iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78268

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 14 Issue III Mar 2026- Available at www.ijraset.com

Deepfake Detection Based Smart Voting System

Shravani Sachin Nalawade[1], Riya Sandeep Jadhav[2], Vaishnavi Krishnat Mohite[3], Tanishka Vaibhav Matane[4], Mrs. P. D. Ghadge[5]
Department of Information Technology, Karmaveer Bhaurao Patil Polytechnic, Satara

Abstract: ***In recent years, the rapid growth of Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning technologies has made it possible to create realistic fake images and videos known as Deepfakes. They can be misused to create fake identities and spread misinformation. This creates serious challenges in systems where identity verification is important, such as Online or Digital Voting systems. In many regions, especially in Rural areas, fake voting and impersonation during elections remain common problems due to weak verification methods. This research proposes a Deepfake Detection Based Smart Voting System to improve security and transparency of voting process. In the proposed system, first voter use their Voter ID for login. After successful login, the system activates a camera to capture a live images of voter and captured image analysed using a Deepfake Detection Model to determine whether it is real or fake. If image is real, the system then compares live captured image with voter's profile picture stored in the database using facial recognition techniques. Only when both images match is voter allowed to cast their vote. The proposed system aims to prevent fake voting, detect deepfake attempts and ensure that only genuine voters participate in elections. By combining deepfake detection and facial verification technologies, the system can help to create a more secure, transparent and reliable digital voting process.***

Keywords: Deepfake Detection, Face Verification, Secure Voting, Digital Identity Verification.

I. INTRODUCTION

In recent years, the quick advancement of Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning technologies has used in many fields such as Security systems, Digital communication and Multimedia. One of the emerging technology due to this advancement is Deepfake Technology, which uses deep learning algorithms to create highly realistic fake images and videos. While Deepfake technology has useful applications in entertainment, education and filmmaking, but it can also be misused to create fake identities, spread misinformation and manipulate digital content. As a result, deepfake detection has become an important research problem in the fields of computer vision and cybersecurity. Deepfake technology first gained attention around 2017, when a social media user used deep learning techniques to swap faces of celebrities in videos. At starting, deepfakes were commonly used for entertainment purpose only through applications like FaceApp, Reface and DeepFaceLab. But as the technology advanced, it became more dangerous. Today, deepfakes are a serious problem because people use them to spread fake news and lies, steal identities to take money form banks or businesses, trick people by making famous leaders or politicians say thing they never said. For example, during the war between Russia and Ukraine in 2022, someone shared a fake video of the Ukrainian President telling his soldiers to give up. This shows how deepfakes can be used to confuse people and change what they believe. By 2026, these fakes have become so common that experts say nearly 90% of what we see online could be made by AI [4].

The large use of social media platforms such as Facebook, Instagram, Twitter and YouTube has lead to spread Deepfake Content. Nowadays, everyone have smartphones by using user-friendly editing tools, people can easily create and share digital media online. Due to open-source deepfake generation tools such as Faceswap, StyleGAN and SimSwap anyone can easily create realistic manipulated content. As a result, the risk of deepfake misuse has increased, creating challenges for digital security, privacy protection and public trust [6]. To identify this problem, researchers are working on Deepfake Detection Techniques. The aim of these techniques is to identify digital media is real or fake. In previous days, deepfakes focused on unnatural shadows, facial distortions and lighting difference. Later, expert started looking for digital footprints left behind by the computer during deepfake generation process. Modern deepfake detection systems are use machine learning and deep learning models. These programs train by using thousands of media to understand difference between real and fake one. Some system also check for natural human behaviour such as eye blinking patterns, facial movements and speech synchronization to detect manipulated videos [9].

Many countries are using Digital and Electronics Voting System to improve the efficiency and transparency of elections. Digital voting systems can simplify the voting process, reduce manual work and provide faster vote counting. But digital voting systems face several security challenges. One of the major problem is voter impersonation and fake voting. In many regions such as rural areas, identity verification method is weak due to this individuals can cast vote illegally so it can affect the election result.

©IJRASET: All Rights are Reserved

To improve security in voting systems, many technologies such as biometric authentication have been introduced. Biometric methods use unique human characteristics such as fingerprints, iris patterns or facial features to verify identity. Facial Recognition has become one of the most widely used approaches because it is convenient and does not require physical contact with devices. A facial recognition system captures a person's image using a camera and compares it with stored images in a database to confirm identity. Deepfakes have created new risks for security systems that use our faces. High-quality fake images and videos can trick a computer into thinking a stranger is actually the real owner. This allows hackers to prevent to be other people to get into private accounts. We now need smarter systems that don't just check who the person is. New systems must also prove that the image and video itself is real and not a digital trick.

