



An International Journal (AMIJ)
Singaporean Journal of Scientific Research(SJSR)
Vol.11.No.1 2019 Pp. 17-22
available at:www.sjsronline.com
Paper Received :30-11-2019
Paper Accepted:25-12-2019
Paper Reviewed by: 1. Dr. P. Surya Prakash 2. Basu Reddy
Editor : Dr. Binod Kumar

Computerized Online Voting System using RFID Technology and Image Processing

E.Vetrimani

Assistant Professor, Department of Computer Science and Engineering
RVS College of Engineering and Technology,Coimbatore

Dr.M.Arulselvi

Associate Professor, Department of Computer Science and Engineering,
Annamalai University.

Abstract

In this concept, System will have two step verification portal, one is RFID data verification of voters and followed by successful face authentication will allow to vote for their desired candidate. These two new authentication technique in voting system will reduce the piracy issue of voters and counterfeit vote. Currently in India, there are two types of voting system in practice. They are secret Ballet paper and Electronic Voting Machines (EVM), but both of the process has some limitation or demerits. In India, Computerized voting system has not yet been implemented. The current voting system is not secure and time consuming as well. The people who are not eligible to vote can also cast their votes by unwanted means, which may cause various problems. That is why in this concept we have to propose a system or way for voting which is very effective in voting. Here we have two level of security in voting process. The first level is the verification of RFID number and second level is face recognition. The security level of our system has been highly improved by the use of new method for each voter. The authentication of the user in the system is improved by using face recognition in the application, which will be able to identify whether the user is authenticated user or not.

1. INTRODUCTION

Electronic voting machine has already been developed and widely used in many developed countries. But during the election time, verification process takes a lot more time and there is possible to occur counterfeit vote. Now a day in India two types of method are being used for voting. The first method is secret ballot paper, in which many papers are used and second method is EVM (electronic voting machine) which is in use since 2003. We have to propose a method for computerized voting that is more secure than the existing system. Here face recognition concept is used to identify the exact person whose image is stored in the database. Two levels of verification were used for the voters in our proposed system. The first one is RFID number verification, if your election commission id number is correct in RFID Data Verification then you have to go for Second level of security which is the main security level where the system recognize the face of the real voter from the current database of face images given by the election commission which is already connected with RFID. If the image taken matches with the respective image of the voter in the database, then a voter can cast their vote in the election.as you have to know that in existing system is not much more secure because in existing system security level is only voter card so any one can give vote for other person by just carrying their voter card but here we can provide a way for voting which is more secure

than existing system.

2.LITERATURE SURVEY

A. *Location-free Voting System with the help of IOT Technology*

The proposed concept uses fingerprint sensor of the smart phone to cast the vote of the voter. An application must be installed on the voter's smartphone. This application is used to identify the fingerprint. Smart phone's fingerprint sensor is linked with the provided application to identify the uniqueness of the original voter. Security provided is medium. This proposed system allows the voter to cast their votes only on the day of Election. The voters are not be able to cast the vote other than the day of Election. On the day of voting, voter scans their fingers along the fingerprint sensor of the smartphone. Accuracy depends on fingerprint sensor of the mobile phone. Detection of fraud is one of the core components of this system. It avoids casting of multiple votes by any voter. Electoral voting systems provides facility to voters so that they are able to vote from any location without any geographical restrictions all over the world which considers mobility, privacy, security, and easiness. Current voting systems provided all over the world have similar problems in each of them. The main concept in this paper is to provide a voting system that uses smart phone's fingerprint sensors in order to identify genuine voter and provide high accuracy, security, and mobility to make voting system more practical and location-free.

B. *Smart Electronic Voting System Based On Biometric Identification-Survey*

In this paper, author defines Use of GSM (Global System for Mobile Communication) module in order to enhance the speed and provide high security of the voting system. Using GSM module, the message will be passed to the voter's mobile mentioning that he has successfully casted his vote. Using IOT the counted votes can be easily sent to the total database server so that all of the counted votes and the elected party that has been selected can be announced easily. For avoiding misconceptions during elections, many advanced techniques are being proposed using different methods. But in the field of biometric identification, we can get the better results and it is also trustworthy. This system works on the basis of master-slave server. We are able to transfer the voted data online to the MASTER server unit. According to the proposed concept, number of slave systems are kept at various locations. All the slave system are coupled to the nearest Master System. This system is able to identify if a particular person has already casted their vote or not. If a person has casted his vote earlier then a mechanism is set to buzzer the alarm and the message displaying error appears and he is not able to cast the vote so that we are able to prevent misconceptions during elections. This paper provides the various works which are being proposed based on the voting system which uses biometric identification as a major concept. Some other works have different algorithms being used and some other works have different techniques provided are based on the multimodal biometric identification.

