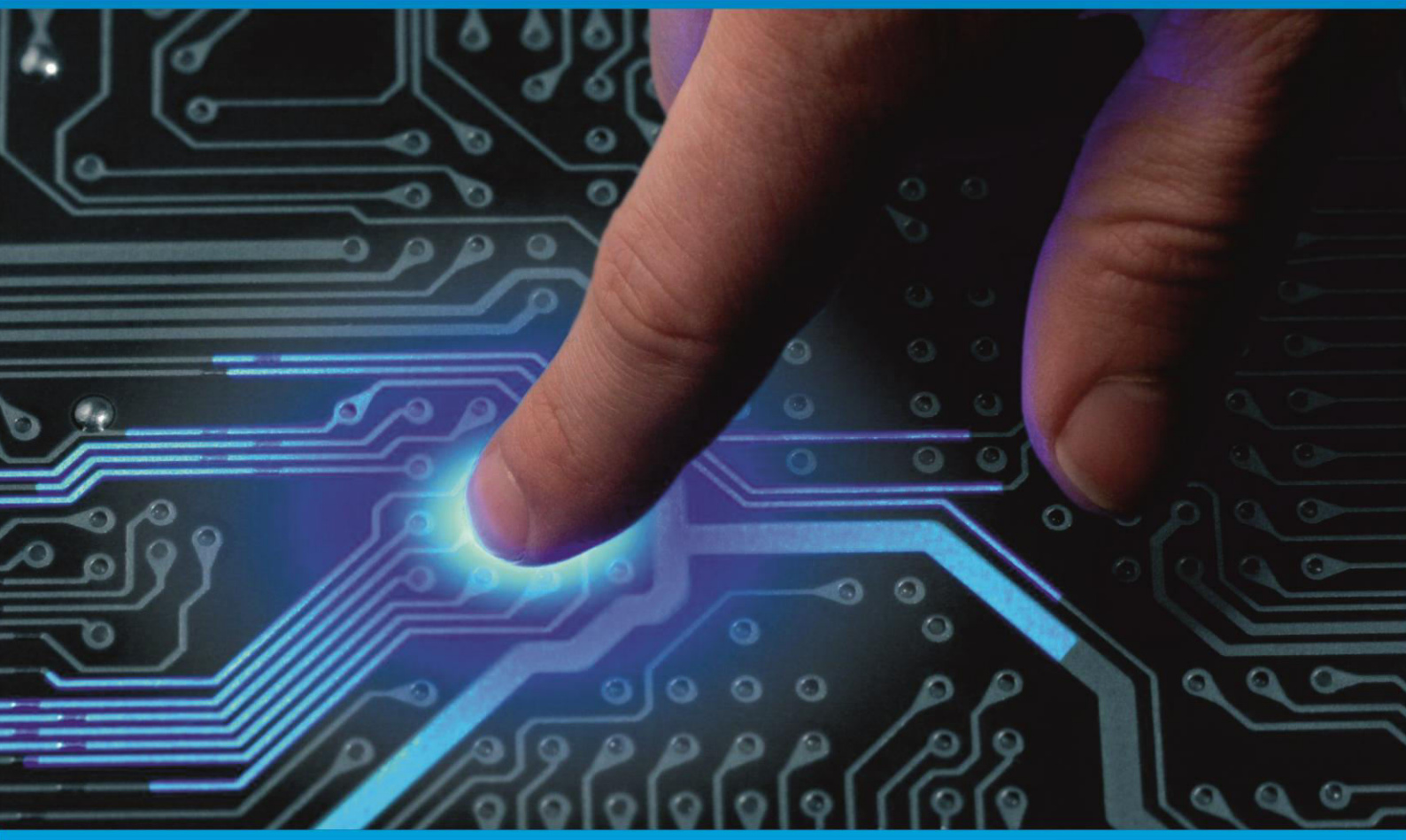
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905114 |

Smart Voting System through Facial Recognition

Srushti Wani[1], Pallavi Sonawane[1], Aishwarya Kadare[1], Anudeep Lohgaonkar[1], Prof. R. K. Tare[2]

UG Students, Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, India[1]

Department of Computer Engineering, NBN Sinhgad School of Engineering, Pune, India[2]

ABSTRACT: Elections are essential defining attributes of any democracy that is being governed by the people expressing their choices or articulate opinions in the form of voting. The basic idea of this project is to create smart voting machine that will help to eliminate defrauding of the manual voting systems and prior versions of electronic voting. The premise looks into and proposes a system that includes different layers of verifications to assure the reliability of the device. With the inclusion of biometric face and fingerprint sensor, each voter is entered into the system only after being recognized and checked with the given database of enlisted voters. Once the equivalent face and fingerprints are identical with the information provided, the voter will be permitted to proceed for choosing their preferred candidate from the panel of buttons. The votes are stored in the server and the counting is finished at the end of election, after the admin's authentication the result will be displayed. This voting system would approach higher security and expecting that it will raise voting percentage.

