International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 4th Sept 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-09

Title: SMART VOTING SYSTEM

Volume 09, Issue 09, Pages: 115-118

Paper Authors

CH. CHANDRA MOULI, M. LAASYA PRIYA, J. UTTEJ, G. PAVAN SRI SAI, DR. R. VIJAY KUMAR REDDY

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SMART VOTING SYSTEM

CH. CHANDRA MOULI[1], M. LAASYA PRIYA[2], J. UTTEJ[3], G. PAVAN SRI SAI[4], DR. R. VIJAY KUMAR REDDY[#]

[1-4]Student, [#] Assistant Professor, Department of Information Technology, Prasad V Potluri Siddhartha Institute of Technology

Abstract:
In this paper a novel certification method in online voting system using facial detection of the voter. In India, at present there are two types of voting scheme in put into practice. They are top secret Ballet paper and Electronic Voting Machines (EVM), but both of the procedure has a few limits. Indian online voting is a face up to put into practice. The present voting system is not in safe hands. The voters require going dispersed places like polling booths and standing in a lengthy line up to cast their vote, for the reason that most of the people miss their possibility of voting. The voter who is not eligible can also cast their vote by false that means which may lead to a lot of troubles. So in this paper, we have to recommend a scheme for voting which is extremely effectual in voting system. In this process, we have 3 stage of security in voting procedure. The initial level is the authentication of Aadhar number, second stage is the authentication of Voter ID and third stage is facing matching. The protection level of our scheme is really enhanced by the novel application technique for every voter. The user authentication procedure of the scheme is enhanced by addition face detection using by application which will recognize whether the user is authenticated user or not.

Keywords*:* Face recognition, Smart Voting, Security

Introduction

Voting is fundamental right for each and every individual in our country. Each and every person has the “right to vote”. But not everyone is utilizing their right, because of various reasons. The voting is held in various levels, like municipal elections, State elections and Central Elections. So, in order to make voting easy and increase the voting percentage we use technology to enhance the method of voting through face recognition. Coming to the security we are using LBPH (Linear Binary Pattern Histograms) algorithm. In this algorithm, the face is captured and trained. At this stage during training, first the faces are converted into gray scale images and then the points or pixels obtained through the gray images are then converted into Histograms and these histograms contains some values and these values are converted into a single value i.e., from binary digits to a decimal number. Because of this there will be an enormous increase in the voting percentage as each and every one can vote easily by going to their nearest polling booths. And most importantly the false or fake voting will be reduced.

Existing System

The existing system is not too effective. At present there are two types of voting methods, they are:

- Ballot Voting
- EVM Voting

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Ballot Voting:

A ballot is a device used to cast votes in an election, and may be a piece of paper or a small ball used in secret voting. In this the voter is given a paper which consist of all the party symbols along with representative names in it. Here, people come to the polling booth, take the ballot paper and pole their vote by putting stamp on the desired party symbol. Finally, the ballot paper is folded and dropped into the ballot box. At last, the votes are counted by the Election commission officers.

Fig.1 Ballot Voting

EVM (Electronic Voting Machine) Voting:

An EVM is a device which is used for voting. This machine consists of party symbols along with the representative's name and a button at the end for each and every party name. The voters come near the EVM machine after completion of their verification at the early level before voting. After verification the voter go near the EVM and cast their vote by pressing the button. After pressing the button, 7 seconds later a beep occurs with a green light that indicates that the vote is submitted. The above procedures are not so accurate as there may be possibility for the false/fake voting. The ballot papers maybe lost at the time of counting which may affect results of the particular area or people may miscount the number of votes which leads authority into wrong hands. EVM machines sometimes get corrupted and polling gets stopped temporarily and a lot time is wasted or EVM may be tampered and the casted votes may be polled to a particular party only, even the vote is casted to different candidates or party. This may lead authority into wrong hands.

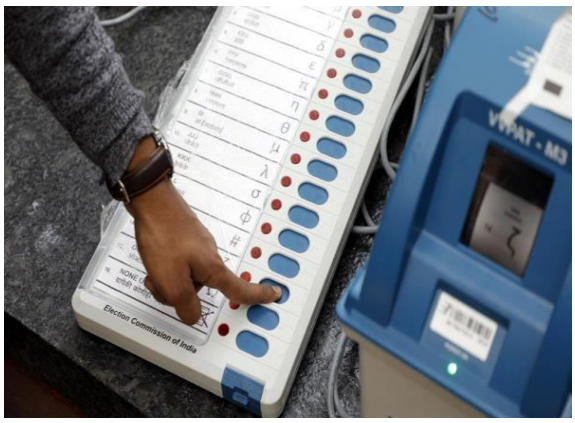

Fig. 2 EVM Voting

The above two procedures also lack a security as one's vote can be casted by another voter or even a miscellaneous person. This factor is known as fake voting. Without proper authentication there is a possibility of fake voting. So, the existing system is not efficient for voting. Even though there is very few false/fake voting, this minor setback can turn the results to opposite direction.

Proposed System

In this paper, we are operational with three dissimilar security hierarchies, they are:

Level 1: Aadhar id number

Initially at the time of voter registration, the system will ask for the Aadhar ID from the end used (voter). The entered exclusive number is demonstrated from the database

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

afford by the election commission.

Level 2: Voter id card number

In the second stage of authentication, the voter has to come into the election commission voter's id number. The entered id number is verified from the database afford by the election commission.

Level 3: Face identification with particular election commission afford id number

In this hierarchy, Local Binary Patterns Histogram (LBPH) algorithm is used to authenticate the facial image of the voters from the database afford by the election commission. If the face is matched with the given data and faces, it gives a message "Face Detected" then it directly redirects to the voting page. If the face is not matched then it gives a message as "Fraud Detected". After going to the Voting page, the voter casts their vote in the webpage and then submits their vote. When the vote is submitted it gives a message "You have voted successfully. If the voter tries to vote again in the same session then it shows a message "You have already voted".

