E-voting Using One Time Password and Face Detection And Recognition

[1.] Ayesha Shaikh, [2.]Bhavika Oswal, [3.]Divya Parekh, [4.]Prof. B. Y. Jani
[1,2,3,4.] Department of Computer Engineering, Pune Vidyarthi Griha's College Of Engineering And Technology, Parvati Darshan, Pune-09.

***Abstract*— This paper introduces an online voting system in which the election data is stored and processed. To achieve higher level of security, two levels of authentication techniques are used. First authentication technique used is a Face Detection and Recognition system. In this method of authentication, the voter's face image captured during the registration is compared with the image captured by the webcam at the time of casting vote. Second level authentication is done using One Time Password (OTP) principle. After the first level of authentication is done, a pseudo random number is generated using the OTP principle that is used by the voter while casting the vote. These techniques provide a more secure platform thus overcoming vulnerabilities of the traditional voting system.**

I. INTRODUCTION

Considering how far e-commerce has come there should be provision for people to vote online with good security and convenience. In [1] it is revealed that there is a raising interest for voting on social networking tools like Facebook or Twitter and through SMS. This system allows users to send their votes directly to web services, for its computation and display the results to the voters which gives some decision power to voters. Online voting increases participation in voting as people can cast their vote form any place, any time.

A. E-voting technique

In this paper, two authentication techniques are proposed- Face Detection and Recognition(FDR), and One Time Password(OTP).In Face Detection and Recognition [2] the voter's image is captured and passed to a face detection algorithm which is used to detect his face from the image and save it as the first matching point. In [3] One Time Password principle produces pseudorandom password each time the user tries to log on. This OTP will be send to voter's mobile phone. An OTP is a password that is only valid for single login session thus improving the security.

B. E-voting for better security

This system provides a better security as it ensures that no voter is allowed to vote more than once. Also the system takes care that no voter can determine for whom anyone else voted and no voter can duplicate anyone else's vote. Every voter can make sure his/her vote is cast.

II. LITERATURE STUDY

A. Direct Recording Electronic (DRE) voting systems:

DRE systems[4] completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN, a smartcard, or some other token that allows them to approach a voting terminal, enter the token, and then vote for their candidates of choice. When the voter's selection is complete, DRE systems will typically present a summary of the voter's selections, giving them a final chance to make changes. Subsequent to this, the ballot is "cast" and the voter is free to leave.

B. Electronic vote collector (EVC)

In this platform, the voters deposit their votes on their own personal computers, while a mobile device pass close those machines and collect their stored votes, under the coordination of a management software working in a stationary server. It is presented as a taxonomy of e-Voting systems, and the authors present requirements for the project and implementation of e-Voting systems. It is described a local e-Voting system which eliminates physical ballot-boxes, reducing costs and efforts, and consequently being less time consuming. It is described an experimentation about e-Voting by cell phones, by SMS protocol.

C. Online Voting System with Multi Security using Biometric and Steganography:

Highly Secure Online Voting System with Multi Security using Biometric and Steganography, the basic idea is to merge the secret key with the cover image on the basis of core image. The result of this process produces a stego image which looks quite similar to the cover image. The core image is a biometric measure, such as a fingerprint image. The stego image is extracted at the server side to perform the voter authentication function. It used secret message with 288 bit length. As the actual secret key is never embedded in the stego image, there will be no chance of predicting secret key from it.

III. PROPOSED WORK

A. *Face Detection and Recognition*

In Face detection and recognition first the image is grabbed by an interface. Then the input image is blurred for noise reduction. Separation of RGB components of every pixel takes place after which HSV values are obtained. The HSV image undergoes thresholding. Thresholding is the simplest method of image segmentation. It is usually used for feature extraction where required features of image are obtained. After the image is cropped, resizing of image takes place in scaling. Area of concern of image is obtained during the segmentation process. Template matching is a process in which features of an input image with the imge stored in database are compared and matched.

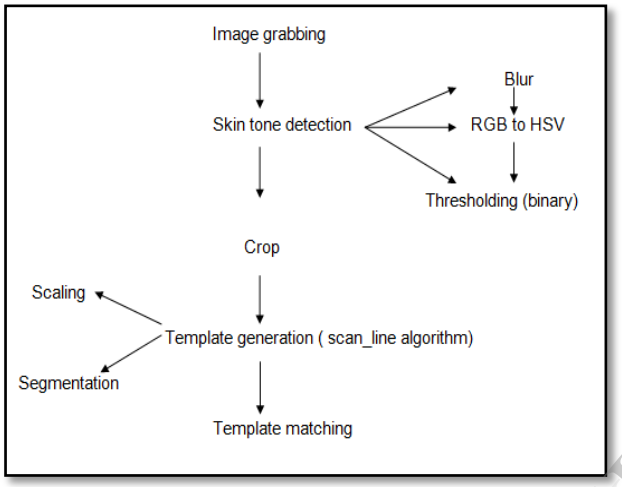

Figure1.Steps of Face Detection and Recognition algorithm

B. *One Time Password*

Let us assume that For OTP,

Let S be a set of functions where PRNG- Psuedo Random Number Generator, SHA-Secure Hash Function, DB-Database, OTP- One Time Password generated. OTPH-Hashed OTP that will be stored in the database.

S = {PRNG,SHA,DB,OTP,OTPH},

Random OTP = PRNG (seed),

OTPH = SHA (OTP),

Result is the Boolean value received from the comparison function.

