Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/2257
DOI URL: http://dx.doi.org/10.21474/IJAR01/2257
ISSN NO. 2320-5407

RESEARCH ARTICLE

SECURE ONLINE VOTING SYSTEM.

[*]Manjusha Vijay Amritkar[1], Roshani Dudhe[2], Komal Sawant[2], Shraddha Phutane[2] and Puneet Dadhich[2].

1. Assistant Professor.
2. Student.

Manuscript Info

Manuscript History

Received: 29 September 2016
Final Accepted: 30 October 2016
Published: November 2016

Key words:-
Ballots, interactive voting, transmission, network, IECI, polling station

Abstract

Secure Online Voting System is an interactive voting system application with which users can vote from any location remotely using their information stored prior in database securely. Online voting system involves transmission of ballots and votes via network. Security is maintained at different levels like while voting and at the time of transmission of ballots also.

The main objective of this work is to develop an interactive voting system application with which users can participate using their information stored prior in database while creating the voter ID and the information need to be updated at an period of less than six months for perfect user verification by the Independent Electoral Commission of India (IECI). In this system people who have citizenship of India and whose age is above 18 years and of any sex can give their vote through online without going to any physical polling station.

Introduction:-

Secure online voting system is a voting system in which the election data is recorded, stored and processed primarily as digital information and it needs to address, obtain, mark, deliver, and count ballots via computer. Therefore voter identification and authentication techniques are essential for more secure platform mechanisms to overcome vulnerabilities of the client used by the voter to cast her vote. The voting process by registered users is very cumbersome.

Voting system is the base of Indian democracy in which voters choose their leaders to show their presence for the way that they will be supervised. Voting scheme have evolved from counting by hands in previous days to system that include papers, punch card, optical scan machine and mechanical lever i.e. to the electronic voting system. This traditional voting system is the time consuming process therefore maximum of Indian population is not able to vote because of their busy schedule plus the voting process by registered users is very cumbersome.

Present scenario of voting system in INDIA is full-fledged on paper. Many of the citizens whose name is listed in the jurisdiction area are having mobility issues. Secure online Voting System overcomes this problem by online voting. In “Secure online voting system” a voter can use his\her ‘voting right’ online without any difficulty. He/she has to fill a registration form to register him/her with the use of face recognition and finger print. During voting all the entries is checked by the DATABASE which has already all information about the voter. If all the entries are correct then voter is eligible to give vote. If conditions are wrong then that entry will be discarded.

Corresponding Author:- Manjusha Vijay Amritkar.
Address:- Assistant Professor.

Verification is done using Face detection and recognition (FDR) system and thumb impression scanning. While transmission of the vote, encryption is used to avoid unauthorized modification. It will lessen human efforts to reduce the time consumed for result calculation.

OBJECTIVE:-

The main objective of this work is to develop an interactive voting system application with which users can participate using their information which is stored prior in the database while creating the Adhar ID. The information need to be updated in the period of less than six months for user verification by the Independent Electoral Commission of India (IECI). In this system people who have citizenship of India, whose age is above 18 years and of any sex can give their vote through online system without going to any physical polling station. Every time the user logs in to the system, the user is validated with the ID and image of the voter in the database. Through this development we can obtain a secured website which comprises of all the voting methodologies in a single website.

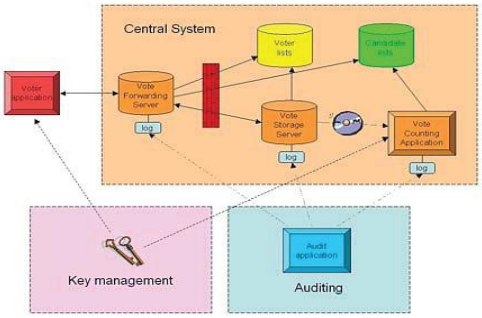


Figure 1: Architecture of secure online voting system

METHODOLOGY:-

The System first checks whether this person has the right to vote or not from the age of person. If he/she is an illegible voter then he goes to the next form for face recognition. The voter's image is captured online and passed to a face detection algorithm (Eigen face or Gabor filter) which is used to detect his face from the image and save it as the first matching point. The voter's Adhar card number is used to retrieve and return his saved photo from the database of the system which is passed to the same detection algorithm (Eigen face or Gabor filter) to detect face from it and save it as second matching point. The two matching points are used by a matching algorithm to check wither they are identical or not. If the results of the matching algorithm shows that those two points match then thumb impression scanning is done. It will be matched with the existing database from Adhar Card number then a voting form is presented to him. While transmission of the vote, encryption is used to avoid unauthorized modification.

Fingerprint recognition or authentication refers to the automated method of verification of two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated (i.e. a biometric) due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use in government sectors and collections by law enforcement and immigration.

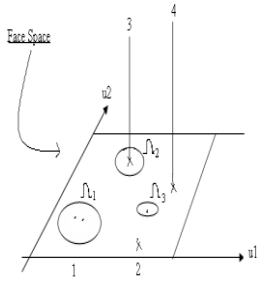
In this research, we proposed an authentication technique using a Face Detection and Recognition system and thumb impression scanning in online voting to achieve the rules of Supreme Electoral Council as follow: Only eligible persons vote, No person is allowed to vote more than once and at more than one place. The vote is secret, and each (correctly cast) vote gets counted and to achieve the aims of online voting as follow: increase participation, lower the costs of running elections, and improve the accuracy of results.

EIGEN FACE RECOGNITION:-

The information theory approach of encoding and decoding face images extracts the relevant information in a face image, encode it as efficiently as possible and compare it with database of similarly encoded faces. The encoding is done using features like eyes, ears, nose, lips, and hair.

Mathematically, principal component analysis approach will convert every image of the training set as a vector in a very high dimensional space. The eigenvectors of the covariance matrix of these vectors would incorporate the variation amongst the face images. Now each image in the training set is converted to the eigenvectors (variations). This can be displayed as an '*eigenfaces*' representing its contribution in the variation between the images. These eigenfaces look like ghostly images and some of them are shown in Figure 3. In each eigenfaces some sort of facial variation can be seen which differs from the original image.

The high dimensional space with all the eigenfaces is called the image space (feature space). Also, every image converted is actually a linear combination of the eigenfaces. The amount of overall variation of one eigenfaces is the eigenvalue associated with the corresponding eigenvector. If the eigenfaces with small eigenvalues are neglected, then an image can be a linear combination of reduced no of these eigenfaces. For example, if there are M images in the training set, we would get M eigenfaces. Out of these, only largest eigenvalues images say M' eigenfaces are selected. When the face image to be recognized (known or unknown), is projected on this face space (Figure 2), we get the weights associated with the eigenfaces, that linearly approximate the face or can be used to reconstruct the face. Now these weights are compared with the weights of the known face images so that it will be recognized as a known face in used in the training set. In simpler words, the Euclidean distance between the image projection and known projections is calculated; the known face image is considered with minimum Euclidean distance.



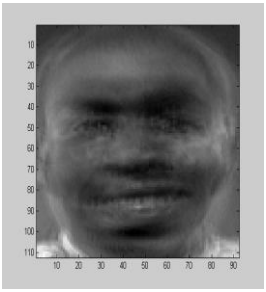


Figure 2: The face space and the three projected images on it. Here u1 and u2 are the eigenfaces
Figure 3: The projected face from the training database.

The algorithm for the facial recognition using eigenfaces is basically described in Figure. 4. First, the original images of the training set are transformed into a set of eigenfaces *E*. 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, which is stored in the set W. One way to do it would be to regard each weight vector as a point in space and calculate an average distance *D* by some Euclidean distance measure between the weight vectors from W_X and the weight vector of the unknown image W_X.

If this average distance exceeds some threshold value Θ then the unknown image W_X lies too "far apart" from the weights of the faces. In this case, the unknown image is considered as not a face. Otherwise it is considered as known image and its weight vector W_X is stored for later classification. The optimal threshold value Θ has to be determined empirically.

FINGER PRINT RECOGNITION:-

Fingerprint recognition referred as an automated method of identifying or confirming the identity of an individual based on the comparison of two fingerprints. **Fingerprint recognition** is one of the most well known biometrics, and it is by far the most used biometric solution in every organization for authentication.

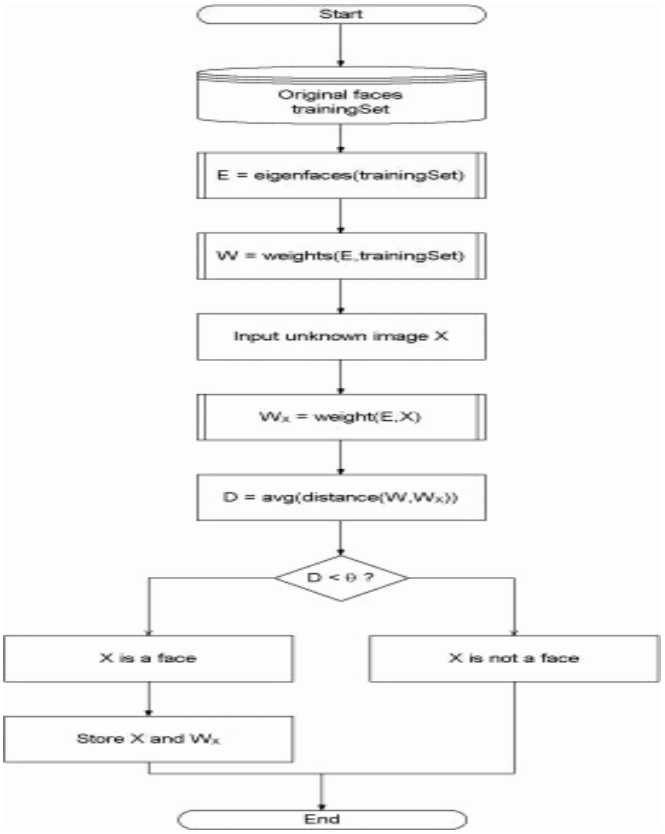


Figure 4: High-level functioning principle of the eigenfaces-based facial recognition algorithm.

The reasons for fingerprint recognition being so popular are the ease of acquisition, established use and acceptance as compared to other biometrics, and the fact that availability of numerous (ten) sources of this biometric on each individual.

A fingerprint usually appears as a series of dark lines that represent the high, peaking portion of the friction ridge skin, while the valleys between these ridges appears as white space and are the low, shallow portion of the friction ridge skin Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path.

Figure 5: Minutiae

Figure 6: Other fingerprint characteristics

For over decades, fingerprint recognition system has been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years. The determination and commitment of the fingerprint industry, government evaluations and needs, and organized standards bodies have led to the next generation of fingerprint recognition, which promises faster and higher quality acquisition devices to produce higher accuracy and more reliability. Because fingerprints have a generally broad acceptance with the general public, law enforcement, and the forensic science community, they will continue to be used with many governments' legacy systems and will be utilized in new systems for evolving applications that require a reliable

biometric. Because of these advantages our secure online voting system is going to use this system as second level of verification of voter to make our system more secure as shown in Figure 7.

The purpose of the verification is to tell if the two templates being compared come from the same object, e.g. the same finger. The matching algorithm analyzes the templates to produce a similarity score and if the score reaches a certain threshold the algorithm decides that it is a match.

A perfect biometric system would always make correct decisions, but in reality this is not possible. Depending on the amount of useful information available in samples that could be used to characterize objects, and the capabilities of the complete biometric system (and the algorithms in particular), the decision is more or less probable to be correct.

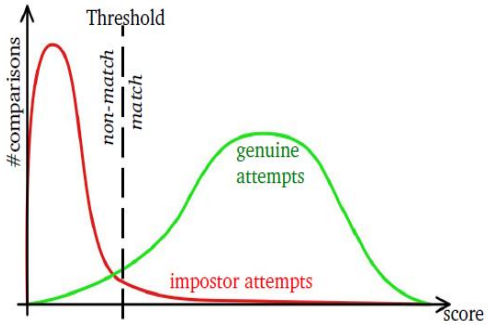


Figure 8: Distribution of score by attempt type.

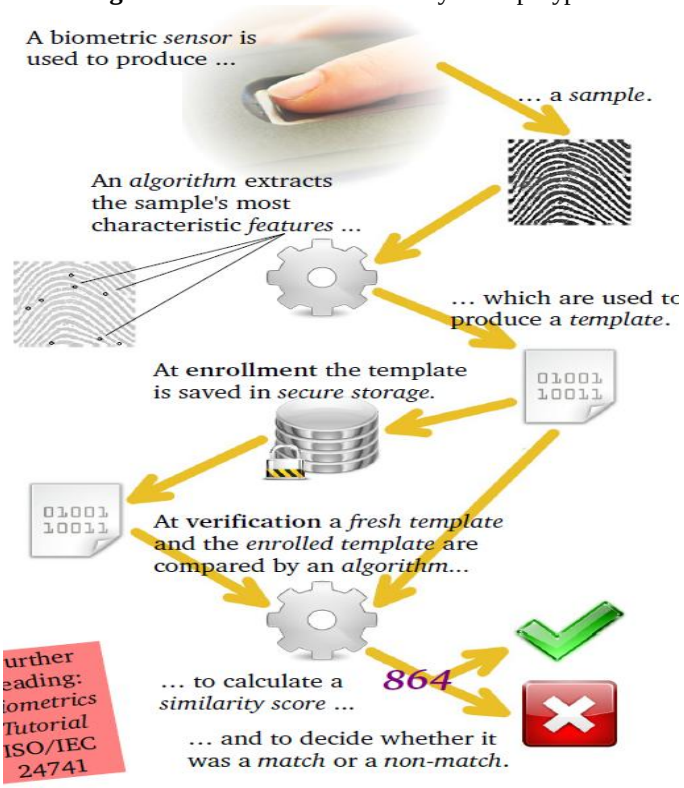


Figure 7:- Fingerprint recognition systems

In this research, we proposed an authentication technique using a Eigen Face Detection and Recognition system and finger print impression scanning in online voting to achieve the rules of Supreme Electoral Council as follow: Only eligible person can vote, no person can vote more than once, the vote is secret, and each (correctly cast) vote gets counted. This research is useful to increase voting participation, lower the costs of running elections, and improve the accuracy of results.

CONCLUSION:-

Secure Online Voting System can help to increase number of voters as individuals will find it easier and more convenient to vote especially those who are abroad. It can be used for those who do not have issued and registered for their voter ID card. It can increase user level security using pulse rate detection to avoid black mailing and bullying. It can help reduce to reduce manual process.It can reduce human errors while calculation of votes.It can help to reduce man power required at voting booths.It can help to reduce time consumed .It can help to save resources.It can ensure secure transmission of vote .

REFERENCES:-

1. K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan, "Highly Secured Online Voting System over Network," in Indian Journal of Science and Technology | Print ISSN: 0974-6846 | Online ISSN: 0974-5645.
2. White paper on "Understanding Biometric Performance Evaluation" .
3. Document on fingerprint recognition.
4. Swaminathan B, and Dinesh J C D, "Highly secure online voting system with multi security using biometric and steganography," in International Journal of Advanced Scientific Research and Technology, vol 2(2), 195–203.
5. Anand A, and Divya P, "An efficient online voting system," in International Journal of Modern Engineering Research, vol 2(4), 2631–2634.
6. M A Imran, M S U Miah, H Rahman, May 2015, "Face Recognition using Eigenfaces," in International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 5.
7. Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti Margaret MacAlpine J. Alex Halderman, November 3–7, 2014, "Security Analysis of the Estonian Internet Voting System," in CCS'14, Scottsdale, Arizona, USA. ACM 978-1-4503-2957-6/14/11.