To address this problem, this research proposes a Deepfake Detection Based Smart Voting System designed to improve the security and transparency of the digital voting process. The proposed system integrates deepfake detection techniques and facial recognition technology to ensure that only genuine voters are allowed to cast their votes.

In the proposed system, the voter first logs into the system using their Voter ID. After successful login, the system activates a camera to capture a live image of the voter. The captured image is first analysed using a deepfake detection model to determine whether the image is real or artificially generated. If the system detects that the image is fake or manipulated, the voting process is blocked to prevent fraudulent activity. If the captured image is verified as genuine, the system proceeds to the next step of face verification. In this step, the live captured image is compared with the voter's profile picture stored in the database. If the images match successfully, the system confirms the voter's identity and allows them to cast their vote. If the images do not match, the system denies access to prevent unauthorized voting.

By combining deepfake detection and facial verification technologies, the proposed system aims to prevent fake voting, reduce impersonation and ensure that only genuine voters participate in elections. This approach can improve the reliability, transparency and security of digital voting systems and help build greater trust in modern election technologies.

The main contributions of this research are summarized as follows:

1) Development of a Deepfake detection based verification system for secure voting.
2) Integration of Facial recognition and deepfake detection for multi-layer voter authentication.
3) Prevention of Fake voting and Voter impersonation in digital voting systems.
4) Improvement of security, transparency and reliability in the election process.

The rest of this paper is organized as follows. Section II presents a review of related research in deepfake detection and digital voting security. Section III explains the proposed system architecture and methodology. Section IV discusses the experimental setup and system results. Finally, Section V concludes the paper and presents future research directions.

II. LITERATURE REVIEW

Edwards et al. presented a detailed review of deepfake technology and the methods used to detect manipulated media. The paper explains how advancements in artificial intelligence and deep learning have made deepfake content more realistic, making it difficult to distinguish between real and fake videos, images and audio. The authors studied different deepfake detection approaches, including various architectures, machine learning techniques and datasets used by researchers. The review highlights that many detection systems depends heavily on the quality and diversity of datasets used for training. One major challenge identified is the lack of diverse and well-balanced datasets, which can reduce the ability of detection models to perform well on new or real-world data. The study concludes that improving dataset diversity, standardization and ethical considerations is important for developing more accurate and reliable deepfake detection systems in the future [4].

Mubarak et al. conducted a comprehensive survey on deepfakes and their detection in visual, audio and textual formats. The study explains how artificial intelligence has made it easier to generate fake media such as manipulated videos, synthetic voices and AI-generated text. The authors discuss the serious impact of deepfakes on society, including misinformation, political manipulation, loss of trust in media and cybersecurity threats. The paper reviews different detection techniques used to identify fake content in images, audio and text and compares their strengths and weaknesses. The study also highlights that text-based deepfakes are often ignored in research even though they can strongly influence online discussions and spread misinformation. The authors conclude that there is a need for a unified detection framework that can identify different types of deepfakes in real time. They also emphasize the importance of adaptable detection systems, public awareness and proper regulations to reduce the negative impact of deepfake technology [6].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Patel et al. studied deepfake generation and detection techniques using machine learning and deep learning models. The paper explains how technologies such as generative adversarial networks (GANs) are used to create fake images, videos and audio through methods like face swapping and voice conversion. The authors reviewed different detection models and datasets used to identify deepfake content. The study highlights challenges in developing accurate and robust detection systems and emphasizes the need for scalable and reliable models. The authors conclude that improving detection techniques and increasing public awareness are important to reduce the negative impact of deepfake technology [9].

Jung et al. proposed a deepfake detection method called DeepVision, which identifies fake videos by analysing human eye blinking patterns. The system tracks changes in blinking behaviour, such as blink frequency, duration and timing because deepfake videos often fail to reproduce natural blinking patterns. The method uses machine learning and statistical analysis to detect abnormal blinking patterns in videos. The study showed that the proposed approach achieved about 87.5% accuracy in detecting deepfake videos. The authors concluded that analysing biological behaviours like eye blinking can improve deepfake detection, although the method may have limitations in some cases [8].

Reghava et al. presented a study on deepfake detection using artificial intelligence and deep learning techniques. The paper explains how deep learning can create highly realistic fake images and videos, which may threaten privacy, democracy and national security. The authors reviewed different algorithms used to generate deepfakes and the detection methods developed to identify manipulated media. The study also discusses current challenges, research trends and future directions in deepfake detection. The authors emphasize the importance of developing reliable detection systems to prevent misinformation and misuse of digital content. They conclude that continuous research, improved detection technologies and public awareness are necessary to effectively reduce the risks associated with deepfake technology [5].

