Webcam Based Facial Recognition Using OTP Verification for Voting System

[1]Prof. Akshay S. Agrawal, [2]Mr. Gupta Bhavesh I, [3]Mr. Maurya Ajay R, [4]Mr. Phadnis Heramb B.
[1]Asst. Professor, [2,3,4]UG Student, [1,2,3,4]Computer Engg. Dept. Shivajirao S.Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.
[2]bhaveshgupta027@gmail.com, [3]mauryaajay47@gmail.com, [3]heramba.phadnis@gmail.com

Abstract—In urban region voting is the major issue as the identification of the person is the most important issue. As they do not have mostly the identity proof rather than the voting card & the fake voting is done on the large scale. To avoid this, the project should be developed in such a way that it will store the identity of the voters & at the time of voting this identity will be matched using the facial recognition system to avoid the fake voting. This system will capture the face of the voter and match with the existing faces in the stored databases. After the verification of the valid face identify, an OTP will be generated and send to the voters register mobile and then he will use that provided OTP and then only his validation is succeeded and allowed to vote.

Keywords: Spontaneous facial expression, Eigen face, Principal Component Analysis (PCA), OTP (One Time Password), Image processing.

I. INTRODUCTION

India is an egalitarian country. Indian government is of the people, for the people and by the people. Therefore, elections play an important role. The most important feature of a democracy includes that the people must have the right of citizenship to choose the ruler for their country, state or local area. Thus, electoral process that is election by voting is an important aspect. With the evolution of technology, various voting techniques have been implemented such as ballot machines, EVMs, Kiosks and so on. [1]

However, currently many E-voting systems have also been introduced namely punch scan, optical scan, specialized voting Kiosks and so on. Online voting using internet is one of the methods that have emerged. This system has been developed so that the voters at different remote locations can vote during general elections in his/her country. Voters just need internet access. [1]

With the advent of technology, mobile phones with programmable platforms have emerged. Also, latest technologies such as biometrics (thumb scans, iris scans and face recognition) can be used to assure security for the voter authentication. Using some of the above-mentioned techniques and technologies, an effort has been made to develop an E-voting system for a modern individual. [1]
The two authentication techniques are Face Detection and Recognition and One Time Password(OTP). In Face Detection and Recognition, the voter's image is captured and passed to a face detection algorithm which is used to authenticate his face from the image and save it as the first matching point. In 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. [2]

II. LITERATURE SURVEY

A. *Direct Recording Electronic (DRE) voting*

DRE systems 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 few states allow voters to cast votes without any verification at all. After this, the voter is typically given a PIN, a smartcard, or some other proof that allows them to reaching a voting terminal, enter the proof, and then vote for their candidates of choice. When the voter's selection is complete, DRE systems will typically present a curt of the voter's selections, giving them a last chance to make changes. Subsequent to this, the ballot is "cast" and the voter is free to leave. [2]

B. *Electronic vote collector (EVC)*

In this platform, the voters drop their votes on their own personal computers, while a mobile device pass close those machines and collect their stored votes, under the coordination of management software working in a stationary server. It is presented as 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. [2]

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

Highly Protected 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 much 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 hidden 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. [2]

D. *Fingerprint Recognition*

Fingerprint recognition or fingerprint verification refers to the computerized method of verifying a match between two Human fingerprints. Fingerprints are one of many forms of biometrics used to spot individuals and verify their uniqueness. A fingerprint looks at the patterns set up on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional law enforcement method of matching blueprint; others use straight minutiae matching devices and still others are a bit extra unique, including things like more border patterns and ultrasonic. A larger variety of fingerprint devices are available than for any supplementary biometric. Fingerprint authentication may be a good choice for this touch sensing voting systems, where you can give users sufficient explanation and guidance, and where the system operates in a controlled environment. It is not shocking that the terminal access application area seems to be based almost exclusively on fingerprints, due to the moderately low cost, small dimension, and ease of integration of fingerprint authentication devices that will be implemented. [3]