Experimental Results

In this process we do the following steps:

i. First a GUI opens with the options create dataset, train dataset, recognize and exit.

ii. In the GUI first click on the Create dataset, then the anaconda prompt ask for the Aadhar ID and Voter ID details to register.

iii. After that a window is opened and then captures the face of the person.

iv. Next, click on Train dataset on the GUI to train the existing images in the Database.

v. Later, Click on recognize button on the GUI to recognize the person. If the face is detected then it directly redirects to the voting page, or it wil not redirect.

vi. Finally, the user can cast their vote and Submit. Once the vote is submitted it shows "You have voted successfully". If the user tries to vote again, then it shows "Fraud Detected".

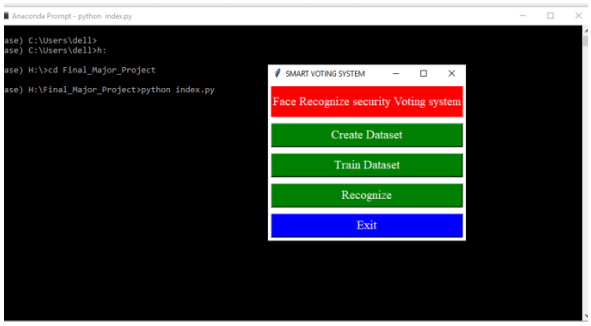

Fig. 3 GUI with options

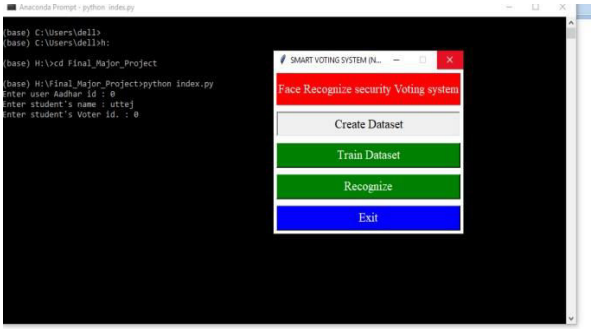

Fig. 4 Details are filled for registration

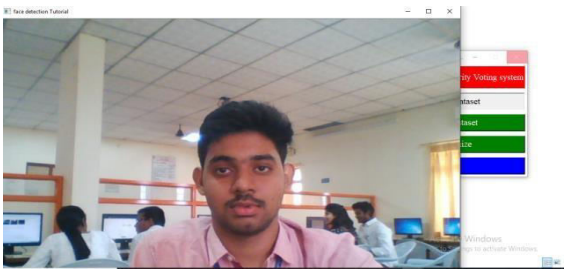

Fig. 5 Capturing of faces

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

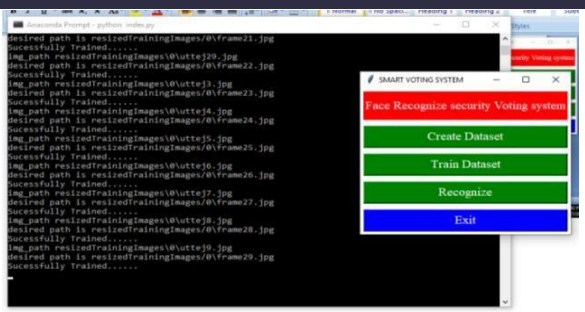

Fig. 6 Training of all the images in the Database

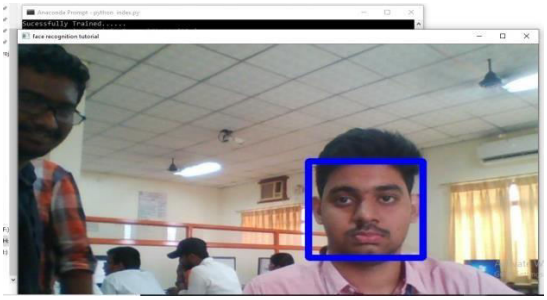

Fig. 7 Face is trained successfully

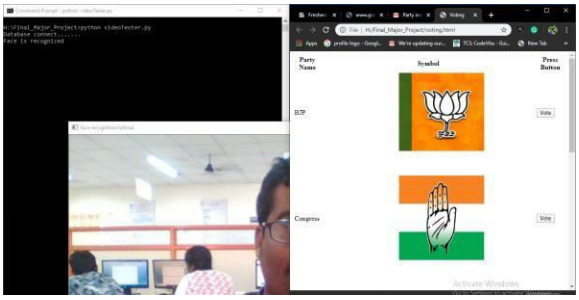

Fig. 8 Voting page is opened after recognition

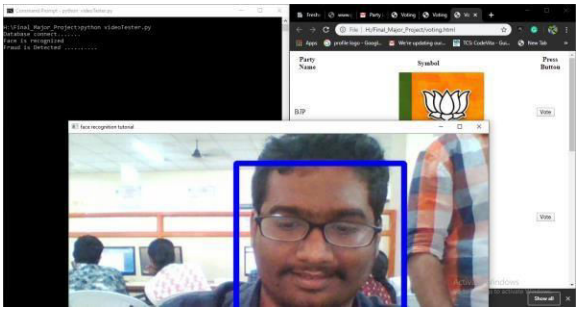

Fig. 9 If the voter tries to vote again a message is generated as "Fraud Detected"

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. 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.

References

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

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

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

[4] https://medium.com/better-programming/step-by-step-face-recognition-in-images-ad0ad302058a

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

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

[7] Biometrics – Identity Verification in a Networked World – Samir Nanavati, Michael Thieme, Raj Nanavati, WILEY-Dream Tech.