C. *Anti-Cheating Presence System Based on 3WPCADual Vision Face Recognition*

This paper focuses on a face recognition method using half-join normalization with dual vision camera as a face image acquisition tool and using 3WPCA(Three level Wavelet Decomposition-Principal Component Analysis) as its feature extraction. Use of Dual vision camera has been able to provide detectable face images from two different positions of the left and right lens. Image retrieved from the two corners of the left lens and the right lens can provide a merged face image in database combining left lens face image and right lens face image. The use of two sides of the face angle is used to avoid fake facial data such as the use of a photo of a person or an image similar to a person's face. This research can produce a presence system based on good face recognition and can be used to identify dummy face data with its recognition accuracy up to 98%.

D. *E-Smart Voting System with Secure Data Identification using Cryptography*

In this paper the author focuses on the strategy used and functions of E smart voting system (ESVS) which is very much secured, biometric authentication system which is provided with verification system based on OTP that also improves the voting process in the time of election. The vote casted by the user is first encrypted and then stored in the database. In this concept Aadhar number of user is used for verification and identification of the voter. With smart voting system, voter is able to cast their vote with their mobile phone and avoid all kind of queues at polling booth. At first, Aadhar number is provided by the voter in the ESVS. The ESVS then uses the Aadhar number to authenticate the user through OTP which will be received on their registered Aadhar linked mobile number. People without Smart phones are also able to cast their vote through ESVS with an additional step of authentication through highly secured Aadhar based biometric authentication. Smart Voting System successfully allows people to vote through their smart phones which helps to reduce the queues at the polling booth. Also, highly reliable biometric authentication mechanism is provided for people who do not want vote using smart phones thus prevent electoral fraud.

II. PROPOSED SYSTEM

In this project we are working with three different stages

- 1) Level 1: RFID number. At the time of voter registration system will request for the unique id from the voter. Unique id is verified from the database provide by the election commission.
- 2) Level 2: Face recognition with respective election commission id number. In this level, Haar Cascade algorithm is used to verify the facial image of the voters from the database provided by the election commission.
- 3) Level 3: Face recognition successful face authentication will allow to vote for their desired candidate

III. IMPLEMENTATION OF THE MODEL

1. Every New User in the India is first register for Voting.

So, our first step is registration

2. At that time of Registration System Capture, the Face of the user by using Web Camera and Store the Face sample with RFID (Adhaar) in the Server Database for Security Purpose.
3. At the time of election, we will use two level of security first one is RFID id verification second one is voter id verification third one is face recognition.
4. System will be checking whatever unique id and voter id entered by the voter is correct or not.
5. If unique (RFID) id or voter id is correct than system will take image of voter and compare with the respective image of database or server.
6. If the image in database is matching with the captured image of the voter, then he/she is allowed to cast is vote.
7. On the voting page all the party whatever party contest in the election symbols /buttons will be there. Voter can cast his /her vote in the election.
8. As soon as voter will give vote the id of voter logout automatically so we can say that a voter can give only one vote. (Auto refresh)
9. On counting form only election commission authorized user can login with the secure id and password if both id and password is correct then voting process will be continuing.

IV. DESIGN / METHODOLOGY

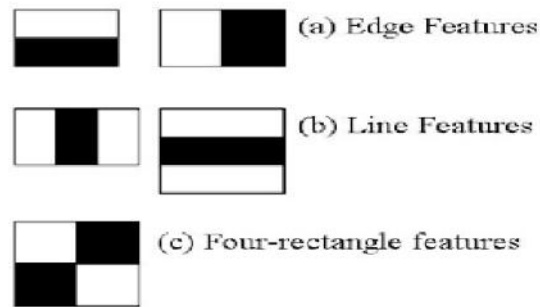
This proposed concept is a web-based system so basic features related with web-based technologies such as client-server, database, image processing properties determine the software requirement of the system.

The software product is a standalone system and it is not the part of larger system. The system will be made up of two parts. Before the Election Day the application is used for general purposes such as viewing candidates' profiles and election results in past years. The voter is verified using face recognition technology used. These votes are accepted by the system on the server. The Election Commission Authority arranges the whole system according to its requirements on the server where the system is running.

V. FACE DETECTION USING HAAR CASCADES

Object Detection using Haar feature-based cascade classifiers is an effective object detection method proposed by Paul Viola and Michael Jones in their paper, "Rapid Object Detection using a Boosted Cascade of Simple Features" in 2001. It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images.

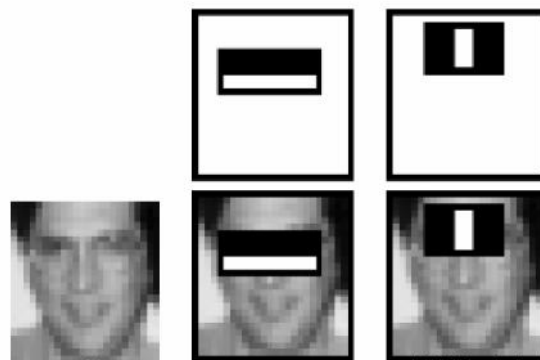
Here we will work with face detection. Initially, the algorithm needs a lot of positive images (images of faces) and negative images (images without faces) to train the classifier. Then we need to extract features from it. For this, haar features shown in below image are used. They are just like our convolutional kernel. Each feature is a single value obtained by subtracting sum of pixels under white rectangle from sum of pixels under black rectangle.



