Online Voting Using Face Recognition and Password Based Security System

R.Sandhiya [1], D.Indumathy [2]

PG Student [CS], Dept. of ECE, Rajalakshmi Engineering College, Chennai, Tamilnadu, India [1]

Assistant Professor, Dept. of ECE, Rajalakshmi Engineering College, Chennai, Tamilnadu, India [2]

ABSTRACT:In the online voting system, people can vote through the internet. In order to prevent voter frauds, we use two levels of security. In the first level of security, the face of the voter is captured by a web camera and sent to the database. Later, the face of the person is verified with the face present in the database and validated using Matlab. The comparison of the two faces is done using Local Binary Pattern algorithm. The scheme is based on a merging an image and assigns a value of a central pixel. These central pixels are labeled either 0 or 1. If the value is a lower pixel, a histogram of the labels is computed and used as a descriptor. LBP results are combined together to create one vector representing the entire face image. A password (OTP) is used as the second level of security, after entering the one time password generated to their mail it is verified and allow to vote. It should be noted that with this system in place, the users, in this case, shall be given an ample time during the voting period. They shall also be trained on how to vote online before the election time.

KEYWORDS: Online voting, Face recognition, LBP, OTP.

I.INTRODUCTION

The election is a well-known thing in modern days of Democracy. Electronic online voting over the Internet would be much more profitable. Many voters would appreciate the possibility of voting from anywhere. This paper proposes a people who have citizenship of India and whose age is above 18 years of age and any sex can give his\her vote online without going to any polling station. There is a database which is maintained in which all the names of voter's complete information is stored.

There are some basic security requirements that need to be fulfilled by any voting system. These are: firstly, the anonymity of a voter's ballot must be preserved, and voters must not be able to prove how they have voted; secondly, the voting system must be tamper-resistant to a wide range of attacks; thirdly, a voting system must be user-friendly. In addition, voting process must be transparent and comprehensible enough so that voters and candidates can readily accept the results. In general, such online voting should satisfy such requirements as follows:
1. Accuracy
2. Simplicity
3. Verifiability
4. Democracy
5. Privacy
6. Security

For such an online voting system, security and privacy are the main concerns. From that point of view, an implementation of the online voting system appears with face recognition and password (OTP). Our approach suggests a practical application of the existing face recognition and password (OTP) that ensures the integrity of the vote cast by voter and authentication of the voter at the two levels. The advantage of the online voting system is that voter can vote from anywhere through the internet. Subsequently, the result of the election is computed from the sum of the votes which have been voted by the voters.

Literature Survey: Deutsch [3] proposed voting system based on Punch-card and mark-sense optical scan systems as well as DRE. It does not include any biometric security. After that many secure voting systems have been proposed. Malladi *et.al.* [6] process of voting starts with the card punching and the real process of online voting through ATM terminal. It ensures duplicate vote avoidance through dual-tier authentication using One Time Password (OTP) and a Random Security Question (RSQ). Jambhulkar *et.al.* [5] and Mursi *et.al.* [9] proposed Cryptographic schemes and a digital signature that ensures the integrity of the vote cast by voter and authentication of the voter.Malkawi *et.al.* [8], Sridharan [14] and Anandaraj *et.al.* [1] proposed e-voting system using simple biometrics for election process.Katiyar *et.al.* [13] proposed an online voting system using steganography. It uses images as cover objects for steganography and as keys for cryptography. The steganography is to hide the information imperceptibly into a cover, so that the presence of hidden data cannot be diagnosed. Nazatul *et.al.* [10] the scheme uses Fuzzy Extractor to provide biometric based authentication, while cryptography for the secret password which is used to provide password-based protection of the voter.

This paper proposes an online voting system scheme using face recognition and password (OTP) for security purpose. To the best of our knowledge, this is the first work that integrates face recognition with OTP for the online voting system. The noteworthy features of the proposed scheme can be summarized as follows:

- It fulfils the security requirements of a traditional voting system and brings the flexibility of the online voting system.
- It can use face recognition and OTP to authenticate the voters.

II.PRELIMINARIES

A. Face Detection and Recognition**:** Face detection and recognition are still a very difficult challenge and there is no unique method that provides a robust and efficient solution to all situations face processing may encounter. In some controlled conditions, face detection and recognition are almost solved or at least present a high accuracy rate but in some others applications, where the acquisition conditions are not controlled, face analysis still represents a big challenge.