KEYWORDS: Smart Voting: Biometric, Facial and Fingerprint Recognition, Arduino, Web camera, LCD.

I. INTRODUCTION

Elections are the foundation of any democracy and the true spirit of democracy lies in people choosing their own government. but, the way elections are conducted right now in our country has defects and loopholes, which are being used for the advantage of political parties.

The current system has a lot of loopholes, like the possibility of duplicate votes, faking the count, nowadays with the rise in population the need for checking the validity of the voters has become a problem. All of which tampers the true meaning of democracy. In order to avoid these issues, the government of India introduced Electronic voting machine (EVM) system. This device has been praised for their simple alignment, ease of usage and reliability. The machine has to be transported and monitored with more man power and it is expensive. The system proposed here is a solution that addresses all the aforementioned concerns. Through the smart voting system that uses facial and fingerprint recognition, the possibility of duplication of the vote is also reduced through the same. This innovation refers to electronic voting systems where the election data is recorded, stored and processed effectively as digital information. Therefore, the essentiality of designing a secure smart voting system is very important. Usually, mechanisms that ensure the security and privacy of an election can be time-consuming, expensive for election administrators, and inconvenient for voters, that's why it is necessary to generate a secure voting system to overcome the challenges like authentication of voters, security of the voting process and protecting voted data etc.

II. RELATED WORK

S. Kumar and E. Walia, "Analysis of electronic voting system in various countries", International Journal on Computer Science and Engineering. Voting is that the bridge between the governed and government. The present electoral system has many security holes, and it's difficult to prove even simple security properties about them. A electoral system which will be proven correct has many concerns. There are some reasons for a government to use electronic systems are to extend elections activities and to scale back the elections expenses. Still there's some scope of labor in electronic electoral system because there's no way of identification by the electronic electoral system whether the user is authentic or not and securing electronic mechanical device from miscreants. This paper provides an summary of the experiences of other countries using electronic mechanical device.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905114 |

D. Nikam, D. Shetiye and D. Bhoite, "A critical study of electronic voting machine evm utilization in election procedure", International Journal of Trend in Scientific Research and Development, pp. 1-3, 03 2019. It also can be possible to ascertain the expenditure of election through this app. This app is beneficial to all or any citizens, voters, election officers, political parties, self service centre, media and political analyst. the most and important step is actual voting though Electronic mechanical device (EVM). At the start many questions were raised whether literate and illiterate can use this machine properly. It seen that everybody is using this machine. Presently the button called None of the above(NOTA) become a part of discussion. thanks to EVM following points become possible: 1) Fast counting of voting 2) Accurate counting of voting. 3) Avoidance of misbehavior /misconduct. Even promotion and dissemination by candidate is feasible through information technology. It can possible to urge likes about opinions and image of candidate through facebook and twitter.

R. Patel, V. Ghorpade, V. Jain and M. Kambli, "Fingerprint based evoting system using aadhar database", International Journal for Research in Emerging Science Technology, vol. 2, 2015. The existing system of election is running manually and therefore the piloted electronic voting using electronic mechanical device (EVM) has many limitations in its mechanism. during this paper we've proposed an automatic biometric electronic electoral system , where a four layered network system has been used for sending the votes from client to the most database, and there exist three application servers and a client. meaning , the proposed systems starts with automated registration system that might provide the secured database of the voters' information, and voter details are going to be stored against their finger prints within the main database. Finally, at the top of the day, casted votes are going to be counted automatically which might take lesser time than the manual system and therefore the result would be accurate, faster and reliable, and thus minimize the corruption.

