International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 2803–2810

Towards Secure Electronic Voting Using An Improved Face Recognition Model For Electoral Fraud Detection

[1]Lalitha R, [2*]Kanimozhi Suguna S,[3]Saravanan J,[4]Shanthosh K P,[5]Vigneshwar K, and [6]Dimitrios A. Karras

[1,3,4,5]Dept. of Computer Science and Engineering

Rajalakshmi Institute of Technology, Chennai, India

[2]Assistant Professor, Dept. Of CSE, School of Computing, SASTRA Deemed University, Thanjavur, India*

[6]Professor, Department General, Faculty of Science at National and Kapodistrian University of Athens, Greece*

[1]lalitha.r@ritchennai.edu.in, [2]kanimozhi.suguna@gmail.com [3]saravananjayakumar6@gmail.com, [4]shanthosh.k.p.2017.cse@ritchennai.edu.in , [5]vigneshwar.k.2017.cse@ritchennai.edu.in, [6]dakarras@uoa.gr*

Abstract

At the heart of every democracy is a commitment to hold regular, free and fair elections. Elections empower the electorate with the right to choose who governs them. There has been a constant evolution in the voting system, with each new system getting better than the one before. Still, the possibility of electoral fraud remains, which leads to doubts regarding the result. A system that uses a facial recognition system can authenticate individuals before they cast their vote by verifying their face with the image associated with their Electoral Photo Identity Card number to prevent impersonation. Repetition of voters can be identified by running a facial recognition scan on voter's face against everyone who has already cast their vote. The system would also maintain an electronic poll book which could be used to get the count of votes registered in a particular constituency to detect ballot stuffing or tampering of Electronic Voting Machines.

Keywords: Biometric Authentication, Elections, Electoral fraud, Face recognition.

I. INTRODUCTION

Elections are an integral part of democracies. But democracies across the world face one common problem when it comes to elections: electoral fraud. Each country follows their own method to prevent this but still, electoral fraud claims are raised after most elections. Ballot stuffing, tampering of electronic voting machines, etc., remains a major concern and doubt linger in most people's mind about the current system. Thus, changes are required to the system in place to win over the trust of the electorate and conduct an election without any controversies. The system employs facial recognition to detect and deter electoral fraud in the hopes of conducting a free and fair election. Face detection and recognition has been a significant interaction tool used in the security systems, access control which has gained enough popularity in the last few decades.Face recognition is the process of comparing an input image against a database of images and determining whether there is a match or not. The first process in any face recognition algorithm is face detection. Face detection refers to identifying whether there are any faces in an image and, if present, determine the location of the faces present. The next process is to extract features from the located faces. The extracted features vary depending upon the algorithm used for face recognition. The most common features are the location

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

of the eyes, eyebrows, nose, mouth, and lips. Finally, these extracted features from the input image are compared with those in the database to perform face recognition and identify individuals.

The applications of face recognition can be classified into two categories [1]:

- *Verification:* An 1-1 matching in which an image of an unknown individual who claims an identity and the image associated with that identity compared to determine whether their claim is true. Their general use cases are in security and identity verification to authenticate and provide access to the said individual.
- *Identification:*An 1-N matching in which an image of an unknown individual is compared with a database of images of known individuals to determine their identity. It is utilized for surveillance and by the criminal justice system for identifying persons of interest.

The factors which could pose challenges for face detection and recognition algorithms are [4]:

- *Pose:*The image of a face may vary depending upon the position of the capturing device with respect to the face. It could lead to the partial or complete obstruction of certain features of the face.
- *Presence or absence of structural components:* Facial features such as beards, moustaches, and glasses may or may not be present, and they vary a lot over time.
- *Facial expression:*A person's facial expression directly affects the appearance of their face and features.
- *Occlusion:*A face could be obstructed by an object or by another person in the image.
- *Image orientation:*Rotations about the camera's optical axis causes variations to the face images.
- *Imaging conditions:*While capturing, factors like lighting and camera characteristics affect how the image appears.

