E Voting Using Android System

Namrata Thakur[1], **Vrushalee Ambavale**[2]

[1, 2]Lokmanya Tilak College of Engineering, Navi Mumbai, Maharashtra, India

Abstract: ***The advancement in the mobile devices, wireless and web technologies given rise to the new application that will make the voting process very easy and efficient. The e-voting promising the possibility of convenient, easy and safe way to capture and count the votes in an election. This paper provides the specification and requirements for E-Voting using an Android platform. The e-voting means the voting process in election by using electronic device. We also described how the android mobile phones are efficient and can be used for voting. The android platform is used to develop an application.***

Keywords: Android, E-voting system, Open Source, Image processing, Encryption Techniques

1. Introduction

Voting for any social issue is essential for modern democratic societies now a day. The voting process in today's context is behind its time in respect of the usage of modern ICT as seen by experience .So it is becoming very important to make the voting process more easy and efficient. In other hand the rapid development in operating system of the mobile phones gives rise to the application development on the large scale. The main reason behind the tremendous development in android application development is that the android is an open source operating system. The paper will be describing the basic idea of the project E voting system on android.

2. Literature Survey

Existing Voting System

The technology used in India for voting is Electronic voting machines. There are 2 systems developed for conducting an electronic voting machine. These are the DRE (Direct Recording Electronic) and Identical Ballot Boxes.

1) A DRE voting system records votes by means of an electronic display provided with mechanical or electro-optical components that can be activated by the voter, that processes voter selections by means of a computer program, and that records that processed voting data in memory components. It produces a tabulation of the voting data that is stored in a removable memory component and may also provide printed renditions of the data. The system may further provide a means for transmitting the processed vote data to a central location in individual or accumulated forms for consolidating and reporting results from precincts at a central location. DRE systems additionally can produce a paper ballot printout that can be verified by the voter before they cast their ballot.
2) The Identical Ballot Boxes hold the ciphered vote, encrypted with the PMA voting key and the ciphered Identification Card Number, encrypted with their personal 4 digit key. It is designed to accept connections from the vote distribution server, and ensures an acceptable level of security as far as remote vote manipulation is concerned.
3) Integrated Election Software package, running on a Microsoft Windows computer, allows the election official to set up and record the details of an election. When voting is completed, it counts the votes and displays the outcome of the count results [1].

3. Proposed E Voting System

Voting will be done through mobile device. First an application is required through which voters can communicate. We need to use existing database in which voters information exist. Voters/citizens information is available in register database Secure data centre is required to store and fetch the data as per requirement. Mobile based voting system throughout voting process an internet connection is essential. Assume that almost every next person is having mobile phone on which our application program will execute. After connection is established voters need to download application from a specific source.

The Process for E Voting:

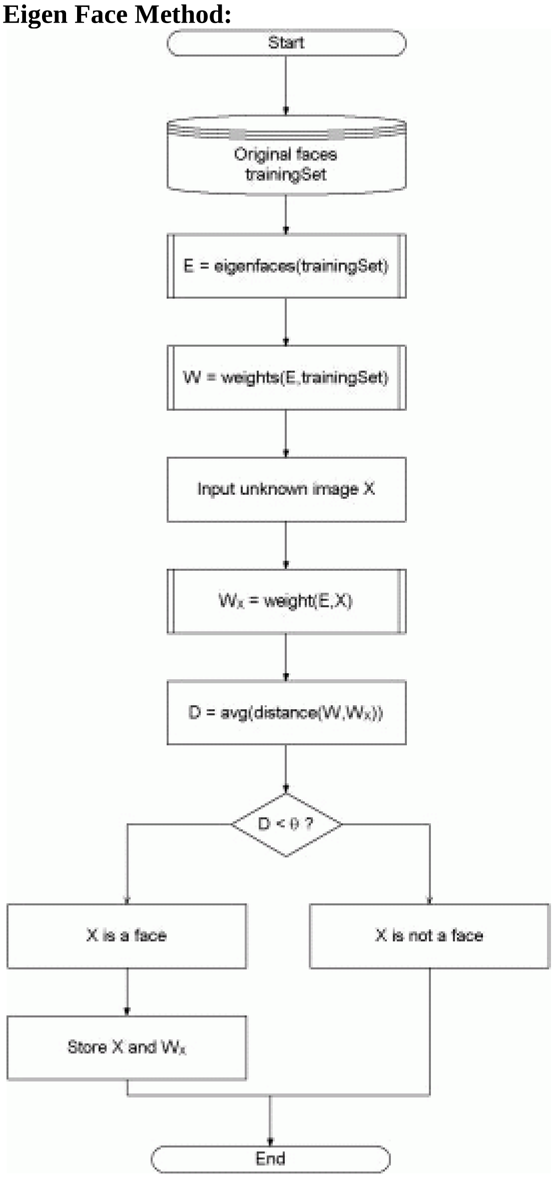
1) Registration: The voter will use his device on which the E-voting application will be installed. Using this device, the voter will enter his voter ID, username, password, user photo, Email Id which will be stored in database.
2) Sign in: Enter username, password, and user face recognition (to check validity Voters are asked to input their access data, which were registered during the Register stage to verify their eligibility in the election.)
3) Now, the CA (Central Authority) maintains the database of voter details and also a database of voters who have already voted. The CA will check whether the voter has already voted; if yes, the voter will not be allowed to vote again. If the voter has not voted before, the CA will check the validity of voter. If the voter is a valid voter then One Time Password (OTP) will be generated by the CA using the voter ID and the timestamp. This OTP will be sent to the voter's E Mail address that has already been registered in the database. When the voter receives this OTP he can use it to log into the system to cast their vote.
4) After logging in, a list of candidates will be displayed on the screen of the voter's device. The user can select any of the candidates and further confirm their vote for the candidate.
5) When a candidate is selected and the vote is cast then encryption occurs using the encryption technique.
6) After selecting particular candidate counting is incremented by one, separate database is used to store the count of votes.

7) The counting of all votes is made; every single cast vote is decrypted and verified. All votes that were cast should be validated and the final result must be the same as the sum of all votes validated.

3.1 Image Processing

In this system, for authentication face recognition is playing main role. Live image will be captured by mobile frontal camera. This captured image will be sent to the server for further processing. By using this image, server checks whether user is authorized or not. User is permitted for voting only if he is authorized. All registered data is stored in database. We are using server for creation and transmission of OTP [3].

Eigen Face Method:


Start
Original faces trainingSet
E = eigenfaces(trainingSet)
W = weights(E,trainingSet)
Input unknown image X
W_x = weight(E,X)
D = avg(distance(W,W_x))
D < θ ?
X is a face
X is not a face
Store X and W_x
End

Algorithm:

1. The algorithm for the facial recognition using eigenfaces is basically described in above figure. First, the original images of the training set are transformed into a set of eigenfaces *E*.
2. Afterwards; the weights are calculated for each image of the training set and stored in the set *W.* Upon observing an unknown image *X*, the weights are calculated for that particular image and stored in the vector W_X. Afterwards, W_X is compared with the weights of images, of which one knows for certain that they are faces (the weights of the training set *W).*
3. One way to do it would be to regard each weight vector as a point in space and calculate an average distance *D* between the weight vectors from W_X and the weight vector of the unknown image W_X.
4. If this average distance exceeds some threshold value (theta) then the weight vector of the unknown image W_X lies too "far apart" from the weights of the faces. In this case, the unknown *X* is considered to not a face. Otherwise (if *X* is actually a face), its weight vector W_X is stored for later classification. The optimal threshold value theta has to be determined empirically.

3.2 Encryption and Decryption

Asymmetric Key Cryptography

In order to encrypt and decrypt the votes that will be cast during the voting stage, RSA algorithm is used. This asymmetric primitive has a pair of two keys, the public key and the private key. It involves three steps that are: key generation (which occurs at the Registration Stage), encryption (during the Voting Stage) and decryption (at the Counting Stage). The key pairs are generated based on two large prime numbers that must be kept in secret just as the private key. Any encrypted text with one key of the pair, can be decrypted with the other one. If encryption occurs with the public key then it must be decrypted using the private key and vice versa.

Blind Signature Primitive

To meet the privacy requirement and loose the connection between the voter and the vote, blind signature based on RSA comes into play. The content of a message is blinded first before it is signed in such way the signer does not now the original content of what he is signing. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. A new key pair is generated aside from the one used in the encryption/decryption phase which occurs at the voting and counting stages.

4. Conclusion

This project focused on the analysis of development of E-voting application on an android platform. The usability of this system is very high if it will be used in real life election process. It will definitely helpful for the users who wish to vote and the voting process will be made very easy by using this application.

References

[1] "E-voting on Android System" paper (International Journal of Emerging Technology and Advanced Engineering) prepared by : Kirti Autade, Pallavi Ghadge, Sarika Kale ,Co-authors- Prof. N. J. Kulkarni, Prof. S. S. Mujgond, February 2012.

[2] E-Voting System Using Android Application M.S.Sai Mohit , M.Karthik , T.Rajavel , Ms. J.Sangeetha

[3] E-Voting Using Android Mobile by Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane

[4] Amir Omidi and Mohammad Abdollahi Azgomi,"An Architecture for E-Voting Systems Based on Dependable Web Services", Innovations in Information Technology, 2009. IIT '09, pp. 200 – 204, Dec. 2009.

[5] Cesar R. K. Stradiotto and et al Web 2.0 E-Voting System Using Android Platform

[6] P. N. Huu, V. Tran-Quang, and T. Miyoshi, "Image compression algorithm considering energy balance on wireless sensor networks," in IEEE Int. Conf. Industrial Informatics (INDIN), Osaka, Japan, Jul. 13–16, 2010, pp. 1005–1010.

[7] "Electronic voting," Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.