Rana et al. presented a systematic literature review on deepfake detection by analysing many research studies related to this field. The paper reviews different detection techniques and classifies them into categories such as deep learning methods, classical machine learning methods, statistical approaches and blockchain-based techniques. The study also compares the performance of these methods using different datasets. The authors found that deep learning models, especially convolutional neural networks (CNN), are widely used and provide better accuracy in detecting deepfake content. The paper concludes that although deep leaning techniques show strong performance, deepfake detection still faces many challenges and requires further research to develop more reliable detection systems [2].

Son et al. proposed a deepfake detection framework that improves the ability of detection models to work on different types of deepfake videos. The method uses supervised contrastive learning and a dual-stream architecture to analyse both spatial and temporal features of videos. A 3D CNN is used to capture motion information, while a 2D CNN extracts facial images features and the combined features are classified using an SVM model. The system was tested on multiple datasets and showed better performance in detecting unseen deepfake techniques. The study concludes that learning stronger feature representations can improve the generalization and reliability of deepfake detection systems [7].

Bagde et al. studied deepfake detection using deep learning techniques. The paper explains how advancements in artificial intelligence and machine learning have made it possible to create higly realistic fake images and videos that can spread misinformation and cause social harm. The authors reviewed different tools and algorithms used for creating deepfakes and focused on methods used to detect manipulated media. The study highlights challenges in identifying deepfakes because they closely resemble real content. The authors conclude that effective detection depends on good training good, strong models and continuous research to develop more reliable deepfake detection systems [1].

Ahmed et al. presented a review of visual deepfake detection techniques and the tools used to create and detect manipulated media. The paper explains different deepfake generation methods such as face swap, facial reenactment and synthetic face creation. The authors analysed various detection approaches based on spatial, temporal, frequency and spatio-temporal features. The study also discussed commonly used datasets, detection models and their limitations. The authors concluded that although many detection techniques have been developed, challenges such as real-time detection, high computational requirements and accuracy still remain and more robust methods are needed in future research [3].

III. METHODOLOGY

The proposed Deepfake Detection Based Smart Voting System is designed to increase the security and trustworthiness of digital voting. Many online voting platforms face issues such as identity theft, voter impersonation, and the misuse of manipulated images or videos. With the rapid development of artificial intelligence, deepfake technology can create realistic fake faces that may trick identity verification systems. To address this problem, the proposed system integrates deepfake detection with facial recognition to verify the authenticity of voters before allowing them to cast a vote.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

The system follows a sequence of stages that include authentication, live image capture, deepfake analysis, facial verification, vote submission, secure storage of votes, result generation, and multiple security controls. Each stage adds an extra layer of protection to ensure that the voting process remains fair and secure.

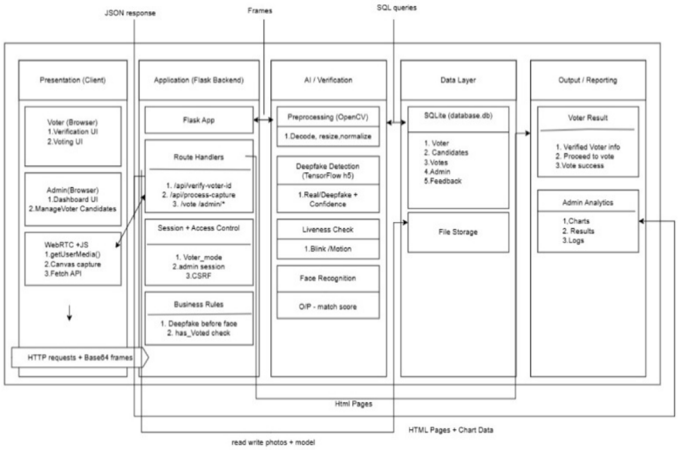


Fig 1. System Architecture

A. User Authentication

The first stage of the system is user authentication. In this step, a voter enters the voting portal and logs in using their Voter ID and password. These credentials are checked against the information stored in the system database. If the entered details do not match the stored records, the system immediately rejects the login attempt and displays an error message. This prevents unauthorized users from accessing the voting platform. When the login details are correct, the system allows the voter to move forward to the next stage. This step serves as the initial security layer and ensures that only registered voters can access the system.

B. Live Image Capture

After successful login verification, the system activates the device camera to capture a real-time image of the voter. The purpose of this step is to confirm that the voter is physically present during the voting process. Instead of allowing users to upload images, the system captures the photo directly through the camera. This approach reduces the possibility of using edited photos, stored images, or pictures of another individual. The captured image represents the voter's current facial appearance and is then sent to the next stage for analysis. Using live image capture helps the system rely on real-time data rather than static
or potentially manipulated images.