1) Face Detection: Face detection is a specific case of object-class detection, which the main task is to find the position and the size of objects in an image belonging to a given class. Face detection algorithms were firstly focused on the detection of frontal human faces, but nowadays they attempt to be more general trying to solve the face multi-view detection: in-plane rotation and out-of-plane rotation. However, face detection is still a very difficult challenge due to the high variability in size, shape, color and texture of the human faces. Generally, face detection algorithms implement face detection as a binary pattern classification task. That means, that given an input image, it is divided into blocks and each block is transformed into a feature.

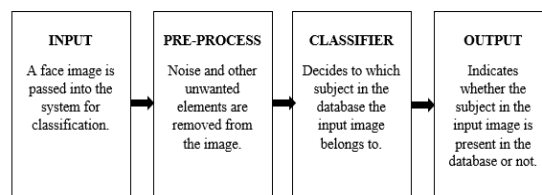| **INPUT**	**PRE-PROCESS**	**CLASSIFIER**	**OUTPUT**
A face image is passed into the system for classification.	Noise and other unwanted elements are removed from the image.	Decides to which subject in the database the input image belongs to.	Indicates whether the subject in the input image is present in the database or not.

Fig. 1. Generic representation of a face recognition system.

Face detection methods can be classified in the following categories:

- Knowledge-based methods: these techniques are based on rules that codify human knowledge about the relationship between facial features.
- Feature invariant techniques (e.g. facial features, texture, and multiple features): they consist of finding the structural features that remain invariant regardless of pose variations and lighting condition.
- Template matching methods (e.g. predefined templates and deformable templates): these approaches are based on the use of a standard face pattern that can be either manually predefined or parameterized by means of a

function. Then, the face detection consists of computing the correlations between the input image and the pattern.

- Appearance-based methods (e.g. Neural Networks, Support Vector Machine, and Eigenface): contrary to models searching techniques, appearance-based models or templates are generated training a collection of images containing the representative variations of face.
- Color-based methods: these techniques are based on the detection of pixels which have the similar color to the human skin. For this propose, different color spaces can be used for RGB, normalized RGB, HSV, CIE-xyz, CIE-LUV, etc.

2) Face Recognition: Face recognition is a challenging task which receives much attention as a result of its many applications in fields such as security applications, banking, law enforcement or video indexing. The task of face recognition in still images consists of identifying persons in a set of test images with a system that has been previously trained with a collection of face images labeled with each person identity.

Face recognition can be divided into following basic applications, although the used techniques are basically the same:

- Identification: An unknown input face is to be recognized matching it against faces of different known individuals database. It is assumed that the person is in the database.
- Verification: An input face claims an identity and the system must confirm or rejects it. The person is also a member of the database.
- Watch List: An input face, presented to the system with no claim of identity, is matched against all individuals in the database and ranked by similarity. The individual identity is detected if a given threshold is surpassed and if not is rejected.

B. Password *(OTP)*: A one-time password (OTP) is a password that is valid for only one login session on a computer system or any other digital device. OTPs avoid a number of shortcomings that are associated with password-based authentication. The most advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. A number of OTP systems also aim to ensure that a session cannot easily be impersonated without knowledge, thus reducing the attack surface further.

OTP generation typically make use of pseudo-randomness or randomness, making of successor OTPs by an attacker difficult. Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client the password is provided (OTPs are valid only for a short period of time).
- Using a mathematical algorithm to generate a new password based on the previous password, the new password is based on a challenge (e.g., a random number chosen by the authentication server).

III.PROPOSED METHODOLOGY

This section presents a description of online voting. Online voting consists of two entities: registration, online voting panel. The main purpose of this entities are: registration includes details and an image as input from the voter and stores it in a database. The online voting panel includes two: pre-processing and result.