K. Cao and A. K. Jain, "Automated latent fingerprint recognition", IEEE transactions on pattern analysis and machine intelligence, vol. 41, no. 4, pp. 788-800, 2018. Latent fingerprints are one among the foremost crucial sources of evidence in forensic investigations. As such, development of automatic latent fingerprint recognition systems to quickly and accurately identify the suspects is one among the foremost pressing problems facing fingerprint researchers. One of the primary steps in manual latent processing is for a fingerprint examiner to perform a triage by assigning one among the subsequent three values to a question latent: Value for Individualization (VID), Value for Exclusion Only (VEO) or No Value (NV). However, latent value determination by examiners is understood to be subjective, leading to large intra-examiner and inter-examiner variations. Furthermore, in spite of the rules available, the underlying bases that examiners implicitly use for value determination are unknown.

L. Gupta, Java AES 256 Encryption Decryption Example, Dec. 2019, [online] Available:https://howtodoinjava.com/security/aes-256-encryption-decryption.
Cryptography springs from Greek word 'crypto' means secret 'graphy' means writing that's used to conceal the content of message from all except the sender and thus the receiver and is employed to authenticate the correctness of message to the recipient. Today information security is that the challenging issue that touches many areas like computers and communication. Cryptography is such how that confirm of integrity, availability and identification, confidentiality, authentication of user and also as security and privacy of data are often provided to the user. during this paper we've defined and analysed various cryptographic symmetric algorithms like DES, Triple DES, Blowfish, AES and IDEA and asymmetric key cryptographic algorithms like RSA. they need been analysed on their ability to secure data, key size, block size, features.

III. PROPOSED SYSTEM

A. System Architecture:

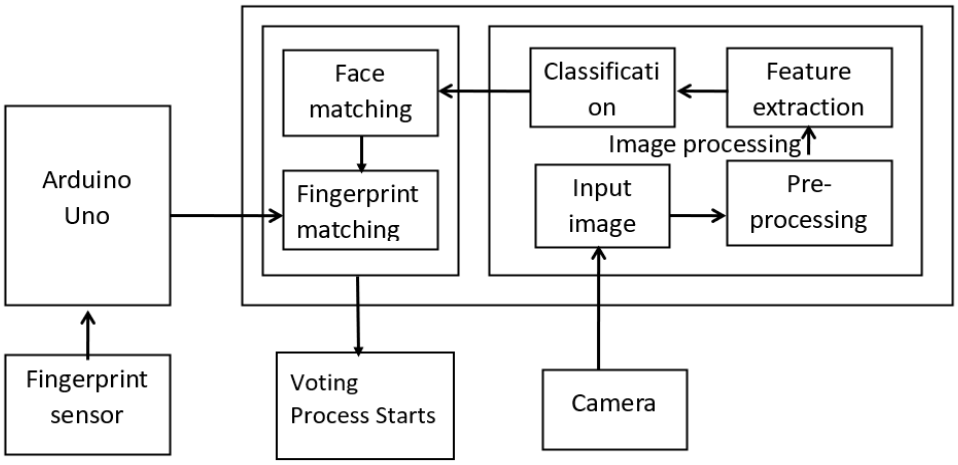
In this system voting is introduced using technique like face recognition.

1. The system captures image of Voter. Then the Face recognition process is carried out that is the image will go through steps like preprocessing and feature extraction and processed image is compare with image from dataset.
2. When face is recognized then the system checks for fingerprints recognition via fingerprint sensor.
3. If both are recognized Then only authenticated user will allow to cast the vote.If it is not recognised by system then it shows unauthorized user and returns to voting page.
4. Also, After the voting gets over the members of the booth must securely pack the ballet box and have to get through a lot of paper trials which is a tedious job. Hence to cut the chess around the bushes our system can display the result within half an hour or maximum 1 hour

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905114 |



B. Algorithm:

Haar Cascade Algorithm is used for process of face detection. Haar Cascade algorithm is an object detection algorithm of machine learning which is use to identify objects in given image or video.
Haar Cascade algorithm contains four stages:

1. Haar Integral Selection:

Haar feature is basically calculations that are implements on adjacent rectangle shaped regions at a particular location in a detection window.

2. Creating Integral Images:

The following haar features can be difficult to find out for a large image. At this stage an integral image takes place.Rather than calculating at every single pixel, rather it generates sub-rectangles and originate array references for each and every sub-rectangles. After that these are used to calculate the haar feature. These will make an algorithm a little faster.

