, there remains a lack of standardized benchmarks to validate various detection methodologies (Q. Liu & Celebi, 2021). Previous research on deepfake detection has predominantly focused on employing Deep Learning (DL) techniques, which can be categorized into two main methods: Convolutional Neural Networks (CNN)-based and Region Convolutional Neural Networks (RCNN)-based approaches (X. Zhou et al., 2020).

CNN-based methods typically extract facial images from video frames and utilize CNNs for training and prediction to obtain image-level results. In this section, we outline the proposed workflow utilized for deepfake detection.

A. *Pre-processing*

This paper presents DeepVision, an architecture tailored for the detection of Deepfakes through the analysis of eye blinking patterns. The proposed method, DeepVision, is characterized by a streamlined process structure that involves pixel value normalization and data augmentation to bolster the dataset's size when the number of images is limited. Video frames are extracted and subjected to facial recognition and tracking algorithms to identify and track faces within each frame. Subsequently, regions surrounding the eyes are isolated for further analysis. These sequential steps, documented in [9, 8], play a pivotal role in enhancing classification accuracy and expediting the training process.

B. *Data Collection*

Gather a diverse dataset of videos with subjects blinking naturally. Include a variety of people, races, and ages to make the model robust. Collect deepfake videos that include manipulated facial expressions, including blinking. Gather a large dataset of real human eye blinking patterns under various lighting conditions, facial expressions, and head movements

C. *Segmentation and Labeling*

Segmentation serves the purpose of discerning manipulated or fake videos from genuine ones. This process involves three main techniques: manual, semi-automatic, and fully automatic [2]. Manual segmentation entails manually tracing and distinguishing between real and fake elements, yielding high accuracy at the cost of being time-intensive. Semi-automatic segmentation involves initial user input for data, striking a balance between accuracy and efficiency. Conversely, fully automatic methods eliminate the need for manual parameter setting, autonomously detecting and segmenting deepfake videos, thereby streamlining the segmentation process.

D. *Feature Extraction*

Feature extraction plays a pivotal role in enhancing system accuracy by identifying and selecting prominent features for analysis. By reducing data dimensionality, it transforms the initial dataset into a more manageable format, facilitating efficient processing. This process involves identifying the most relevant information within the data, thus improving the system's ability to discern patterns and make accurate predictions. Ultimately, feature extraction enables the system to focus on the most informative aspects of the data, leading to enhanced performance and effectiveness.

E. *Post-processing*

Post-processing techniques play a crucial role in analysing both deepfake and real videos. These methods encompass various strategies, including imposing shape limits on samples, applying context-based constraints for enhanced accuracy, and implementing spatial control.

By refining the analysis of deepfake videos, post-processing techniques contribute to better understanding and identification of manipulated content. Additionally, labeling, which involves annotating and categorizing video regions, is considered part of post-processing. This step further enhances the analysis and interpretation of both deepfake and authentic video segments, facilitating more accurate detection and classification.

F. *Model Training*

Train a deep learning model, such as a convolutional neural network (CNN) or recurrent neural network (RNN), using the extracted features from the real and deepfake datasets. The model should learn to differentiate between real and deepfake eye blinking patterns. [7].

G. *Validation and Testing*

Evaluate the model's effectiveness by utilizing a distinct validation dataset Fine-tune the model as needed to achieve the desired accuracy and reduce false positives and false negatives.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

IV. PROPOSED SYSTEM

A. Administration Module

The administration module for a deepfake detection system using human eye blinking patterns plays a crucial role in managing and maintaining the system. The administration module is critical for ensuring the effective and efficient operation of the deepfake detection system, maintaining security, and facilitating user management and support. It serves as the backbone of the entire system, ensuring its reliability and functionality Management Module:

The management module for a deepfake detection system using human eye blinking patterns is responsible for overseeing the broader strategic aspects of the system, including planning, resource allocation, coordination, and decision-making. The management module plays a pivotal role in overseeing the strategic direction and sustainable growth of the deepfake detection system. It is responsible for ensuring that the system remains effective, efficient, compliant with regulations, and aligned with the organization's overall goals.

B. *Res Next CNN for Feature Extraction*

For extracting the features and precisely determining the frame level properties, we suggest using the ResNext CNN classifier instead of developing the classifier from scratch. In order to appropriately optimize the gradient descent of the model, we then will fine-tune the infrastructure by] selecting an appropriate learning rate and adding any additional necessary layers. Following the pooling layers, 2048-dimensional feature vectors are supplied into the CNN as input.

C. Long-term Recurrent CNNs

We use the Long-term Recurrent Convolutional Neural Network (LRCN) to store the temporary state of the eye. The LRCN model mainly consists of 3 parts: (1) feature extraction, (2) sequence learning and (3) state prediction. The input eye region is converted to discriminative features by the feature extraction module. It is implemented by Convolutional Neural Network (CNN) based on the VGG16 framework without the fc7 and fc8 layers.