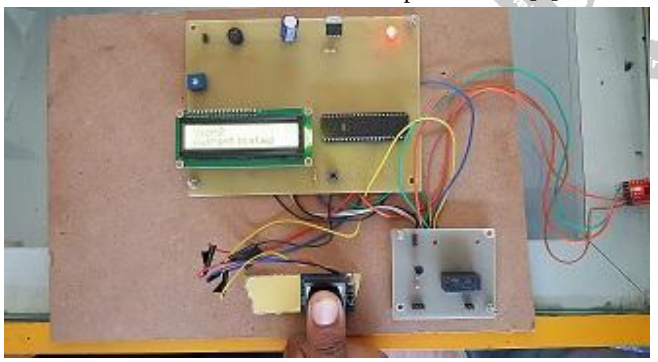


Fig 1. Fingerprint scanning process

E. *Poll-Site Internet Voting System*

In this system, the voters cast their votes from any poll-site via ballot. Vote tallying is a fast and certain process. Security risks are managed because election officials control the physical environment as well as the voting platform.

F. *Kiosk Voting System*

In this system, all voting machines are placed away from polling stations. Public places such as libraries, schools, colleges are used as voting stations. The physical environment and voting platform is still controlled by election officials. Security and privacy is maintained with the help of volunteers, officers and even cameras. This prevents coercion or other types of problems.

G. *Remote Voting Via Internet:*

In this voting system, the voter can cast his/her vote from any location with internet access. The system aims at providing convenience and comfort to the voters. However, the major drawback of this system is that there are numerous security matters which are difficult to supervise and have not been administered by this system. With the advent of technology many enhancements have been made in the voting equipment. Those include:

1. Paper-Based Voting.
2. Lever Voting Machine.
3. Punch Card.
4. DRE Voting Machine
5.

III. AIM

The main Aim of the system is:

- Arrangement of improved voting services to the voters through fast, timely and convenient voting.
- Reduction of the cost incurred by the Election commission of India during voting time in paying the very many clerks employed for the advantage of the success of the manual system.
- Check to ensure that the members who are registered are the only ones to vote. Cases of “Dead People” voting are also minimized.
- Therefore, vital points that this system emphasizes on are listed below: -
  1. Required less number of staff during the election.
  2. This system is lot simple to independently moderate the elections and subsequently reinforce its transparency and fairness.
  3. Less capital, less effort, and less labour intensive, as the primary cost and running a secure online portal.

Increased number of voters as individual will find it easier and more convenient to vote, especially those abroad.

IV. EXISTING WORK

In the existing voting system, the whole election process is divided constituency wise to facilitate the security forces and to make the election system fair. To maintain discipline and security requires a great amount of man power so, it is bit crucial to accomplish election in a single day. Allocation of polls is done by election commission in advance. Generally polling booth is setup in school and community halls. The public can come to know about the location of voting. Time and place for voting is predefined. Each polling station is opened for at least 8 hours on the Election Day. [4]

Figure below shows first of all the voter need to reach at polling booth. The first step is the identity verification, carried out by an associated person on the duty. Then officer makes mark of inedible ink on the balloter's left forefinger thereafter voter has to sign in register followed by reaching inside the voting compartment. To mark a vote, a voter has to press blue candidate button on EVM machine across the name and symbol of his/her choice. When the button is pressed, the red lamp will glow against the symbol with beep sound which indicates that vote is successfully recorded. Every time this process needs to be repeated as well as adjustment of building and manpower on the location of voting is required. [4]

Fig 2. Existing System

TABLE 1. Comparative Study

Sr. No	Paper Title	Author's Name	Technique Used	Merit	Demerits
1	A Secure E-Voting System Using Face Recognition and Dactylogram	Patil Rahul H., TarteBabita B., Wadekar Sapana S., Zurunge Bhakti S., Prof. Phursule Rajesh	Election-Voting System, Secure E-Voting, Face Recognition, Dactylogram.	Time Complexity is more	Less understandability for users
2	E-Voting System for Modern Individual	Madhumita Deshpande, Deepali Zambre, Prajakta Mandle, Komal Hankare, Kanchan Shelke	Android, Face Recognition, Remote Voting, OTP, Template Matching, Two-factor Authentication	This Paper concisely explains the design and working of the application, which delivers remote voting ability, precision, greater privacy, good interface and reliability towards the entire election process.	Less user applicability
3	E-Voting Using Android Mobile	Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane	Spontaneous facial expression, Eigenface, Principal Component Analysis (PCA).	This paper has successfully introduced a new design of E-voting application using Android Platform.	Difficulty to understand
4	E-voting Using One Time Password and Face Detection and Recognition	Ayesha Shaikh, Bhavika Oswal, Divya Parekh, B.Y. Jani	Detection and Recognition system (FDR), One Time Password (OTP) as an Authentication technique in online voting	The paper focuses on the importance of careful design of the user-interface devoted to the use of wide range of users of different level of expertise with using computers	Less user understandability
5	Webcam Based Facial Recognition Using OTP Verification for Voting System	Ms. Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane	Eigen face, Eigen Vectors, image processing, OTP (One-Time Password), PCA (Principle Component	This paper give better understanding of online voting systems through facial recognition and.	Less user understandability

V. PROPOSED WORK

A. Architecture Diagram

Figure shows the overall architecture of proposed voting process scenario. To carry out the whole procedure successfully an internet connection is essential. Also, every person must have mobile phones to carry out our application successfully.

In the first step the registration process is done by the voters through an application. Then in the second step the application will start its process. It first captures the face of the voter using camera. Then that image is send to the existing database. Here it uses already existed database or centralized database, which contains voter's information

with photos. Then system compares the send images with already stored images in centralized database.

Once the image is recognized successfully or matched with the existing images of the database then the server sends the OTP (One-Time Password) to the voters registered mobile number. Then voter enters that OTP, then database again verifies that entered OTP by voter and if it is correct that means it is valid user.

After that the candidate's list will appears. This list contains the candidate name and in front of that name the button named 'Vote' is provided. Voter should have to press that button then only the voting is done and the voting procedure is completed.

Here security is also necessary to protect the system. For that session level security mechanism is being used. First client need to request valid session id to server. Once server validate client it will respond with session id. By handshaking this session id communication takes place. On each request session id, will be send and validate. Once client logout from system it will destroy session id. Also, password is encoded in MD5 format, so nobody able to see the password text.

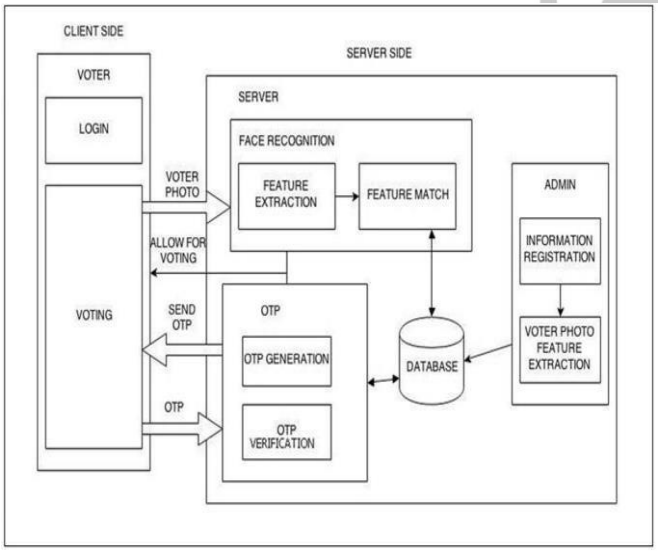


Fig 3. Proposed Voting Process scenario

B. Algorithm

This method is based on information theory which will decompose the face images. Then forms the minute set of the characteristics features images which are called as "Eigen faces". This is nothing but the principal components of the face images of the training set. For face recognition, the Eigen face method is one of the most efficient and simplest approaches. In Eigen face method, the distance is being measured between couples of images. If that distance is less than a provided threshold value, then it is an identified face or else it is an unidentified face.