Fig.2. describes the block diagram of the proposed system. The input to the system is in the form of text and image. It stores the details of the voters with their image. Captured images are applied to the pre-processing, feature extraction and recognition process. Preprocessing deals with techniques for enhancing contrast, removing noise. Feature extraction is used to detect and isolate various desired portions or shapes of a digitized image. Image recognition uses an image-based approach towards artificial intelligence by removing redundant data from face images through image compression using the two-dimensional discrete cosine transform (2D-DCT). The DCT extracts feature from face images based on skin color. OTP generation typically make use of pseudo-randomness or randomness, making of successor OTPs by an attacker difficult. The voting process will be done and the results are stored. OTPs avoid a number of shortcomings that are associated with password-based authentication. Then the voting process has been done and the results are executed.
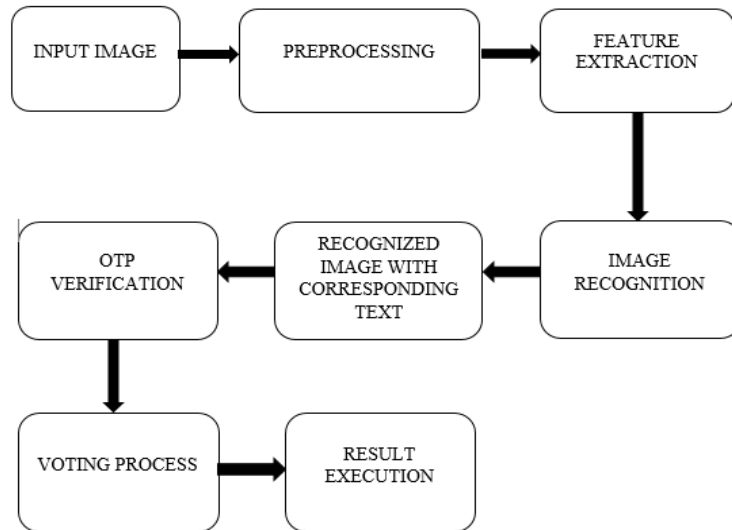
Fig. 2. Block Diagram of Proposed System

Fig.3. explains about the flow of online voting process. At first the user should register their details in the registration process then the web cam capture the image of a voter and store in database for further process. It can also update the details of the voters as well as candidates. The registered voter and candidate can access voting process through internet. They can vote to the registered candidates and it will be stored for counting process. Later the registered votes are counted and the result is viewed by the administrator.
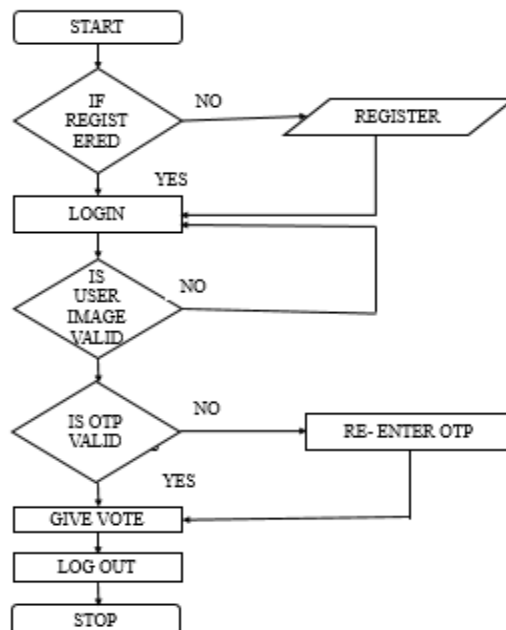
Fig .3. Flow diagram of proposed system

A. Local Binary Patterns: This operator works with the eight neighbors of a pixel, using the value of this center pixel as a threshold. If a neighbor pixel has a higher gray value than the center pixel then it is assigned as one to that pixel, else

it gets a zero. The LBP code for the center pixel is then produced by concatenating the eight ones or zeros to a binary code. A face image is first split into small regions that LBP histograms are extracted and then concatenated into a single feature vector. This vector forms an efficient representation of the face area and can be used to measure the similarities between images.
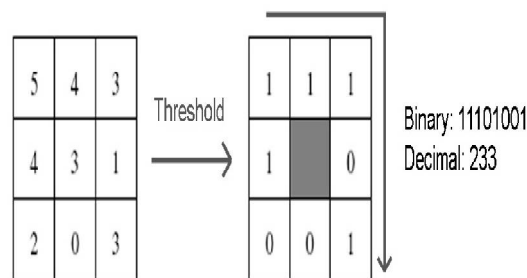