II. LITERATURE REVIEW

Avinash Pratap Budaragade and Vajrashi R. Biradar [5] proposed a system which made use of a magnetic card reader device and a fingerprint scanner to authenticate the voters. The voter's personal and biometric information is stored in cloud storage. For the authentication process, the voter has to insert his magnetic strip voter ID into the magnetic card reader to retrieve his information from the database and then, undergoes biometric authentication. The system fetches the required information from the cloud using a client-server model. Theelectronic voting machine (EVM) is automatically activated once the voter is authenticated.

In [6], the authors describe about the development of an EVM which uses fingerprint as a biometric information for authentication. The EVM is designed with a microcontroller at its core, connected to the LCD display, keypad, fingerprint scanner, and GSM module. Once the authentication is done and the vote is cast, the GSM module sends a message to the registered mobile number of the corresponding voter.

Reference [7] uses near-field communication (NFC) with biometrics for authentication. The voter is equipped with an NFC card in place of an EPIC for authentication. When the NFC card is brought, with less than five centimetresdistance from the reader, it communicates with the card to retrieve the personal information and fingerprints from the database. Once it's retrieved, a fingerprint scanner is used to check whether the individual's fingerprint matches the registered fingerprint in the database.

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

In the paper [8], the authors suggest an android application that allows people to cast their votes using mobile devices. It was designed to cater to the needs of organizations, corporations, and commercial businesses to know their employee opinions. The admin can feed the queries to the application with desired options and view the result instantaneously. These can be viewed and answered using the application from anywhere.

In [9], an e-voting system built using blockchain is explored. The usage of blockchain will make the entire voting process transparent and secure. In this paper, the e-voting system has been implemented with the Ethereum platform as it is consistent and widely used. It is built as a smart contract for the Ethereum network using the Ethereum wallets and Solidity language. Once the voting process is over, the votes will be held in the Ethereum blockchain.

Amna Qureshi, David Meg´ıas, and Helena Rif`a-Pous present a VSPReP, a verifiable, secure and privacy-preserving remote polling (e-poll) system[10]. The VSPReP provides vote anonymity through distributed ElGamal cryptosystem, poll integrity and it provides verifiability using cryptographic primitives to create a complex interaction between the voting device and the server. In the same line of research Zinah J Mohammed Ameen [12] has presented a web application based on face recognition and steganography to achieve secure voting but face recognition proposed is only at basic level. Similarly, but involving a more advanced face detection model AanjanaDevi.S I et al. proposed a confidential E-Voting System using face Detection and recognition. The present paper follows similar research direction but with an improved face recognition model. There is large potential in this e-voting systems research but the most successful approaches, so far, present hybrid integral models with non-optimized components. The herein research attempts to improve one such component , the face detection and recognition , based on an improved modelling approach.

III. EXISTING SYSTEM

A large number of polling booths are set up in each constituency to conduct polling in India. A Presiding Officer is placed in charge of each booth with Polling Officers to help the process. The vote will be cast in an enclosure using an EVMor paperballots so that no one can know of the choice the voter made [3]. It is known as secret ballot.

The Election Commission has started using EVMs widely in place of paper ballots. The major concern associated with paper ballots in India was booth-capturing. EVMs were designed to discourage that by limiting the number of votes to five per minute [2]. The printed paper ballots were also more expensive and required substantial post-voting resources to count the ballots [3].

Each EVM has the names and symbols of the candidates in a constituency. A single EVM can accommodate a maximum of 16 candidates. If the number exceeds 16, then more than one EVM may be used. The voters have to press the appropriate button to vote for the candidate of their choice [3].

IV. PROPOSED MODEL

The proposed system doesn’t replace the existing system but works alongside it. It is an additional component to an existing system that facilitates voter authentication through facial recognition and liveness detection, and also keeps track of who voted. Fig. 1 represents the workflow of the face recognition algorithm used.