C. Deepfake Detection

The captured image is then processed by the deepfake detection module. Deepfake technologies use advanced machine learning models to generate highly realistic images or videos that may appear genuine to humans. However, these artificial images often contain subtle inconsistencies that can be detected through specialized algorithms. The deepfake detection model examines different aspects of the image, including facial texture, lighting patterns, pixel distribution, and possible digital artifacts created by deepfake generation tools. By analysing these characteristics, the system determines whether the image is authentic or artificially generated. If the model identifies the image as fake or manipulated, the system immediately stops the voting process and displays a warning message. This prevents attackers from using synthetic media to impersonate real voters.

D. Facial Recognition Verification

If the deepfake detection stage confirms that the image is genuine, the system proceeds to facial recognition verification. During this step, the captured live image is compared with the voter's registered profile image stored in the database. Facial recognition algorithms analyse important facial features such as the distance between the eyes, nose shape, facial landmarks, and overall facial structure. These features are converted into a digital representation and matched with the stored facial data. If the system finds a match, the voter's identity is confirmed and they are granted access to the voting module. If the images do not match, access is denied. This process ensures that only the legitimate voter associated with the account can continue to vote.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

E. Voting Process

Once the voter's identity has been verified successfully, the system allows the user to enter the voting interface. In this section, the voter can view the list of candidates participating in the election. The voter selects their preferred candidate and submits their vote through the system. Before recording the vote, the system performs an additional verification check to confirm that the voter has not already voted. If the system detects that the voter has previously submitted a vote, it blocks the action and displays a notification indicating that the vote has already been recorded. This mechanism prevents duplicate voting and ensures
that each voter can vote only once.

F. Vote Storage and Database Management

After a vote is successfully submitted, the system securely stores the voting data in the database. The database maintains all necessary information related to the election, including voter details, candidate information, and vote records. While recording the vote, the system ensures that voter anonymity is preserved so that the identity of the voter cannot be linked to the selected candidate. At the same time, the vote count for the chosen candidate is automatically updated. Proper database management helps maintain the integrity of the election data and protects it from unauthorized changes or manipulation.

G. Result Management

The result management module is responsible for calculating and presenting the final election results. Once the voting period ends, the system analyses the stored voting data and calculates the total votes received by each candidate. These results are displayed through an administrator panel, which can only be accessed by authorized personnel. This controlled access ensures that the results remain secure and are handled by trusted authorities. Automated vote counting also reduces the possibility of human errors and speeds up the result declaration process.

H. Security Measures

The proposed voting system includes multiple security mechanisms to safeguard the election process. These mechanisms include login authentication, real-time image capture, deepfake detection, facial recognition verification, and duplicate vote prevention. Each step contributes to strengthening the overall security of the system. The integration of artificial intelligence technologies such as deepfake detection and facial recognition significantly reduces the risk of voter impersonation and digital manipulation. By combining these technologies, the system creates a more reliable and transparent digital voting environment, helping increase public confidence in modern electronic voting systems.

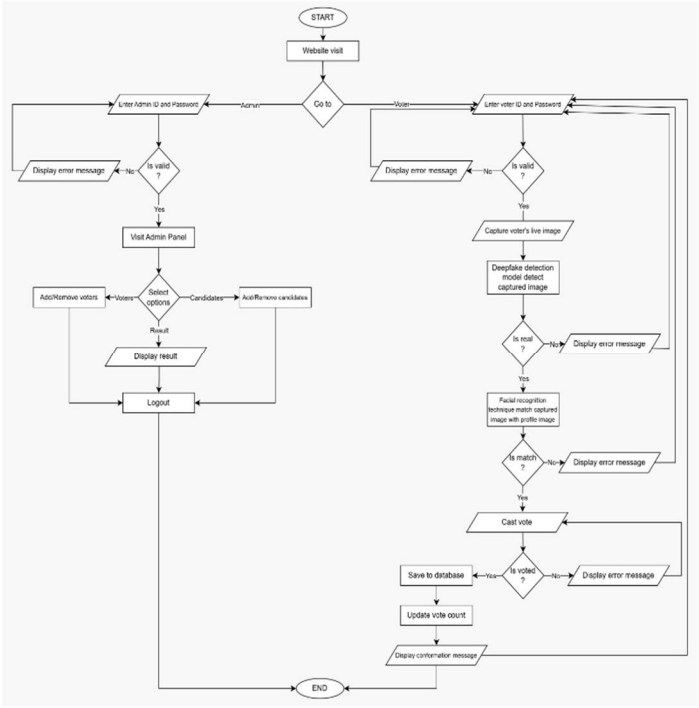


Fig 2. System Flowchart

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

IV. RESULTS AND DISCUSSION

The performance of the proposed deepfake detection model was evaluated using several important metrics such as accuracy, precision, recall, and F1-score. These evaluation measures help in understanding how well the classification model can distinguish between fake and real images. Accuracy shows the overall correctness of the model, precision measures how many predicted fake images are actually fake, recall indicates how well the model detects all fake images, and the F1-score provides a balance between precision and recall.