Result = Comparison (SHA(OTP),OTPH).

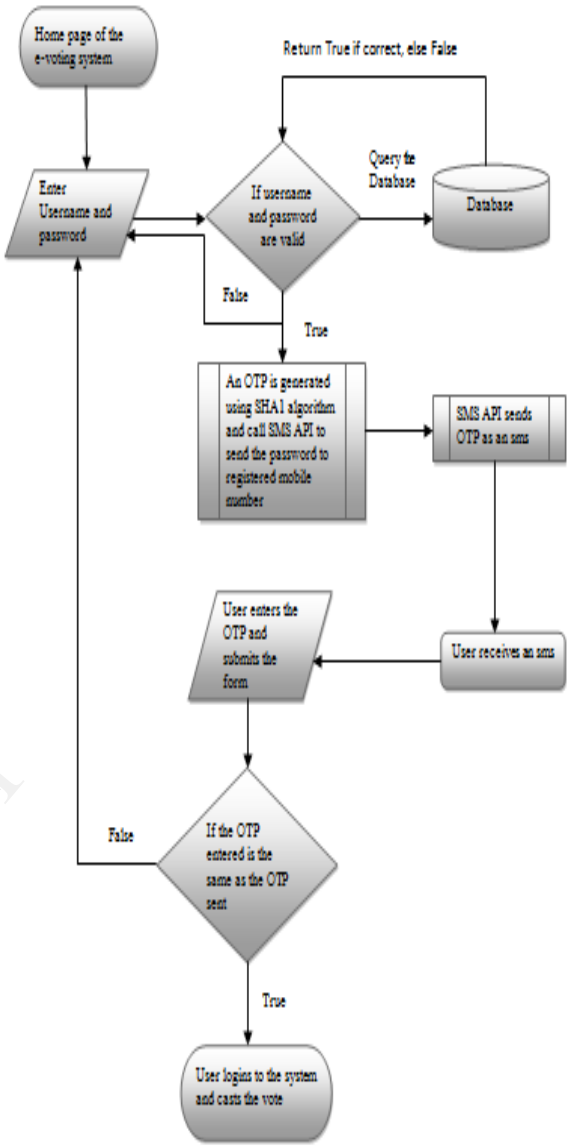

Figure2. One Time Password Generation Steps

IV. SYSTEM ARCHITECTURE

1. Registration (user information)
2. Login
3. Face Detection And Recognition
4. One Time Password
5. Vote

The developed application described inside this paper is based on an e-Voting methodology. The voter's image is captured using a webcam. This image is used as an input to the face detection algorithm. This image is sent to the server side for verifying the user. This is achieved by template matching where the image received from the user side is compared with the image stored in user database at the time of registration. Once the user is verified, a One Time Password is generated and sent to the user's email id/sms on his cell phone. After the users enters the otp, he can cast his vote. The vote cast by him

is then stored in the database and is taken for tallying purpose after the deadline for voting process.

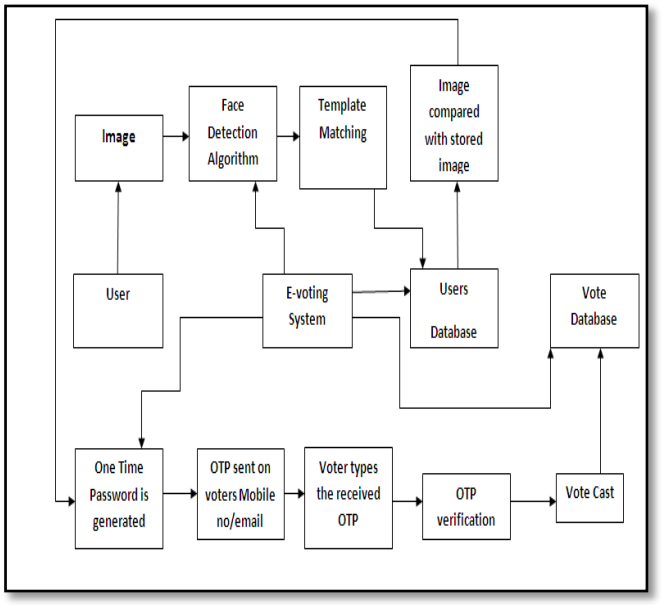

Figure3. E-voting System Architecture

V. CONCLUSION

The major advantage of e-voting is user can cast the vote from any place and at any time with increased security. We have proposed an approach to e-voting system using Face Detection and Recognition system (FDR) and One Time Password (OTP) as an Authentication technique in online voting, thus security increases as there are two levels of authentication and it will overcome the problem of fake votes.

REFERENCES

[1]. SKINNER, C. "75% of young adults want to vote by sms in the election. 89% expect text voting to be introduced soon". PC ADVISOR. February18, 2010

[2]. Noha E. El-Sayad, Rabab Farouk Abdel-Kader, Mahmoud Ibraheem Marie" Face Recognition as an Authentication Technique in Electronic Voting" (IJACSA) INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2013

[3]. Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones",EIGHTH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: NEW GENERATIONS, 2011

[4]. Tadayoshi Kohno, Adam Stubblefield† , Aviel D. Rubin‡, Dan S. Wallach§,"Analysis of an Electronic Voting System", IEEE COMPUTER SOCIETY PRESS, MAY 2004