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

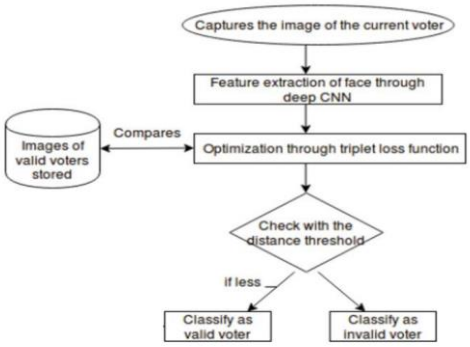


Fig 1: Face recognition workflow

The face recognition system deployed is a library that is built using dlib's state-of-the-art face recognition built with deep learning. The model has an accuracy of 99.38% on the Labelled Faces in the Wild benchmark[11].

Before the election begins, the electorate information along with their images is used to populate a database. This acts as the dataset on which facial recognition will run and extract features from their images. The extracted features are added to the database alongside the voter information. During the election, the face recognition program will compare the features extracted from the voter who is about to vote to the features in the database and liveness detection is done to ensure that it's a live individual and not a photograph of that person held up in front of the camera. The voter is authenticated through these verifications.

The system architecture for the proposed model is specified in Fig 2and the processes mentioned in the figure is explained below.

A. Adding Users

An account is made for each electoral officer and the details of the account are sent to the electoral officers. These accounts can only be created by the admin. These accounts are necessary to access the portal during an election.

B. Login

On the day of the election, the electoral officers can log in to their respective accounts from their designated polling stations. The voter authentication and voting process in a polling station won't begin until the electoral officer has logged into the system.

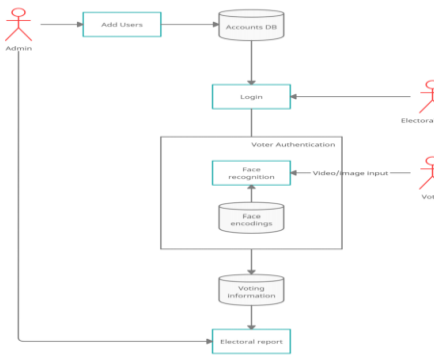


Fig 2: System architecture for the proposed system

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

C. *Face recognition*

The electoral officer enters the voter's Electoral Photo Identity Card (EPIC) number in the portal and then, the voter's facial image is captured through a webcam. This input is compared with the encodings retrieved from the database for authentication. If it's a match, the voter can vote. If not, the voter won't be allowed to vote and their details would be flagged for potential election fraud.

D. *Electoral report*

After the election ends, a report is generated using the information collected during the voting process. This gives us the total count of people who voted in a constituency and also, the people who may have tried to commit election fraud. This can be analysed before the announcement of results to find the guilty ones and punish them as the law see fit.

E. *Algorithm Used*

- *Step 1:* Start
- *Step 2:* Get the voter's EPIC number and an imageof his face as input.
- *Step 3:* Use the EPIC number to fetch the image associated with the EPIC.
- *Step 4:* Compare both the facial images using a face recognition system. Also compare the facialimage with ones who have already cast their vote.
- *Step 5:* If the voter is validated, he is allowed to vote. If not, the voter is flagged for potential electoral fraud and could be investigated further.
- *Step 6:* After the end of the voting process, a report is generated which shows the potential frauds and the number of votes cast.
- *Step 7:* End.

V. IMPLEMENTATION

A. *Input Data*

The input for the system consists of the voter's EPIC number which is used to fetch the voter details and the present image of the voter through a webcam to make a comparison and authenticate the voter.

B. *Output Data*

The output given by the system consists of a Boolean value which is used to authenticate the voter. The voter's details are also fetched and displayed to the election official. If the voter isn't who he claims to be, an alert is sent out to the authorities to take further action. An analytical report is also generated once the election is over.

The implementation can be split into modules that are described briefly below for better understanding of the implementation.