The mathematical formulas used to calculate are given below:

1) Accuracy = (TP + TN) / (TP + TN + FP + FN)
2) Precision = TP / (TP + FP)
3) Recall = TP / (TP + FN)
4) F1-Score = 2 × (Precision × Recall) / (Precision + Recall)

Table 1. Performance Analysis Of Deefake Detection Model

	Precision	Recall	F1-Score	Support
0	0.857788	0.760	0.805938	500.000
1	0.784560	0.874	0.826868	500.000
Accuracy	0.817000	0.817	0.817000	0.817
Macro Avg	0.821174	0.817	0.816403	1000.000
Weighted Avg	0.821174	0.817	0.816403	1000.000

Based on the testing results, the model achieved an overall accuracy of 0.817 (81.7%) on the dataset. The classification report shows the detailed performance of the model for both classes. In the dataset, class "Fake" represents manipulated images, while class "Real" represents genuine images. For the fake class, the model obtained precision of 0.857, recall of 0.760, and F1-score of 0.806, with a support of 500 samples. This indicates that most of the images predicted as fake were correctly identified, although some fake images were not detected by the system.

For the real class, the model achieved precision of 0.785, recall of 0.874, and F1-score of 0.827, also with 500 samples. The higher recall value indicates that the model correctly identified a large number of real images present in the dataset. This shows that the system performs reasonably well in recognizing genuine images without incorrectly labelling them as fake.

The macro average values for precision, recall, and F1-score are 0.821, 0.817, and 0.816 respectively. Similarly, the weighted average values for precision, recall, and F1-score are also 0.821, 0.817, and 0.816. These values indicate that the model maintains balanced performance across both classes and that the prediction results are consistent throughout the dataset.

In total, the model was tested on 1000 samples, and the evaluation results show that the system performs effectively in identifying deepfake content. The precision value indicates that the model makes fairly accurate predictions when labelling images as fake, while the recall value shows that it detects a significant portion of fake content present in the dataset. The F1-score further confirms that the model maintains a balanced relationship between precision and recall.

These results demonstrate that the proposed deepfake detection model is capable of providing reliable classification performance. Although a few misclassifications occur, the overall prediction accuracy remains satisfactory. Such performance is useful in applications like digital media verification, social media monitoring, and cybersecurity, where detecting manipulated images is important. By accurately identifying fake media, the system can help reduce the spread of misleading or manipulated information and support the development of more trustworthy digital platforms.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

To evaluate the performance of the proposed deepfake detection system, a confusion matrix is used. The confusion matrix helps in analysing how well the classification model performs by comparing the actual class labels with the predicted class labels generated by the model. It provides a detailed view of the prediction results and helps identify both correct and incorrect classifications. The matrix consists of four important components: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). These values make it easier to understand how effectively the model distinguishes between fake and real images.

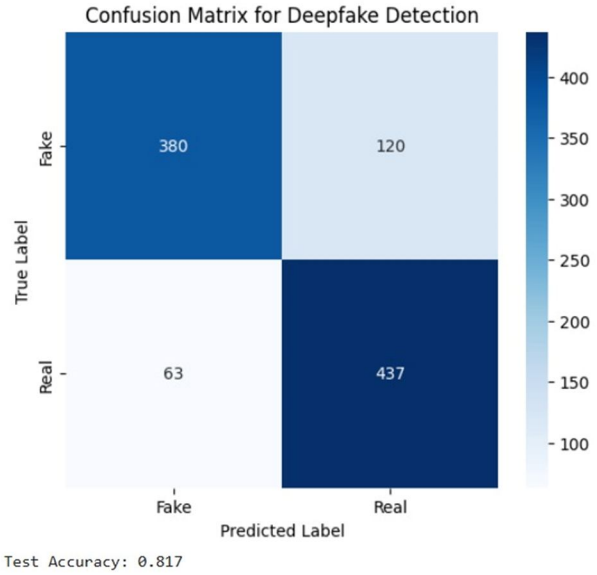


Fig 3. Confusion Matrix

According to the confusion matrix shown in Figure 3, the model correctly classified 380 fake samples as fake, which are known as True Positives (TP). This indicates that the model successfully detected manipulated or fake content present in the dataset. In addition, the model correctly identified 437 real samples as real, which are referred to as True Negatives (TN). This shows that the system is capable of recognizing genuine images without falsely marking them as fake. Correct identification of both fake and real samples is important for improving the reliability of the detection system.

However, some misclassifications are also observed. The model predicted 63 real samples as fake, which are called False Positives (FP). This means that a few genuine images were incorrectly identified as fake by the model. Similarly, the model predicted 120 fake samples as real, which are known as False Negatives (FN). This indicates that some manipulated images were not detected by the system. Although these errors exist, their number is still lower compared to the number of correct predictions made by the model.

