

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 5, May 2024

AI Based Smart Voting using Face Recognition

Dr. Anitha T N¹, Sai Kian T N², B P Satwick³, Ameetreddy⁴, Shravan M⁵

HOD & Professor, Department of CSE¹ B.E. Students, Department of CSE^{2,3,4,5} Sir M Visvesvaraya Institute of Technology, Bangalore, India

Abstract: As society changes and technology plays a bigger role in shaping daily life, the security, effectiveness, and accessibility of traditional voting systems are being questioned. This research presents a novel approach to create an online smart voting system using facial recognition technology. The technology promises to improve the convenience and integrity of electoral processes by integrating cutting-edge facial recognition algorithms with secure online voting platforms. It also addresses common problems such as voter fraud, long lines, and geographical restrictions. The system verifies each vote's legitimacy by registering voters' facial biometric information, securely storing it in a centralized database, and providing live facial authentication while voting. Strong security protocols, such as multi-factor authentication and encryption methods, are notably used to protect voter privacy and prevent election results manipulation. Additionally, the system's removal of the requirement for voters to physically be present at polling places improves voter accessibility, especially for underprivileged or geographically separated groups, which encourages higher levels of political engagement. Through extensive testing and validation that includes both simulated and real-world voting scenarios, the efficacy of this novel approach will be closely examined. Consent, transparency, and data privacy are ethical issues that need to be properly addressed in order to ensure compliance with legal and regulatory requirements. In conclusion, the face recognition online smart voting system is a ground-breaking advancement in electoral technology that might fundamentally alter the way elections are held by enhancing their integrity, efficiency, and inclusivity

Keywords: AI-Based, Facial Recognition, Authentication, Web-Based Application, Security Enhancement

I. INTRODUCTION

Increased calls in recent years for convenient and accessible modes of voting have led to the exploration of innovative solutions that balance security and inclusivity. Face recognition technology presents an attractive pathway toward catering to these requirements by virtue of its ease in use and reliability in the verification of identity without necessarily prejudicing the integrity of the voting exercise. However, the prospects of admissibility in this context must of necessity include and be informed by ethical, legal, and technical considerations. Key among them is privacy, potential bias in algorithmic decision-making, and the need for a strong cybersecurity posture. Moreover, it calls for public acceptance and trust in the technology developed, putting at the heart of this effort transparent communication and stakeholder engagement in the development and deployment process. The paper, therefore, tries to look into opportunities and challenges that face the adoption of face recognition technology in moving the democratic process forward.

II. LITERATURE REVIEW

Firas I. Hazzaa and colleagues introduced a novel approach titled "Web-Based Voting System Utilizing Fingerprint Technology" aimed at enhancing the efficiency and security of the voting process. Their system leverages web technology to make voting more accessible and effective. The proposed system allows voters to verify their identity using fingerprint authentication, which is then cross-referenced with the stored copy in the database. This implementation ensures a reliable and secure voting process, reducing the chances of fraud. Additionally, the system employs minutiae-based fingerprint recognition, enhancing accuracy and overall system performance.

Swapnil Singh and Krunal Patil introduced a revolutionary system titled "Smart Voting System Using Facial Recognition" designed to enable online voting as an alternative to traditional manual method. The initial phase

Copyright to IJARSCT www.ijarsct.co.in DOI: 10.48175/IJARSCT-18454



330



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 5, May 2024

involved developing a login mechanism where voters were assigned unique IDs to cast their votes securely. This system utilized convolutional neural networks (CNNs) and Haar cascade algorithms to train the dataset for accurate

identification. The subsequent phase focused on face detection using a C++ toolkit and labeling faces for recognition. Ultimately, this innovative approach ensured a secure and legal voting process, enhancing the overall integrity of the electoral system.

The integration of biometric authentication with Electronic Voting Machines (EVMs) provides enhanced security by verifying voter identity through unique biometric traits like fingerprints. This dual authentication system, coupled with voter IDs, significantly reduces the risk of fraud in the voting process. Real-time SMS confirmations to voters' registered mobile phones offer immediate validation of their cast votes, ensuring accuracy and transparency. Utilizing cloud-based storage improves data management efficiency, while GPS tracking helps prevent theft or tampering of voting machines. Overall, this proposed system offers a comprehensive solution to traditional voting system challenges, bolstering integrity, security, and transparency in electoral processes.

Ganesh Prabhu S, Prabu S, and R.R. Thirrunavukkarasu introduced an innovative system called the "Smart Online Voting System." This system operates using Arduino UNO, an LCD display, and push buttons. Within the Arduino UNO, RFID technology is utilized to store user data securely. Voters can then participate in elections online, although this method does require specific hardware components to function effectively.

The paper [5] introduces an advanced online voting system focused on security, integrating face recognition technology and multi-factor authentication. The authors detail the system architecture, emphasizing the incorporation of face recognition for user verification. Additionally, they discuss the implementation of multi-factor authentication via OTP to bolster security measures. Through simulations and evaluations, the system demonstrates its capability to facilitate secure and trustworthy online voting processes.

III. METHODOLOGY

The research methodology pertains to the systematic approach adopted in the development, deployment, and evaluation of the Smart Voting System, with advanced features of facial recognition. The architecture of the system is based on a client-server model where Flask has been adopted for front-end framework development for user interfaces and mysql for back-end database management. The data collection in voter registration starts with the personal information of the user, like name, Aadhar ID, voter ID, and captures his/her facial image with the help of a camera module for identity verification.