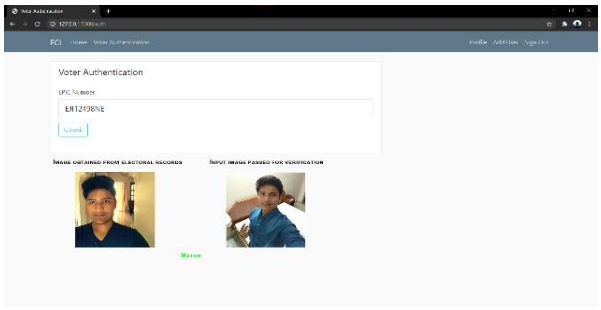
C. *Admin*

The role of the admin is to create and manage accounts for the electoral officials who are in charge of the polling stations and their supervisors. The admin alone can change the password and other details related to the accounts. Once the voting process is over, the admin can use the voting information to generate and view the electoral report which shows potential electoral fraud actions and the total number of votes cast in a given constituency/polling station.

D. *Electoral official*

The electoral official is responsible for monitoring the voter authentication process. He has to enter the incoming voter's EPIC number which allows the system to fetch the voter details, make a comparison and decide whether the individual is who they claim to be and they aren't repeat voters.

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC



E. Encryption

The password for user accounts and other sensitive information has to be encrypted and stored. A 64-bit hashing algorithm is used for this purpose while saving the data in the database. This ensures that even in the event of a security breach, information remains confidential.

F. Pre-processing

Before the deployment of the system, the voters' information of the entire electorate has to be processed and stored in a database. Then, the images associated with each EPIC is used to generate face encodings for each individual. These encoded values are used for facial recognition. Thus, they should be stored in such a manner that they can be retrieved swiftly and efficiently.

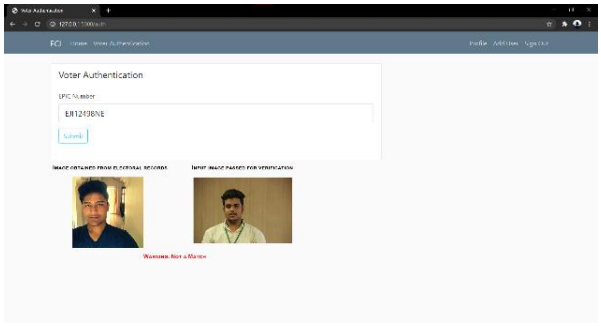


Fig 4: Experimental results on a limited sample space

G. Voter Authentication

The election official inputs the voter's EPIC number to retrieve the voter details from the database. The voter is then requested to stand in front of a webcam for the system to capture their face image and their EPIC number is collected to fetch their details. Then, the facial recognition process begins and compares the voter's face from the video/image source to the one in the EPIC. The elements of the face recognition

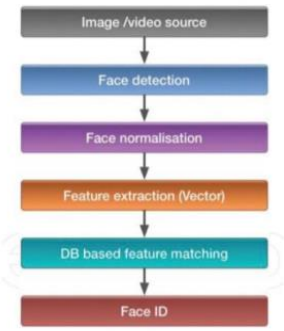


Fig 3: Elements of face recognition

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

process are shown in Fig 3.As shown in Fig 3, first, the face is detected and localized from the input source. Then it's normalized and facial features are extracted, encoded, and stored in the form of a 128-dimensional vector. The features are 128 floating-point numbers in this case which help in distinguishing between different individuals. These encoded values are compared with values from the database to identify and authenticate voters. In this way, the system determines whether the voter is who he claims to be and he hasn't already cast his vote.

VI. RESULTS AND DISCUSSIONS

The development and evaluation have shown that a DCNN trained via a triplet loss function for face recognition can provide results of far greater accuracy rivalling that of humans if the model is trained over a large dataset that accounts for the diversity and different ethnicities. As demonstrated, the proposed system works alongside the existing system of ballots and EVMs to detect and deter electoral fraud. As shown in Fig 4, the proposed system will help the law enforcement officials and election officials by identifying fraudulent voters, and the people by helping them have a fair election. The report generated after the election can be used to visualize the data in the form of heatmaps and such which could be used as input for machine learning problems that focus on voting numbers and patterns for each constituency or for a given region in general.