Overall, the model was tested on a total of 1000 samples, out of which 817 samples were classified correctly. Based on these results, the system achieved an accuracy of approximately 81.7%, which means that the model correctly predicts the class of most samples in the dataset. In addition to accuracy, other performance measures such as precision, recall, and F1-score can also be derived from the confusion matrix to further evaluate the effectiveness of the model. These metrics help in understanding how well the system identifies fake content and how reliably it avoids incorrect predictions.

From the confusion matrix results, it can be concluded that the proposed deepfake detection model performs effectively in distinguishing between fake and real media. The number of correct predictions is significantly higher than the number of incorrect predictions, indicating good model performance. Although a few misclassifications are present, the overall results show that the system is capable of detecting deepfake content with reasonable accuracy. Therefore, the system can be considered useful for identifying manipulated digital media and helping reduce the spread of deepfake content.

To evaluate the effectiveness and reliability of the proposed deepfake detection voting system, multiple practical test cases were conducted. The objective of these tests was to ensure that the system correctly authenticates legitimate users while preventing unauthorized access, identity misuse, and deepfake-based attacks. The testing process focused on verifying the system's facial recognition and deepfake detection capabilities under different scenarios.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

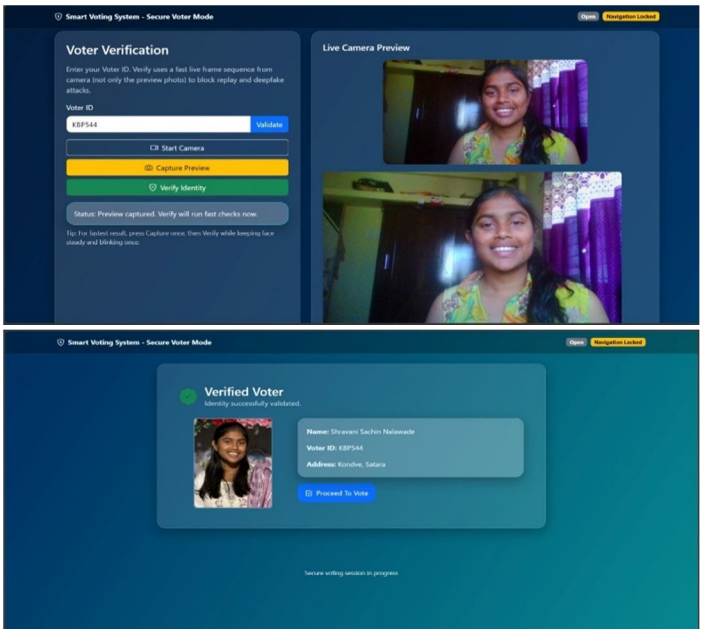


Fig 4. Successful Login of Authorized Voter

In the first test case, a registered voter attempted to log in using their valid voter ID along with their genuine facial image captured through the system camera. The system successfully verified the user's identity by matching the captured image with the stored facial data in the database. After successful authentication, the system redirected the user to the voting page, allowing them to cast their vote. This result indicates that the authentication mechanism works correctly for legitimate users and ensures a smooth voting experience.

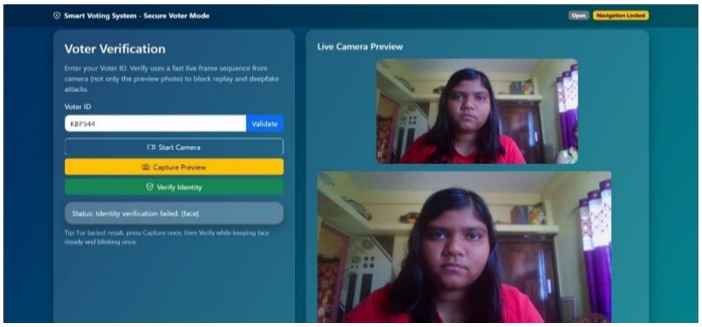


Fig 5. Face Recognition Mismatch during Voter Authentication

In the second test case, a valid voter ID was entered but the facial image of another person was presented instead of the registered user. During the verification process, the system compared the captured facial features with the stored biometric data and detected a mismatch. As a result, the system displayed an error message and denied access to the voting page. This test confirms that the system is capable of preventing identity impersonation and unauthorized voting attempts.

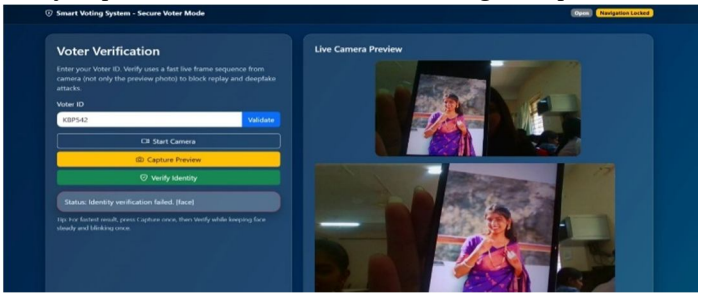


Fig 6. Authentication Attempt Using User Photograph on Mobile Screen

In this test case, a valid voter ID was entered and instead of the actual user, a photograph of the registered person was shown on a mobile phone screen in front of the camera. The system captured the image and processed it through the face verification and deepfake detection module. During analysis, the system recognized that the input was a still photo rather than a live person. Because of this, the authentication process failed and the system displayed an error message. The user was not allowed to continue to the voting stage. This test confirms that the system can detect photo spoofing attempts and helps protect the voting system from unauthorized access.

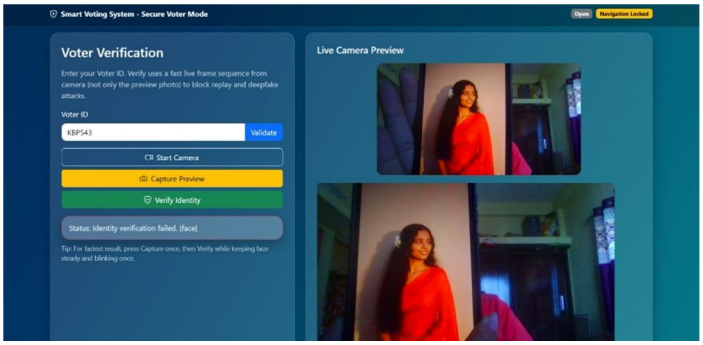


Fig 7. Deepfake Face Detected from Mobile Screen and Access Denied

In the fourth test case, a valid voter ID was used along with a deepfake facial image displayed on a mobile phone screen in front of the camera. The system analysed the captured input using the deepfake detection model and identified inconsistencies associated with manipulated media. Consequently, the system rejected the authentication request and generated an error message, preventing the user from proceeding further. This demonstrates the system's ability to detect deepfake-based attacks and maintain the integrity of the voting process.

Additionally, the system was tested multiple times to ensure consistency, reliability, and robustness of the authentication mechanism. The results showed that the system consistently allowed access only to verified users while effectively blocking fraudulent attempts. The integration of facial recognition and deepfake detection techniques significantly enhances the security of the voting platform by reducing the risk of identity theft, impersonation and manipulation through synthetic media.

Overall, the testing outcomes indicate that the proposed system provides a secure and reliable digital voting environment. Legitimate voters can successfully access the voting interface, while unauthorized users and deepfake attempts are effectively detected and rejected. These results highlight the potential of the system to improve trust, transparency, and security in modern electronic voting systems.