Fig.4. Original LBP Operator

B.Uniform Local Binary Patterns: A Local Binary Pattern is called uniform if it contains at most two bitwise transitions from 0 to 1 or vice versa. In a matter of fact this means that a uniform pattern has no transitions or two transitions. Only one transition is not possible, since the binary string needs to be considered circular. The two patterns with zero transitions, for example eight bits, are 00000000 and 11111111. Examples of a uniform patterns with eight bits and two transitions are 00011100 and 11100001. For patterns with two transitions are $P(P-1)$ combinations are possible. For uniform patterns with P sampling points and radius R the notion $LBP^{u2}_{P,R}$ is used with P sampling points and radius R the notion $LBP^{u2}_{P,R}$ is used.

C. Implementation Of Local Binary Patterns In Matlab: The LBP-method can be applied onimages (of faces) to extract features which can be used to get a measure forthe similarity between these images. The main idea is that for every pixelof an image the LBP-code is calculated. The occurrence of each possiblepattern in the image is kept up. The histogram of these patterns, also calledlabels, forms a feature vector, and is thus a representation for the textureof the image. These histograms can then be used to measure the similaritybetween the images, by calculating the distance between the histograms. The implementation of a code for face recognition with LBP can be split into six main steps. This is based on the methodology described in [Ahonen,et.all (2004)]. The first step is to produce a pattern for every (non-border) pixel. Then every pattern needs to be checked for uniformity, because every uniform pattern will get its own label and all non-uniform patterns will be labeled with one single label. This is done is in the second step. In the third step the images will be divided into the regions, so that in the fourth step for every region a histogram can be constructed. All histograms for one image will be concatenated to one feature vector. In the fifth step all feature vectors will be compared by applying the χ^2. The distance (a measure for the similarity) between every image from the probe set and every image from the gallery set is put in a distance matrix. From this distance matrix a rank list and a rank curve can be generated in the last step.

IV.RESULT AND DISCUSSION

The result explains about the online voting in step by step process. Fig.5 shows that it stores the information of the voter. It includes general information like name, age, sex, date of birth and e-mail ID. It is used to store the database of a voter and mail ID is collected to send an OTP to verify the registered person.

Fig.5. Registration Process

Fig.6 shows about cropping only the face section from the image and converting it to grayscale.
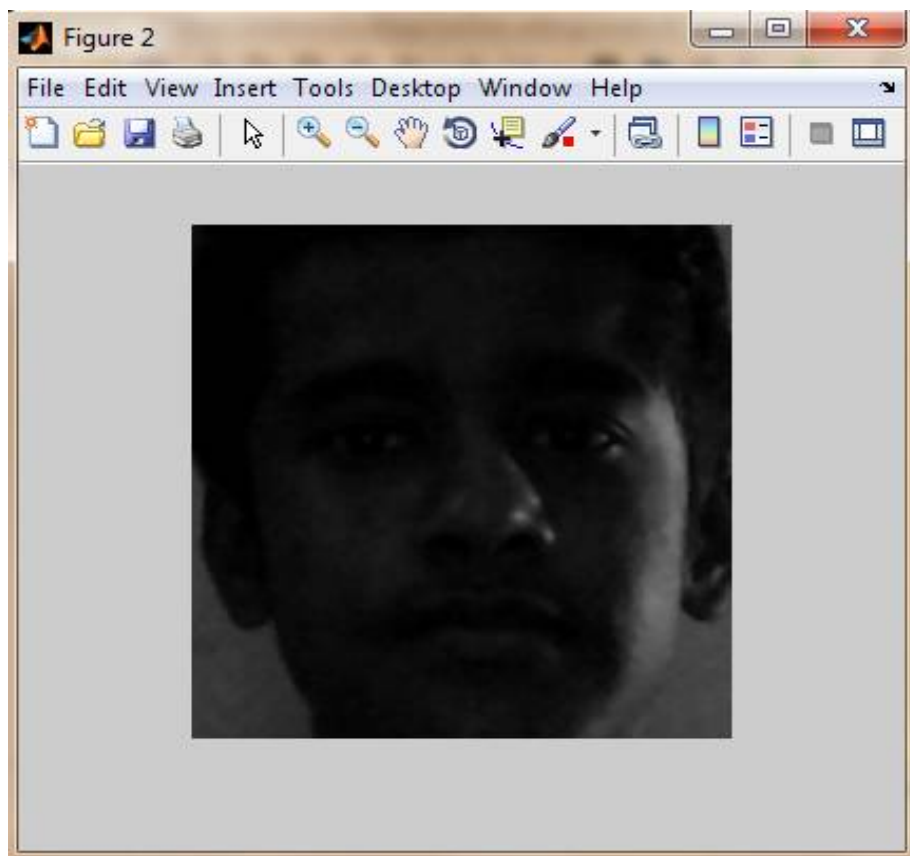