VII. CONCLUSION

The existing system of ballots and EVMs are under scrutiny during every election. Face recognition systemshave been present for decades now, and the recent developments in the field have increased the accuracy and efficiency of the models, rivalling humans. Thus, the proposed model which incorporates face recognition is a welcome addition that would put an end to these controversies once and for all. Each vote cast has the image of the person who cast it and the thorough verification and identification processes show better performance than humans in identifying repeat voters and individuals trying to masquerade. This would reduce the burden faced by election officers during the elections by reducing their workload and stress. After the elections, when allegations are made against them, the electoral information stored in the system can be used to exonerate them. Thus, the proposed biometric voting system would enable hosting free and fair elections by precluding illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right to democracy.

REFERENCES

[1] Jafri, Rabia &Arabnia, Hamid. (2009). A Survey of Face Recognition Techniques. JIPS. 5. 41-68.10.3745/JIPS.2009.5.2.041.

[2] MadhavanSomanathan. (2019). "India's electoral democracy: How EVMs curb electoral fraud". Brookings Institution, Washington DC. https://www.brookings.edu/blog/up-front/2019/04/05/indias-electoral-democracy-how-evms-curb-electoral-fraud/

[3] Electronic Voting Machine (EVM)–M3 User Manual (2018) https://eci.gov.in/files/file/8991-electronic-voting-machine-evm-m3-electronic-voting-machine-evm-m3-user-manual/

[4] Yang, Ming-Hsuan& Kriegman, David & Ahuja, Narendra. (2002).Detecting Faces in Images: A Survey. Pattern Analysis and Machine Intelligence, IEEE Transactions on. 24. 34 - 58. 10.1109/34.982883.

[5] Avinash Pratap Budaragade and Vajrashi R. Biradar. (2019). International Research Journal of Engineering and Technology. Volume 6, Issue 4, Pages 4089-4093.

[6] Abeesh A I, Amal Prakash P, Arun R Pillai, Ashams H S, Dhanya M, Seena R, 2017, Electronic Voting Machine Authentication using Biometric Information, INTERNATIONAL JOURNAL OF

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC

ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCETET – 2017 (Volume 5 – Issue 16).

[7] A. Das, M. P. Dutta and S. Banerjee, "VOT-EL: Three tier secured state-of-the-art EVM design using pragmatic fingerprint detection annexed with NFC enabled voter-ID card," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 2016, pp. 1-6, doi: 10.1109/ICETETS.2016.7603041.

[8] Prof. P. B. Dhamdhere, Abhishek Kasar, Nilesh Satpute, Priyanka Lekurwale. (2017). A Secure E-voting System using Biometrics Authentication Methods for Android. International Journal of Advanced Research in Computer and Communication Engineering. Volume 6, Issue 2, Pages 80-82.

[9] Koç, Ali & Yavuz, Emre &Çabuk, Umut&Dalkılıç, Gökhan. (2018). Towards Secure E-Voting Using Ethereum Blockchain. 10.1109/ISDFS.2018.8355340.

[10] Qureshi, Amna &Megias, David &Pous, Helena. (2018). VSPReP: Verifiable, Secure and Privacy-Preserving Remote Polling with Untrusted Computing Devices. 10.1007/978-3-319-94421-0_5.

[11] PyPI face-recognition package: https://pypi.org/project/face-recognition/

[12] Zinah JMA (2018) Secure Electronic Voting Application Based on Face Recognition and Ciphering. J Comp Sci Appl Inform Technol. 3(2): 1-11. DOI: 10.15226/2474-9257/3/2/00131

[13] AanjanaDevi.SI et al. (2017).Confidential E-Voting System Using Face Detection and Recognition. International Journal of Engineering and Techniques - Volume 3 Issue 4, July-Aug 2017

ISSN: 223-7857 IJFGCN
Copyright ⓒ2020 SERSC