3. Adaboost Training:

Adaboost trains the classifier to use best features which are basically selected by adaboost. It basically uses a fusion of many weak classifiers to generate a strong classifier which is used by algorithm for object detection.
Weak learners are formed by moving a window across the given input image and calculating Haar features for every subsection of the image. These variations are compared with a learned threshold which used to separate all non-objects from objects. Because these are weak classifiers, an outsized number of Haar features is required for accuracy to make a strong classifier.

4. Cascading classifier

The cascade classifier is formed of a different number of steps, where every step is a collects the weak learners. At boosting stage it trains weak learners, that allows for a classifier which are most accurate from mean prediction of among weak learners. by using related prediction, the classifier identified that object was matched(positive) or goes to the another region that is not matched(negative)
To reject the negative samples as early as possible the above steps are constructed, because the most part of window do not have anything of interest

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905114 |

IV. RESULT

E-voting system is not too efficient in terms of security and also fake voting is noticed everywhere at the time of elections. We can also observe that the hackers can easily hack the EVM machines and perform EVM tampering which leads to false voting. The proposed approach can overcome the problems and drawbacks of existing system, that ultimately reduce fake and false voting. As the face cannot be morphed easily in a live session even this would be a task for the hackers and ensures a secured and pleasant voting environment without inconvenience. From this approach people can easily vote from their nearest polling booths or even from their home if the people are aware of how the technology works and knowing about basic usage of the system.

In this process we do the following steps:

i. Firstly, GUI opens with the options.

ii. In the GUI first click on the start camera button then it will capture the image of the voter and matched the capture image with the image which is already stored in the database. If matched then voter has access to fingerprint recognition else authentication will be failed.

iii. After that fingerprint sensor button is workable if the capture image is matched with stored image. Fingerprint recognition work same as face recognition method. if fingerprint matched then the voting panel window is available for voters. Then voters can vote to any of the party after voting done the number of votes are stored in database and the result will be declared when Admin click on check result and enter the password.

V. CONCLUSION

So, we can observe that the existing system is not too efficient in terms of security and also fake voting is noticed everywhere at the time of elections. We can also observe that the hackers can easily hack the EVM machines and perform EVM tampering which leads to false voting. The proposed approach can overcome the problems and drawbacks of existing system, that ultimately reduce fake and false voting. The idea of adapting digital voting systems to make the pub-lic electoral process cheaper, faster and easier, may be a compelling one in modern society. Making the electoral process cheap and quick, normalizes it within the eyes of the voters, removes a certain power barrier between the voter and therefore the official and puts a particular amount of pressure on the official . It also opens the door for a more direct sort of democracy, allowing voters to precise their will on individual bills and propositions. In this paper, we introduced a unique, smart voting system-based electronic electoral system that utilizes smart contracts to enable secure and cost efficient election while guaranteeing voters privacy. we've outlined the systems architecture, the planning ,and a security analysis of the system

REFERENCES

[1] Umang Shah, Trupt Shah, MarteenKansagara, SaagarDaxini, „Biometric Secured Voting Machine to Avoid Bogus Voting Based on AADHAR CARD" , International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 3, March 2015

[2] Rudrappa B. Gujanatti, Shivaram N. Tolanur, Murughendra S. Nemagoud, Shanta S. Reddy, SangameshwarNeelagund," A Finger Print based Voting System" , International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181. Vol. 4 Issue 05, May-2015

[3] M.Sudhakar, B.Divya Soundarya Sai," Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller,, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan -Feb. 2015)"

[4]SoumyajitChakraborty, Siddhartha Mukherjee, BhaswatiSadhukhan, Kazi Tanvi Yasmin, " Biometric Voting System using Aadhar Card in India „, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 4, April 2016 '.

[5]http://www.ijirst.org/articles/IJIRSTV5I11016.pdf

[6]https://www.pyimagesearch.com/2018/06/18/face-recognition-with-opencv python-and-deep-learning/

[7] https://towardsdatascience.com/a-guide- to-face-detection-in-python-3eab0f6b9fc1

[8]https://medium.com/betterprogramming/step-by-step-face-recognition-in-imagesad0ad302058a

[9] International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4,April 2018

[10]Grady Booch, James Rumbaugh, Ivar Jacobson : The Unified Modeling Language User Guide,PearsonEducation.Rob Pandey, Pauline Wilcox:

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details