Now all possible sizes and locations of each kernel is used to calculate plenty of features. (Just imagine how much computation it needs? Even a 24x24 window results over 160000 features). For each feature calculation, we need to find sum of pixels under white and black rectangles. To solve this, they introduced the integral images. It simplifies calculation of sum of pixels, how large may be the number of pixels, to an operation involving just four pixels. Nice, isn't it? It makes things super-fast.

But among all these features we calculated, most of them are irrelevant. For example, consider the image below. Top row shows two good features. The first feature selected seems to focus on the property that the region of the eyes is often darker than the region of the nose and cheeks. The second feature selected relies on the property that the eyes are darker than the bridge of the nose.

For this, we apply each and every feature on all the training images. For each feature, it finds the best threshold which will classify the faces to positive and negative. But obviously, there will be errors or misclassifications. We select the features with minimum error rate, which means they are the features that best classifies the face and non-face images.

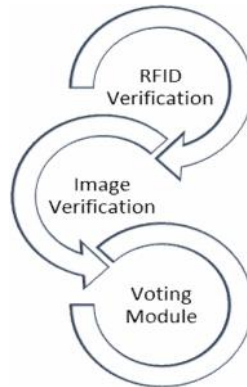


For this, we apply each and every feature on all the training images. For each feature, it finds the best threshold which will classify the faces to positive and negative. But obviously, there will be errors or misclassifications. We select the features with minimum error rate, which means they are the features that best classifies the face and non-face images.

The process is not as simple as this. Each image is given an equal weight in the beginning. After each classification, weights of misclassified images are increased. Then again same process is done. New error rates are calculated. Also new weights. The process is continued until required accuracy or error rate is achieved or required number of features are found.

Final classifier is a weighted sum of these weak classifiers. It is called weak because it alone can't classify the image, but together with others forms a strong classifier. The paper says even 200 features provide detection with 95% accuracy. Their final setup had around 6000 features.

VI. BASIC ARCHITECTURE OF VOTING SYSTEM



VII. RESULTS AND DISCUSSIONS

As we see that existing voting system has many defects such as lengthy process, time taking, not secure, bogus voting, no security level but now we can say that our approach is more useful and secure from the existing system. Highly secured because in this project we have to use face recognition and face comparison so false user can't give votes. We can access result (counting) faster than existing system. Because ballot system takes much more time for counting process. But this computerized voting system increases the trust in voting system as well as Election Commission. Still there remains some limitations and drawbacks in this voting System.

VIII. CONCLUSION

As we see that existing voting system has many defects such as lengthy process, time taking, not secure, bogus voting, no security level but now we can say that our approach is more useful and secure from the existing system. Since, we are using three level of security in this proposed system the false voters can be easily identified. The facial authentication technique is very much useful in identifying the fraud voters, so we can avoid the bogus votes during election commission. As every operation is performed through internet connectivity so, it is onetime investment for government. As data is stored in centralized repository so, data is accessible at any time as well as backup of the data is possible. Smart voting system provides updated result at each and every minute. Also requires less man power and resources. The database needs to be updated every year or before election so that new eligible citizens may be enrolled and those who are dead are removed from the voter list.

REFERENCES

- [1] Edy Winarno, Wiwien Hadikurniawati, Imam Husni Al Amin, Muji Sukur "Anti-Cheating Presence System Based on 3WPCADual Vision Face Recognition:Proc. EECSI 2017, Yogyakarta, Indonesia, 19-21 September 2017", Issue:September 2017, Pages:121-124.
- [2] Amish Basal, Utkarsh Raina, Vaibhavi Pujari, Roushan Kumar "E-Smart Voting System with Secure Data Identification using Cryptography:2018 3rd International Conference for Convergence in Technology (I2CT) The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Issue:Apr 06-08, 2018,Pages:1-4.
- [3] Swetha M S, Thungamani M, Shreejwol Disti, Raman Shah "Smart Voting System Support through Face Recognition" IJRST –International Journal for Innovative Research in Science & Technology| Volume 5 | Issue 11 | April 2019
- [4] Vikas Kumar, MS Swetha, MS Muneshwara, S Prakash, "Cloud computing: towards case study of data security mechanism," vol-2 issue-4 page no-1-8 2011
- [6] MS Muneshwara, MS Swetha, M Thungamani, GN Anil, "Digital genomics to build a smart franchise in real time applications," IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT),IEEE page no 1-4 2017 .
- [7] MS Muneshwara, A Lokesh, MS Swetha, M Thungamani, "Ultrasonic and image mapped path finder for the blind people in the real time system," IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) IEEE, page no 964-969 2017.