D. Graph-Based Segmentation

In graphbased segmentation, a pixel is treated as one of the image. The similarity between adjacent pixels is represented in the edge weights that connect image nodes. These lines and edges allow pixels to be grouped into superpixels or distinct sections. Graphbase d segmentation techniques such as cut graphs and regular cuts [4, 6]

V. RESULT AND ANALYSIS

The output of the model is going to be whether the video is deepfake or a real video along with the confidence of the model. As shown in the figure 1.

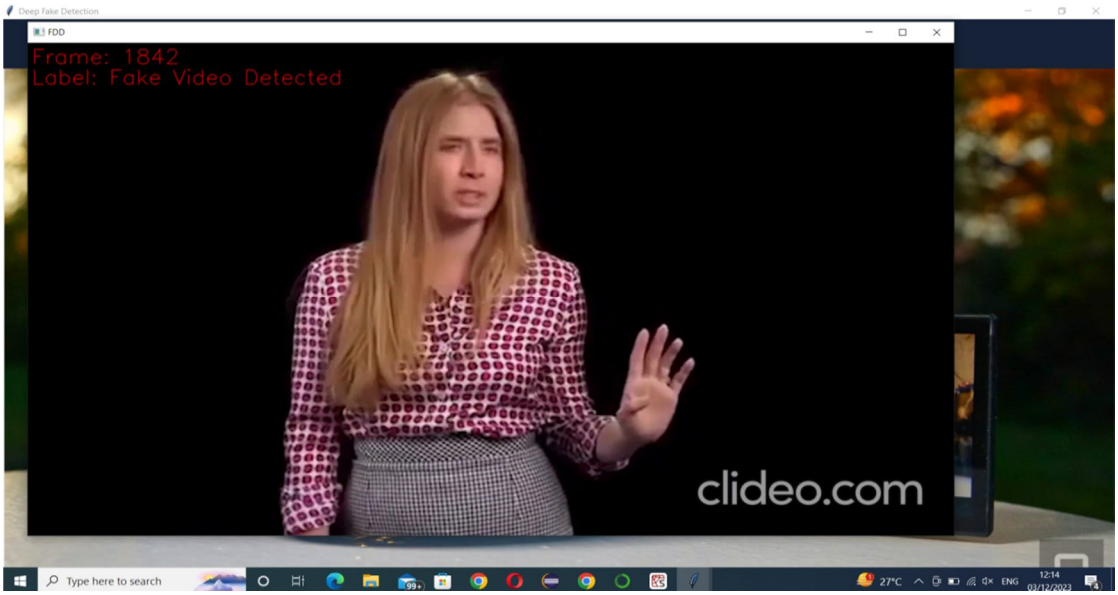


Fig. 1: Expected Results

Our study presented a Convolutional Neural Network (CNN)-based model designed to classify the video and images into two categories fake video and real video. The model's performance was evaluated using a dataset comprising over 1500 videos and images, with the results demonstrating a promising capacity for accurately predicting deepfake. The model achieved an overall accuracy of 85%, with class-specific precision, recall, and F1-scores as mentioned in table no 1.