The integration of face recognition is a major feature in the system, done with the help of opencv and Haar Cascade Classifiers. These algorithms allow the system to detect and recognize the face based on training given to the LBPH Face Recognizer model. The model is trained with the help of captured facial images fed into the system and makes a database of known faces, which can be used in the voting process to authenticate the identity of the voter. This guarantees that only those who are authorized will be able to cast their votes. This measures maintain the security and the integrity of the system.

In addition, the user registration is fortified with extra security features, such as email verification using SMTP and OTP mechanisms. Such a two-step authentication process will certainly add an extra security layer, validate the identity of the user before he is allowed access to the voting functionality. The administrator has been given tools for nominee management to add, edit, and remove nominees from the system. The system will also do the validation check to ensure the uniqueness of the nominee and the symbol associated with him to avoid duplication and maintain accuracy in the voting process.

The act of voting itself is also simplified and secure, whereby verified users leverage the power of facial recognition to authenticate them before casting their ballots. The system detects and prevents duplicate voting through algorithms, hence preserving the integrity of the electoral process. Maintenance of the LBPH Face Recognizer model is performed in periodic updates to improve recognition accuracy and to adapt to emerging facial features.

The analysis of the results is very important for real-time statistics in voting, nominee popularity, and the general trend of voting. The data is provided to administrators through a well-designed and user-friendly interface, and its interpretations can be used as important information for strategic policy-making. The security issues that are cared for

Copyright to IJARSCT www.ijarsct.co.in DOI: 10.48175/IJARSCT-18454



331



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 5, May 2024

include encrypted communication and security data storage to protect personal information and voting data, and ethical issues—addressing the problems of privacy and fairness in the use of facial recognition technology.

There exist performance metrics in the definition that will help to test system responsiveness, scalability, and facial recognition accuracy. These metrics give meaningful feedback with regard to the optimization of system performance and user experience. Admitting that there are limitations to the current system, some future directions include developing advanced AI algorithms for facial recognition, developing mobile apps to extend accessibility, and exploring regulatory requirements for electoral technology.



Fig. 1: User Module Architecture



IV. RESULTS

Fig 2: User Registration

Copyright to IJARSCT www.ijarsct.co.in

DOI: 10.48175/IJARSCT-18454





International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 5, May 2024

				HOME	ADMIN TR	AIN
U	nverifie	d Voters				
Aadhar ID	Name	Email	Action			
31	satwick bp	satwickbp@gmail.com	Verify			
31 49977275776	satwick bp Ameetreddy Dakareddy	satwickbp@gmail.com ameetreddy01@gmail.com	Verify			





Fig 4: Face Recognition For Voting





International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 5, May 2024



Fig 6: Result

V. CONCLUSION

An online voting system with face recognition can be one of the better solutions to meet such challenges and pitfalls of a conventional paper-based election. Various cases of fraudulent voting, as reported from different parts of India, further call for safer and more reliable ways of voting. Our proposed system, using face recognition for voter identification and authentication, offers many benefits. Enhanced security and integrity of the vote, since only the valid voters would be able to cast their vote, hence reducing the chances of bogus or duplicate votes. Further, it makes the whole process of voting easier by avoiding the time-consuming manual verification of voter ID cards.

Such a system, if implemented, leads to tremendous improvements in the electoral process for transparency, accuracy, and efficiency. It does not only address the challenges of fraudulent voting but further improves the accessibility and convenience of the voters. However, security, privacy, and technological infrastructure are very sensitive issues in the adoption of online voting systems. Cybersecurity threats should be defended against with corresponding measures able to protect the privacy and integrity of voters' data. In a nutshell, the development of an online voting system with face recognition technology means modernization of electoral processes, a reliable and safe platform for democratic expression, while reducing the risks of the traditional paper-based voting system.

REFERENCES

- [1]. Firas.I.Hazzaa, Seifedinekadry, Oursamakareem, zein,"Web Based Voting System Using fingerprint Design And Implementation", Vol.2, Issue.4, Dec 2014.
- [2]. Swapnil Singh, Krunal Patil, Shaik Aftab, Kapil Chaudhary, Prof. Sushma A Shirke, "Smart Voting System Using Face Recognition", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 2, May 2022, Page No: 52-57.
- [3]. BalaMurali, Potru Sarada Sravanthi, B. Rupa." Smart and Secure Voting Machine using Biometrics", 2020 Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC), September 2020.
- [4]. Ganesh Prabhu S, Prabu.S, R.R.Thirrunavukkarasu, Nizarahammed.A, Raghul.S, P. Jayarajan "Smart Voting system", 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE 2021.
- [5]. R. P. Jain and P. M. Potdar, "A secure online voting system using face recognition and multi-factor authentication," in International Journal of Computer Applications, 182(34), pp. 22–27, IEEE, 2019.
- [6]. Hasan SM, Anis AM, Rahman H, Alam JS, Nabil SI, Khalilur Rhaman M (2014) Development of electronic voting machine with the inclusion of near field communication ID cards and biometric ingerprint identifier. In IEEE 17th international conference on computer and information technology (ICMT)SSN

Copyright to IJARSCT www.ijarsct.co.in

DOI: 10.48175/IJARSCT-18454