Fig.6. Cropping the image and converting it to grayscale

Fig.7 shows about the panel of the online voting process. It includes two panels, the first one contains the preprocessing and voting. It allow the voter to vote after several verifying process. And the second one includes the result session. It shows the result which party is won in the election.

Fig.7. Process of online voting

Fig.8 shows that the matching the voter from the database and after matching the image the OTP is generated to their mail. Fig.9 shows that it verifies the one time password generated to their mail.
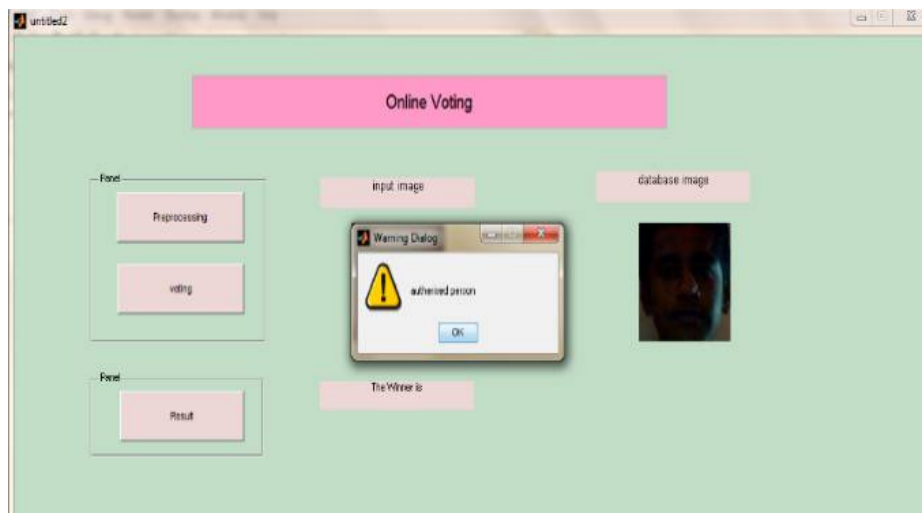

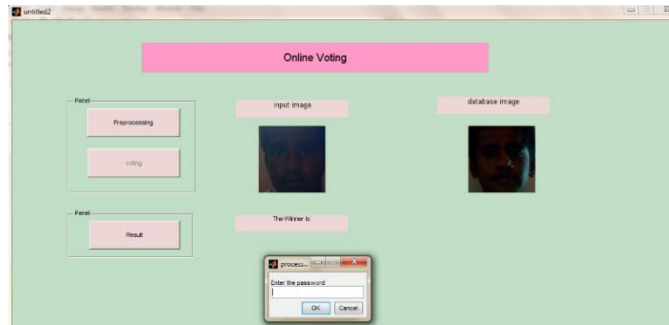Fig.8. Matching the voter from database

Fig.9. Generation of OTP matching

Fig.10 shows the symbols of the registered candidates. Here the symbols allocated to the registered candidates are flowers. And also the buttons are viewed which represents the serial number of candidates.
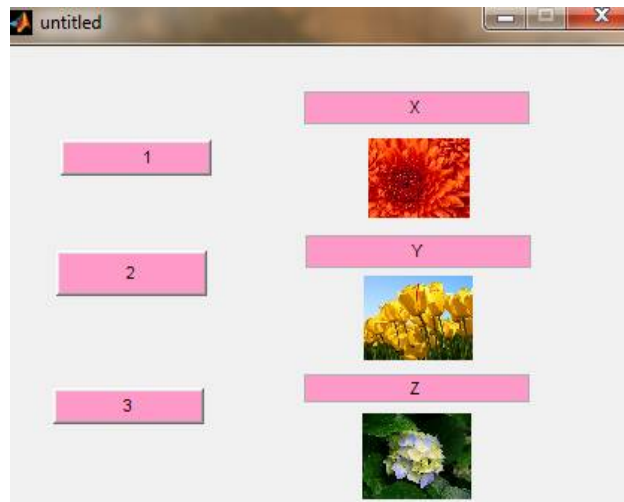

Fig.10. Symbols of the party's

Fig.11 shows the result of the voting process. It indicates which candidate is won in the election with name, symbol and with number of count.

Fig.11. Final Result Execution

V.CONCLUSION

This online voting system will manage the voter's information by which the voter can login and use his voting rights. The system will incorporate all features of the voting system. It provides the tools for maintaining and counting the total number of votes of every party. There is a database which is maintained in which all the names of a voter with complete information is stored. Voting detail is stored in the database and the result is displayed by the calculation. By online voting system percentage of voting is increases. It decreases the cost and time of the voting process. It is very easy to use and it is very less time consuming. Persons who have an internet connection at home with a web camera can vote without taking the strain to come to the voting booth. In future, the same system can be extended to include an administrator mode in which the user details can be updated dynamically through the application only. To improve the security level the face vein is can be matched. In near future, we can even implement the system in mobile phones. The user can access the website through mobile phone and cast the vote.

REFERENCES

[1] Anandaraj S., Anish R., and Devakumar P.V. (2015), 'Secured electronic voting machine using biometric', IEEE International conference on innovations in information, embedded and communication systems.
[2] Bishop M., and Frincke D. (2007), 'Achieving learning objectives through e-voting case studies', IEEE Security& Privacy, Vol. 5, No. 1, pp.53–56.
[3] Herb Deutsch (2005), 'Public opinion's influence on voting system technology', IEEE Standards Association.
[4] Hongyu Zhang., Qianzi You, and Junxing Zhang (2015), 'A lightweight electronic voting scheme based on blind signature and kerberos mechanisms', International conference on advanced networks and telecommuncations systems,pp.978-4799.
[5] Jambhulkar S.M., Jagdish B. Chakole, and Praful. R. Pardhi (2014), 'A Secure approach for web based internet voting system using multiple encryption', IEEE International conference on electronic systems, signal processing and computing technologies.
[6] Kausal malladi, Srivatsan sridharan, Jayprakash L.T. (2014), 'Architecting a large-scale ubiquitous e-voting solution for conducting government elections', IEEE International conference on advances in electronics, computers and communications.
[7] Kohno. T et al., (2004), 'Analysis of an electronic voting system', Proc. 2004IEEE symposium security and privacy, pp. 27–40.
[8] Mohammad Malkawi., Omar Al-Jarrah., Thaier S. Hayajneh., Munzer S. Ebaid, and Mohammed Khasawneh (2008), 'A biometric-secure e-Voting system for election processes', IEEE symposium on mechatronics and its applicationsMay 27-29.
[9] Mona F.M.Mursi., Ghazy M.R.Assassa., Ahmed A. AbdelHafez, and Kareem M. AboSamra (2015), 'A secure and auditable cryptographic-based e-voting scheme', International conference on mathematics and computers in sciences and in industry, IEEE.
[10] Nazatul Haque Sultan., Ferdous Ahmed Barbhuiya, and Nityananda sarma (2015), 'Pair voting: A secure online voting scheme using pairing based cryptography and fuzzy extractor', IEEE International conference on advanced networks and telecommuncations systems.
[11] Nathanael Paul and Andrew S. Tanenbaum (2009), 'Trustworthy Voting: From Machine to System', IEEE   Journal of Computer Society.
[12] Purushothama B.R., and Alwyn R. Pais (2009), 'Design and implementation of secure internet based voting system with user anonymity using identity based encryption system'. In IEEE International conference on services computing, scc '09., pages 474–481.
[13] Shivendra Katiyar., Kullai Reddy Meka., Ferdous A. Barbhuiya, and Sukumar Nandi (2011), 'Online voting system powered by biometric security using steganography', IEEE second International conference on emerging applications of information technology.
[14] Srivatsan sridharan (2013), 'Implementation of authenticated and secure online voting system', IEEE International conference on computing, communication and networking technologies.