Class	Precision	Recall	F1-score
Real	90%	88%	89%
Fake	75%	70%	72.5%

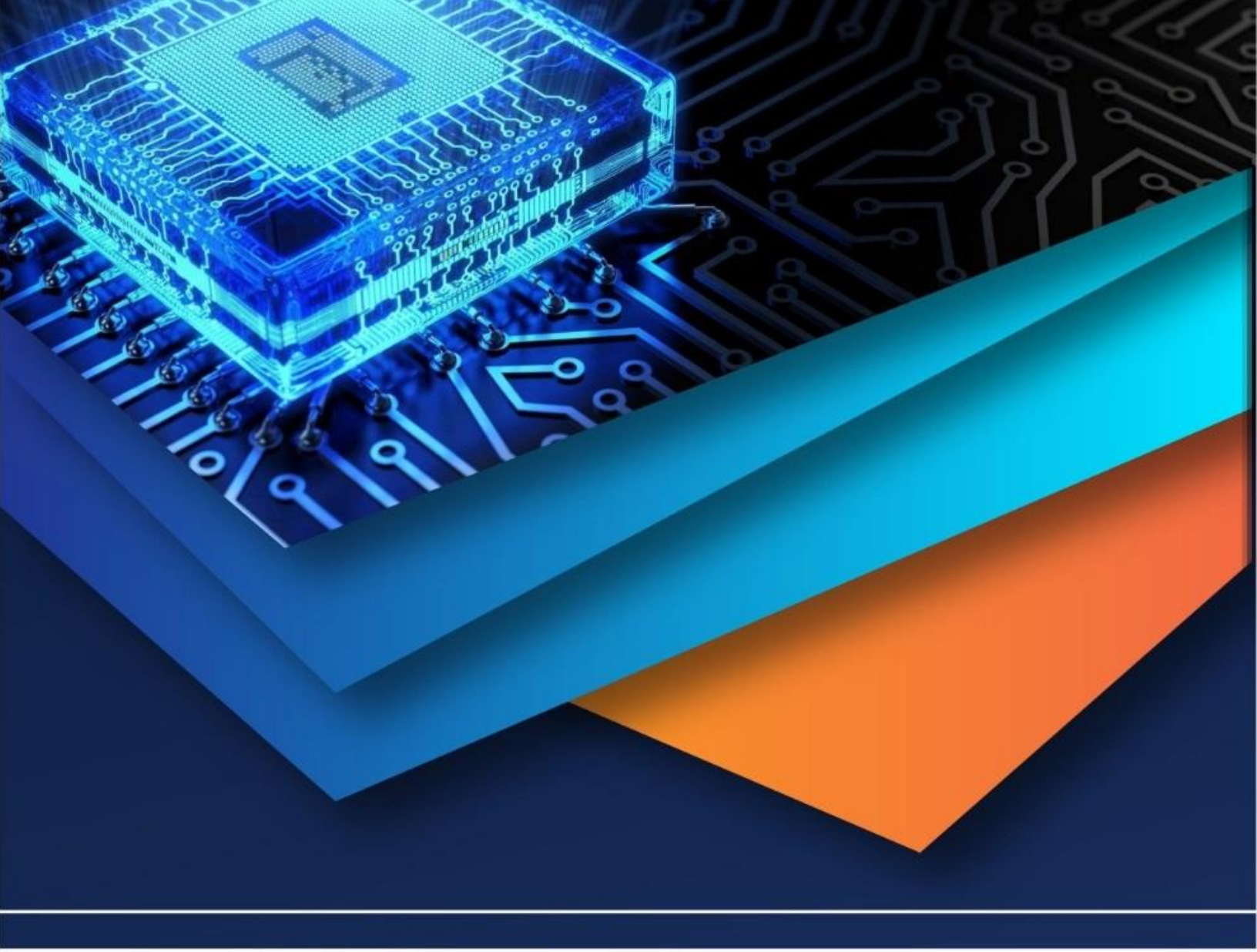
Table no. 1: Class-specific Precision, Recall, and F1-scores

VI. CONCLUSION

In summary, improving detection depth using depth perception is a difficult but important task in today's digital environment. Deepf akes pose a threat to the authenticity of found content, and advances in deep learning have made their creation more common. Howe ver, a more effective and reliable indepth search engine can be created by focusing on important targets and using advanced technol ogy.A neural networkbased method is presented for video classification based on deep video or real video, including the reliability o f the recommendation model. Deepfakes are created from different models with the help of autoencoders as a model for the plan. Ba sed on ResNext CNN and LSTM, our method classifies clips and detects framelevel pixels. According to those not mentioned in the study, the plan will be able to check whether the video is fake or real. We think it will provide instant information with high accura cy.Deepfakes is new tools widely used to expose misinformation and lies about people. Although not all scams are malicious, some still need to be discovered because they threaten the world. The main goal of this research is to discover a reliable method for analyz ing depth images. Many researchers are constantly working to detect fake content using various methods.

REFERENCES

[1] Ruksa Gazi1, Needhi Kore, Raj Jani, Manjyot Singh, Deepti Pawar, “DeepFake Detection Using Eye Blinking,” in International Research Journal of Engineering and Technology (IRJET), IEEE, 2021.
[2] Rithvika SanilM,S.Saathvik, Rithesh RaiK, Srinivas P M, “DEEPFAKE DETECTION USING EYE-BLINKING PATTERN,” in International Journal of Engineering Applied Sciences and Technology (IJEAST), IEEE, 2022
[3] M. M. El-Gayar , Mohamed Abouhawwash, S. S. Askar and Sara Sweidan, “A novel approach for detecting deep fake videos using graph neural network,” in Journal of Big Data, IEEEE, 2024 "
[4] Alakananda Mitra · Saraju P. Mohanty , Peter Corcoran · Elias Kougianos, “A Machine Learning based Approach for DeepFake Detection in Social Media through Key Video Frame Extraction,” SN Computer Science 2021”
[5] Rimsha Rafique, Rahma Gantassi, Rashid Amin Jaroslav Frnda, Aida Mustapha & Asma Hassan Alshehri “Deep fake detection and classification using error-level analysis and deep learning,” in Scientific Reports,2023.
[6] ArashHeidari,NimaJafariNavimipour,HasanDag,MehmetUnal,“Deepfakedetectionusingdeeplearningmethods: A systematic and comprehensive review,” in WIREs Data Mining Knowl Discov 2022..
[7] MD Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, Andrew Sung “Deepfake Detection: A Systematic Literature Review,” in open access journal, IEEE, 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY