E-ISSN: 2321–9637

Volume 1, Issue 4, November 2013

International Journal of Research in Advent Technology

Available Online at: http://www.ijrat.org

# I-VOTING: DEMOCRACY COMES HOME

Ankit Tiwari
Information Technology
K. J. Somaiya
Institute of Engg & IT
Mumbai, Sion
ankit.tiwari@somaiya.edu

Ronak Mewada
Information Technology
K. J. Somaiya
Institute of Engg. & IT
Mumbai, Sion
ronak.mewada@somaiya.edu

Krish Mehta
Information Technology
K. J. Somaiya
Institute of Engg. & IT
Mumbai, Sion
krish.mehta@somiya.edu

Vaishali Mohite
Information Technology
K. J. Somaiya
Institute of Engg. & IT
Mumbai, Sion
mohite@somaiya.edu

**ABSTARCT:**
**i-Voting is a web-based application. This software provides facilities for casting your vote using internet so the name given to our project is “i-voting: Democracy comes home”. Any person who wants to vote should register to the website. Each voter has to fill their details along with their voting id and Aadhar card number to prove their identity and thus voter creates account for voting. Unique biometrically encrypted VID which is equivalent to voting card is generated for every registered voter. User can cast his vote using this biometrically encrypted VID. The server used can be any web server. A backup server will be maintained in case of server break down.**

**The main aim of our proposed system is to increase the voter’s turnout. The system proposed gives the facility to the user to cast his vote online irrespective of the place provided they are a registered user. To authenticate the user, system uses image processing technique. And for integrity purpose the votes and VID are encrypted and stored in database**

***Keywords:*** *Principal Component Analysis, Advanced Encryption System, Data mining, Data Warehousing, Error Correction Code.*

## 1. INTRODUCTION

Voting is a method for a group such as a meeting or an electorate to make a decision or express an opinion—often following discussions, debates, or election campaigns. Democracies elect holders of high office by voting. In a democracy, a government is chosen by voting in an election: a way for an electorate to elect, i.e. choose, among several candidates for rule. In a representative democracy *voting* is the method by which the electorate appoints its representatives in its government. A vote is a formal expression of an individual's choice in voting, for or against some motion (for example, a proposed resolution), for a certain candidate, a selection of candidates, or a political party. A secret ballot has come to be the practice to prevent voters from being intimidated and to protect their political privacy. Voting usually takes place at a polling station; it is voluntary in some countries, compulsory in others, such as Argentina, Australia, Belgium and Brazil. India is the world's largest democracy with current population of about 1.21 billion. The success of democracy and formation of responsible government is directly dependent on the voting power of the citizens. Adult franchise of India amended and reduced the age of voting from 21 to 18. It made provision for more youths to exercise their votes in election. It is sorry to note that the educated class and youths of our country are not taking active part in the elections and exercising vote. Because of which the important votes for our nation are missing. Politicians are taking advantage of illiterates and poor people by providing false assurances. It is time for all of us to think about the importance of voting and educate others also. A stronger democracy can be built with greater participation. It is the duty of every citizen to exercise their vote and help in electing the better candidate. Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet. In general, two main types of e-Voting can be identified:

e-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations); remote e-Voting where voting is performed within the voter's sole influence, and is not physically supervised by representatives of governmental authorities (e.g. voting from one's personal computer, mobile phone, television via the internet (also called i-voting)).

The idea of having electronic voting in Estonia gained popularity in 2001 with the "e-minded" coalition government. Estonia became the first nation to hold legally binding general elections over the Internet with their pilot project for the municipal elections in 2005. The electronic voting system withstood the test of reality and was declared a success by Estonian election officials. The Estonian parliamentary election, 2007 also used internet voting, another world first. In this presented paper i-Voting allows the users to cast their vote on the secured website operated by Election Commission. The advantage of i-voting is user can vote from anywhere irrespective of the place which increases the user’s turnout. Manually counting of votes is not that feasible and requires more time so i-voting is preferable .The proposed system supports simultaneous voting and therefore it can be preferred more.

The user casting his vote should be an authenticated user. The user is authenticated using techniques like Image Processing. For applying this technique system require user’s Voting id and Aadhar card details and current photograph.

The process of i-voting begins with registration. Any user who wants to use this facility must register himself first. Registration for i-voting would be started for 30-40 days prior to the day of election. For registration, user has to enter all his important details among which voting id and aadhar card number are mandatory details to be entered. User has to prove his identity by submitting his current photograph using webcam. This photograph is matched with the respective user’s photograph stored in the aadhar card database. PCA face recognition algorithm is applied on both the images. If both the images match then, the user’s authenticity is proved and he is
registered. He is then provided with a randomly generated password which will be used to login into the account at the
day of election. If the images don’t match then user would not be registered.

At the day of the election, the user logins to the account using his aadhar card number and the password provided him at the time of registration. Here, user again has to prove his identity so he has to submit his current photograph using webcam. This image will be again matched with the respective image of the user stored in the database at time of the registration. If images match then the user is logged in or else the access is denied. Once the user is logged into the account he can view all the details regarding the candidates in his area. Meanwhile the webcam should be kept active throughout the process for monitoring the user. He is therefore asked whether he wants to cast vote or not. If he selects yes then the VID which is stored in the database is displayed else not. As the VID is displayed it is deactivated after 15minutes & therefore user has to cast his vote within that time period. After the voting process is over, the vote will be encrypted and stored in the database.

Literature Survey is explained in section II. In section III System overview are explained. In section IV Principal Component Algorithm is explained. In section V System Architecture. Implementation plan is described in section VI. Future Result are shown in section VII. Conclusion is explained in section VIII. In section IX Future Scope is explained and Reference is explained in section X.

## 2. LITERATURE SURVEY

The presented paper will be working on the ideas given in the following papers:

Using biometric encryption techniques given in the paper “Face recognition with biometrics encryption for privacy – enhancing self – exclusion” proposed by Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, DimitrisHatzinakos [1].

Using PCA face recognition given in the paper “Algorithm of face recognition by PCA”, proposed by Khalid A. S. Al-Khateeb and Jaiz A. Y. Johari [2].

Feature extraction is done with ideas given in the paper "M. Turk and A. Pentland, "Eigenfaces for recognition,"Journal of Cognitive Neurosicence, vol. 3, no. 1, pp. 71–86, 1991[3].

I. T. Jolliffe, Principal Component Analysis, Springer Serires in Statistics, second edition, 2002. [4].

T. A. M. Kevenaar, G. J. Schrijen, M. v. d. Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. IEEE Workshop on Automatic Identification Advanced Technologies, October 2005, pp. 21–26 [5]

Fuzzy vault for face recognition is refered from paper Y. Wang and K. N. Plataniotis, "Fuzzy vault for face based cryptographic key generation," in Proc. Biometrics Symposium 2007, September 2007[6].

AES encryption technique used is used as proposed in paper J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999[7].

Some of the worked that is mentioned in the websites like: Wikipedia[8], iium.com[9], blackbumNews.com[10], blogs.windsorstar.com[11], cs.comell.edu[12], and s28.photobucket.com [13]

## 3. SYSTEM DESCRIPTION

### *3.1 Capture, Conversion and storing of image in the database*

As the work mentioned in the paper [2] the image will be represented in smaller matrix. The coloured image will be first converted into grey – scale image of size 112X92. The range of grey – scale image is from 0 – 255 as shown in the Figure.1. Next step after capturing the input image is to convert it into eigen face and then it in database named as eigen DB.

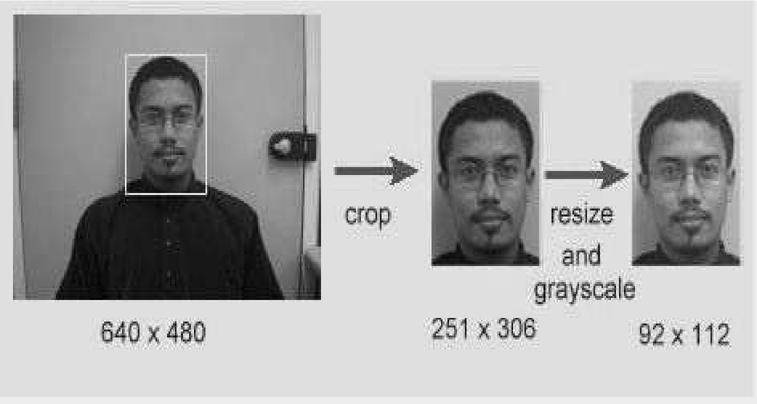


Figure.1 Process of crop and resize

### *3.2 Face Matching*

Now the next phase is face matching which is shown in the Figure 2. PCA algorithm is applied on images for face matching or face recognition purpose. If both the images i.e. aadhar card image and registration image match, user is registered and provided with random password & if it doesn't matches then user has to register again.

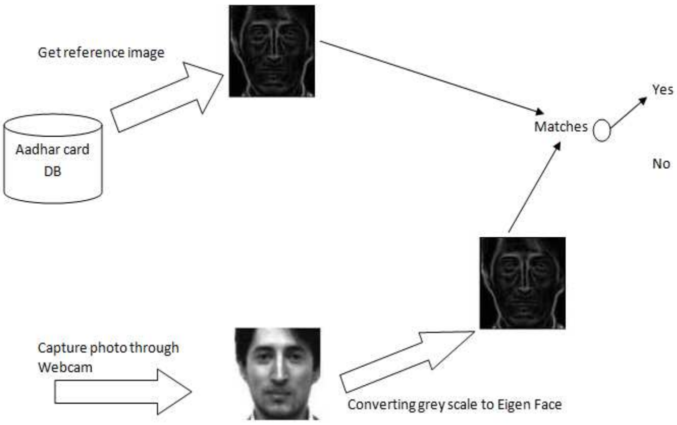


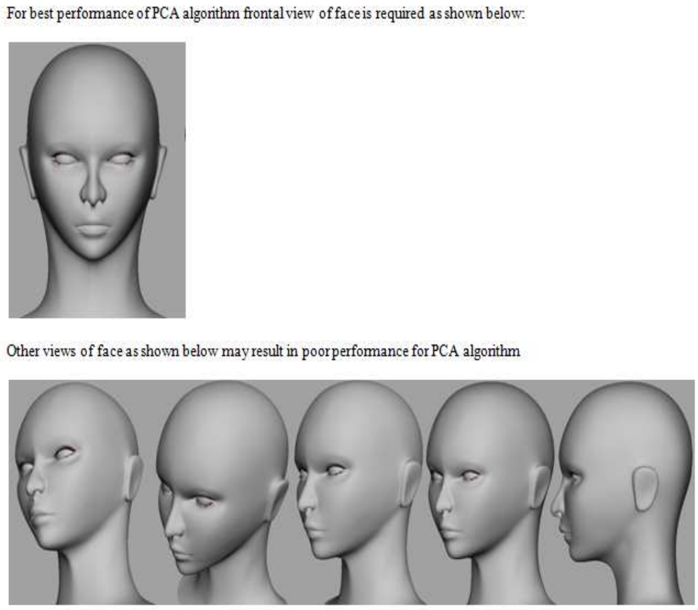
Figure. 2 Face Matching

### *3.3 Encrypting the image and generating key(VID)*

In this phase for face recognition with biometric encryption, rather than storing one's facial image in a database, the facial image is used to encrypt (code) some other information such as a cryptographic key and only the biometrically-encrypted data is stored. This removes the need to collect and store actual biometric data in database and most privacy concerns associated with centralized databases are eliminated. The biometric feature directly into the database we will make be extracting features from image as mentioned in paper [1, 3, 4, 5] for extracting feature of an image. We will be using AES algorithm for generating a cryptographic key. This key will be used as the VID by the person for voting. The vote of the user is stored in the database according to VID. Hence, this VID will help in hiding the identity of the user while votes will be counted.

## 4. PRINCIPAL COMPONENT ANALYSIS

With PCA, the probe and gallery images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics and reveals the most effective low dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces as shown in the figure 4 .Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in a 1D array. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. The PCA approach typically requires the full frontal face to be presented each time; otherwise the image results in poor performance. Above Figure 3 shows different possibilities of facial views.



For best performance of PCA algorithm frontal view of face is required as shown below:

Other views of face as shown below may result in poor performance for PCA algorithm

Figure.3. Facial views for PCA algorithm

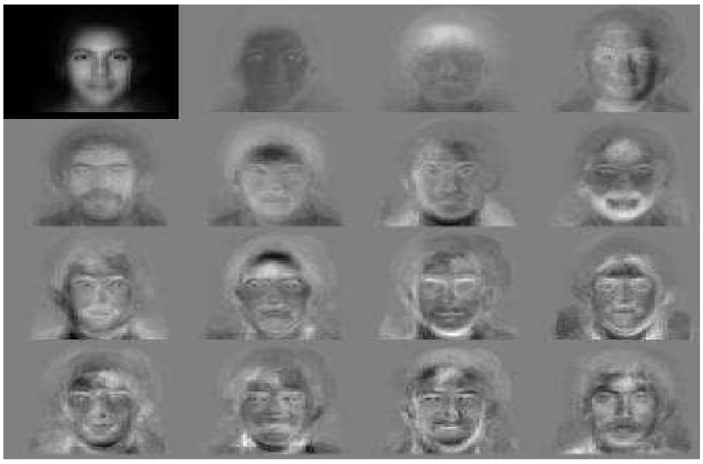


Figure. 4 Generation of eigenfaces

## 5. SYSTEM DEFINTION

### *5.1 System Architecture*

The proposed system shown in Figure 5 allows user to cast his vote online irrespective of the place he is provided he has registered himself. The user first registers himself in the voting website and provides his personal details in which aadhar card number and voting id are mandatory. The registration period will be active for only 30-40 days prior to the day of election. The identity and authenticity of the user is proved by using face recognition technique using PCA algorithm. The user has to submit his current photograph at the time of registration. This photograph will be matched with the photograph available in the aadhar card details. If both the images match then the user is registered and a randomly generated password is given to the user which is used by him at the time of login.

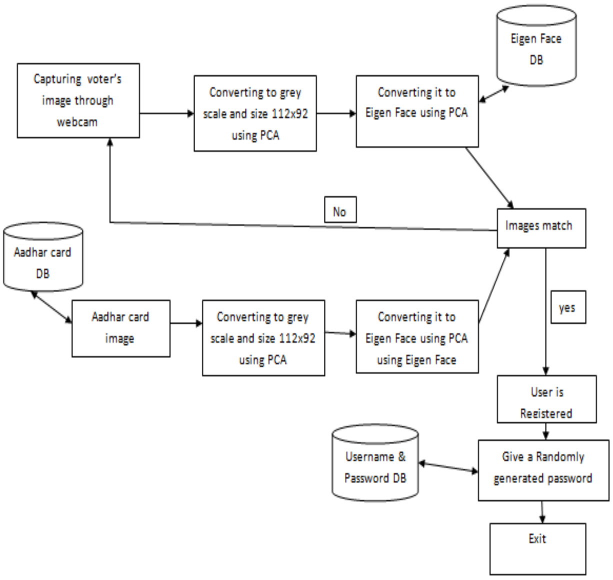

Eigen Face DB
Capturing voter's image through webcam
Converting to grey scale and size 112x92 using PCA
Converting it to Eigen Face using PCA
No
Images match
Aadhar card DB
Aadhar card image
Converting to grey scale and size 112x92 using PCA
Converting it to Eigen Face using PCA using Eigen Face
yes
User is Registered
Username & Password DB
Give a Randomly generated password
Exit

Figure. 5 Registration Architecture

At the backend VID is generated as shown in Figure 6. This VID is generated using the features extracted from the image taken at the time of registration. Image is first converted into grey scale image and of fixed resolution and then the features are extracted. Error detection technique is applied to remove noise from the image. AES algorithm is applied on the extracted feature and key is obtained. This key is used as VID and stored in the database.

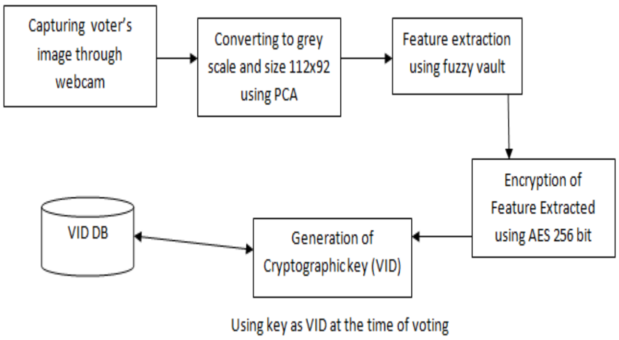

Capturing voter's image through webcam
Converting to grey scale and size 112x92 using PCA
Feature extraction using fuzzy vault
Encryption of Feature Extracted using AES 256 bit
Generation of Cryptographic key (VID)
VID DB
Using key as VID at the time of voting

Figure. 6 VID generation Architecture

At the day of voting, the user logins to the account using his aadhar card number and the password provided him at the time of registration as shown in Figure 7. To make sure the same person who has registered is login to the account again current photograph of the user is to be submitted. Once again face recognition technique using PCA is applied and authenticity is proved. If the images match then the person will be logged in or else access will be denied. Once the user is logged in he can view all the candidates in his area. He is therefore asked to vote and then the VID which is stored in the database is displayed if the user agrees for voting. As the VID is displayed the user has to vote within specified duration else the VID will be de-activated. After the voting process is over, the vote will be encrypted and stored in the database.

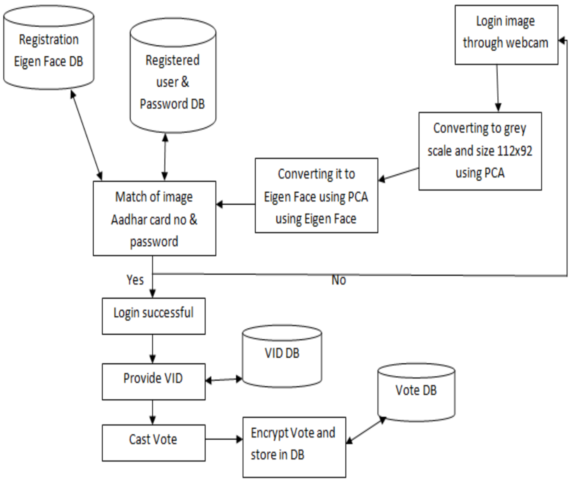

Registration Eigen Face DB
Registered user & Password DB
Login image through webcam
Converting to grey scale and size 112x92 using PCA
Converting it to Eigen Face using PCA using Eigen Face
Match of image Aadhar card no & password
Yes
No
Login successful
VID DB
Provide VID
Vote DB
Cast Vote
Encrypt Vote and store in DB

Figure.7 Login Registration

### *5.2 Algorithm*

The algorithm consists of following steps:
(1) The user has to first register him to use i-voting facility.
(2) For registration he has to provide his personal details and Aadhar card number and Voting Id as mandatory details.
(3) Along with that he has to submit his current photograph for authenticity.
(4) The current image and the Aadhar card image is matched using PCA algorithm.

(5) If images match then the user is registered and provided with a random password.
(6) Features of user’s current image will be extracted using fuzzy vault and AES encryption algorithm is applied and key is generated which we call it as VID.
(7) This VID is stored in the database and locked.
(8) On login day the user provides his Aadhar card number as username and password given to them at registration time.
(9) Along with this he has to again give his photo to make sure that same person is getting logged in who has registered.
(10) Again PCA algorithm is applied and registered image and login image are matched
(11) If images match then the user’s login is successful else the access is denied.
(12) After login the user is provided with the VID with the help of which he can cast his vote.
(13) The vote is then encrypted and stored in the database.
(14) After the voting period is over, the final count of vote is displayed on admin side.

## 6. IMPLEMENTATION PLAN

6.1 Hardware Requirement

The proposed system requires the webcam for capturing the images of the user. It requires the computer with the minimum specification that is P4 processor with 512MB of ram.

6.2 Software Requirement

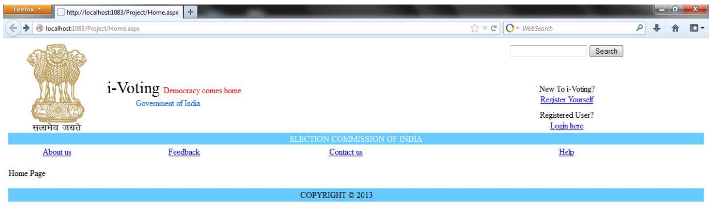
In the proposed system we would be using Matlab 7.2 and higher version software for the matching of the image were as for front end we would be using the Microsoft Visual Studio2010 for the interaction with the users

6.3 Database

We can use the MySQL Server 2008 database as well as Oracle server as image is to be stored in the database.

## 7. EXPECTED RESULT

The resultant output would be a website as shown in Figure 8 which would be used for voting online. The user can cast his vote irrespective of the place and at the other end admin would be able view the total number of the votes. This vote will also be saved in the database.


Firefox
http://localhost:1083/Project/Home.aspx
localhost:1083/Project/Home.aspx
WebSearch
Search
सत्यमेव जयते

i-Voting Democracy comes home
Government of India

New To i-Voting?
Register Yourself
Registered User?
Login here

ELECTION COMMISSION OF INDIA

About us Feedback Contact us Help

Home Page

COPYRIGHT © 2013

Fig.8 Resultant voting website

## 8. CONCLUSION

The concepts that are face matching and database security. Our main purpose is to ease the manual voting process. The system proposed gives the additional facility to the user to cast his vote online irrespective of the place. We have combined the two concepts together that is helper database system and the Principle Analysis Component (PCA) algorithm for the face matching of image while doing transactions.

## 9. FUTURE SCOPE

The system has a wide future scope as can be used in the other online system, online transactions etc. By using our face as voting id card there will be no risk to handle or stolen or misplace the card. There is no need for an individual to go to the respective place and cast his vote. He can cast vote from any place. We can improve the system for the online transactions as well.

## References

[1] Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, DimitrisHatzinakos,"Face Recognition with Biometric Encryption for Privacy-EnhancingSelf-Exclusion",IEEE,1-8,5-7 July 2009.
[2] Khalid A. S. Al-Khateeb and Jaiz A. Y. Johari,"Algorithm of Face Recognition by Principal Component Analysis", IIUM Engineering Journal, Vol 3, No 2 ,2002.
[3] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neurosicence, vol. 3, no. 1, pp. 71– 86, 1991.
[4] I. T. Jolliffe, Principal Component Analysis, Springer Serires in Statistics, second edition, 2002.
[5] T. A. M. Kevenaar, G. J. Schrijen, M. v. d. Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. IEEE Workshop on Automatic Identification Advanced Technologies, October 2005, pp. 21–26.
[6] Y. Wang and K. N. Plataniotis, "Fuzzy vault for face based cryptographic key generation, in Proc. Biometrics Symposium 2007, September 2007.
[7] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.
[8] www.wikipedia.com
[9] www.iium.edu.my
[10] www.BlackburnNews.com
[11] http://blogs.windsorstar.com
[12] http://www.cs.cornell.edu
[13] www.s28.photobucket.com