V. CONCLUSION

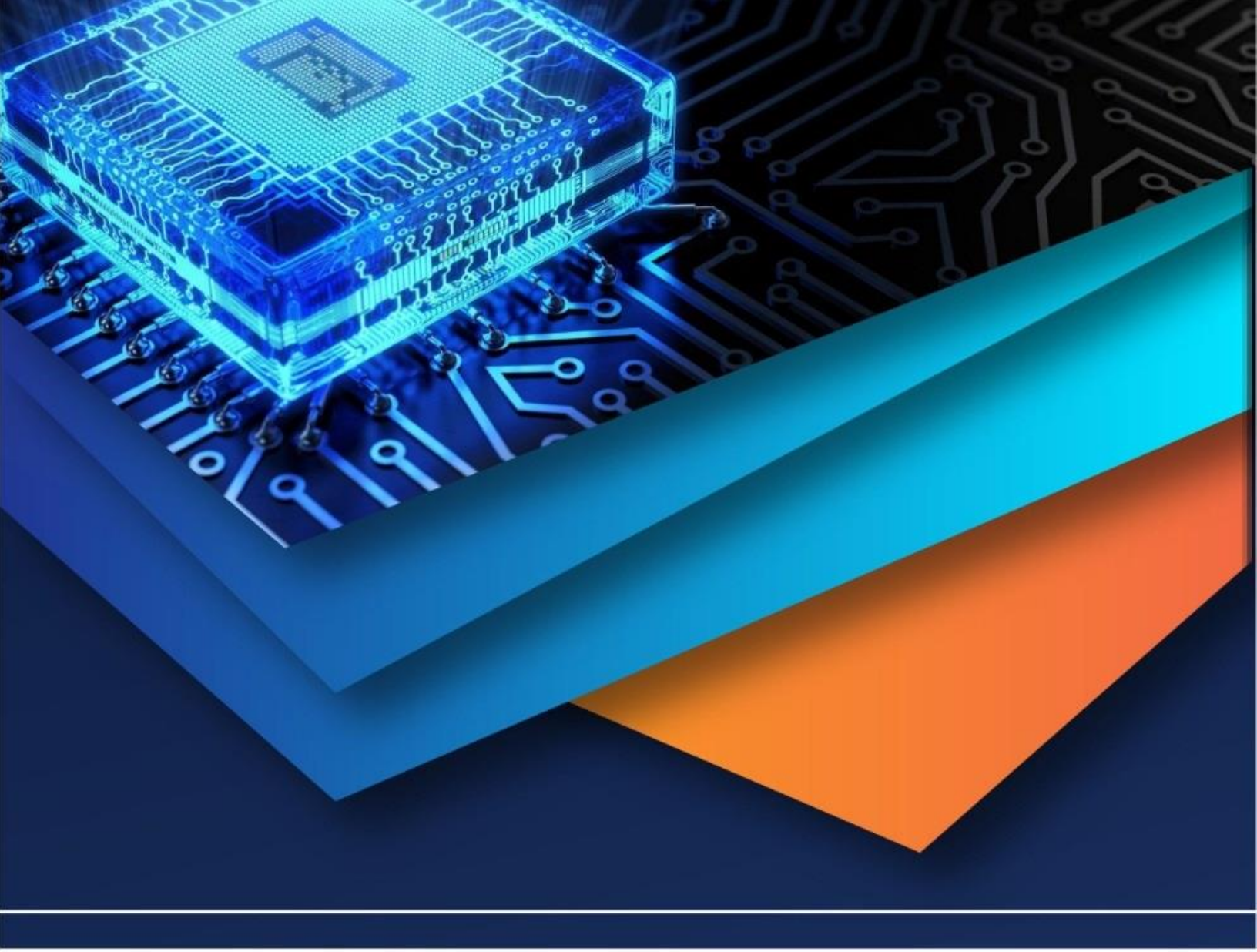
In this project, a deepfake detection-based secure voting system was developed to enhance the reliability and security of digital voting. The system integrates facial recognition and deepfake detection techniques to verify the identity of voters before allowing them to access the voting platform. A machine learning model was implemented and evaluated using performance metrics such as accuracy, precision, recall, and F1-score, along with a confusion matrix to analyse classification performance. Experimental testing was also conducted under different scenarios, including authentication with a valid user, attempts using another person's image, and deepfake image attacks. The results demonstrated that the system successfully allows legitimate users to access the voting page while effectively blocking unauthorized users and deepfake-based attempts. These findings indicate that the proposed approach can improve security, transparency, and trust in electronic voting systems. In the future, the performance of the deepfake detection model can be further improved by using larger and more diverse datasets, as well as applying advanced deep learning architectures to increase detection accuracy. Additionally, the system can be extended for real-time applications, enabling faster and more reliable identity verification in practical voting environments. Future work may also focus on optimizing the model for real-time processing, scalability, and deployment in large-scale voting systems, making it suitable for use in real-world electoral processes and other security-sensitive applications.

REFERENCES

[1] Aparna Bagde et al., "Deep fake Detection using Deep Learning", International Journal of Science, Engineering and Technology, 2023, ISSN: 2348-4098
[2] MD Shohel Rana et al., "Deepfake Detection: A Systematic Literature Review", IEEE Access, Feb 2022, DOI: 10.1109/ACCESS.2022.3154404
[3] Naveen et al., "Visual Deepfake Detection: Review of Techniques, Tools, Limitations, and Future Prospects", IEEE Access, Dec 2024, DOI: 10.1109/ACCESS.2024.3523288

[4] Peter Edwards et al,. “A Review of Deepfake Techniques: Architecture, Detection, and Datasets”, IEEE Access, Octo 2024, DOI: 10.1109/ACCESS.2024.3477257
[5] Raghava M S et al., “AI DEEP FAKE DETECTION RESEARCH PAPER”, IJNRD, Octo 2023, ISSN: 2456-4184
[6] Rami Mubarak et al., “A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats”, IEEE Access, Dec 2023, DOI: 10.1109/ACCESS.2023.3344653
[7] Sangho Son et al., “Advancing Generalization in Deepfake Detection: Supervised Contrastive Representation Learning With Dual Stream Spatio-Temporal Features”, IEEE Access, Aug 2025, DOI: 10.1109/ACCESS.2025.3598782
[8] Tackhyun Jung et al., “DeepVision: Deepfakes Detection Using Human Eye Blinking Patter”, IEEE Access, April 2020, DOI: 10.1109/ACCESS.2020.2988660
[9] Yogesh Patel et al., “Deepfake Generation and Detection: Case Study and Challenges”, IEEE Access, Dec 2023, DOI: 10.1109/ACCESS.2023.3342107

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)