In the Algorithm, it has two set of image blocks, first one is training set image block and second one is test set image block. In training set image block, firstly the Eigen face of image in the database i.e. trained image is obtained. Then the weight W1 is calculated by using the Eigen face and the training set. In the testing set image block, image X is the unknown input image which is nothing but the captured image. The weight W2 is calculated using the input image and the Eigen face. Value of D is calculated by finding the average of distances between W1 and W2. If the D value is less than 0, then the face is recognized. Then the input image X and W2 values are stored. If the D value is greater than 0, then the face is not recognized.

Step 1: Preparation of data: The faces of the training set (Γ_i) has been taken for the processing.

Step 2: Subtraction of mean: Here we have to calculate the average matrix (Ψ) first, then it is being subtracted from original faces (Γ_i) . Then the result of that is stored in the variable Φ_i.

$$\Psi = \frac{1}{M}\sum_{n-1}^{M}\Gamma_n$$

$$\Phi_j = \Gamma_j - \Psi \quad (1)$$

Step 3: Calculating covariance matrix: The covariance matrix C is calculated as,

$$C = \frac{1}{M}\sum_{n-1}^{M}\Phi_n \Phi_n^T \quad (2)$$

Now the eigenvectors (Eigen faces) u_j and its corresponding eigenvalues λ_i of the vector C should be calculated.

Step 4: Calculating eigenvectors and eigenvalues of the covariance matrix: The covariance matrix C in equation 2 has dimensionality as$N^2 \times N^2$, so it has N^2 eigenfaces and N^2 eigenvalues. For example, if we taken 256×256 images then we have to compute total65, 536×65, 536 matrixes and then we have to calculate total65,536 Eigen faces. So, this is quite difficult and not possible. So, for that we use PCA which describes a small set of vectors with the large dimensional space. So here PCA provides only M images and M non- trivial eigenvectors. Hence here for solving the eigenvectors, we can take the eigenvectors of the new matrix as$M \times M$:

$$L = A^T A$$

By using the below math trick, we get the above equation:

$$A^T A v_i = \mu_i v_i$$

$$AA^T A v_i = \mu_i A v_i$$

Here V_i is an eigenvectorofL. So here M eigenvectors of L are being used to form the M eigenvectors u_i of C that will form our Eigen face basis:

$$u_l = \sum_{k-1}^{M} v_{lk}\,\Phi_k \; l = 1, M$$

Here u is Eigen faces.

Step 5: Recognition of the faces: The recognition of new (unknown) face Γ_{new} amongst the known faces is carried out proceeds into two steps. First is the new image is transformed into its Eigen face components and second is the resulting weights form the weight vector Ω_{new}^T

$$co_k = u_k^T(\Gamma_{new} - \Psi)\; k = 1 \ldots . M'$$

$$\Omega_{new}^{T} = [\omega\omega\omega_2 \ldots\ldots \omega_{M'}]$$

The Euclidean distance between two weight vectors $d(\Omega_i, \Omega_j)$ is calculated by using similarity of the images j and$j$. If the minimum Euclidean distance between Γ_{new} and other faces exceeds -on average -some threshold value, one can assume that Γ_{new} is an unknown face, Else it is considered as a known face.

Step 6: Calculating Euclidean Distance: Let an arbitrary instance x be described by the feature vector as,

$$x = [a_1(x), a_2(x), a_r(x)]$$

Here $a_r(x)$ is the value of the r^{th} attribute of instance x. then the distance between two instances as x_i and x_j is defined to be (x_i, x_j) :

$$d(x_j, x_j) = \sqrt{\sum_{r=1}^{n} (a_r(x_i) - a_r(x_j))^2}$$

C. *Mathematical Model*

It uses Set theory to explain the system.

Let G be a closed graph that represents the system

$$G = \{E, V\}$$

Where, E represents the whole set of edges

$$E = \{E_1, E_2, E_3, E_9\}$$

And V is a whole set ofvertices

$$V = \{V_1, V_2, V_3, V_7\}$$

In the graphical representation of the system, vertices in the set V represent the modules which are connected through directed edges in the set E representing the input/output of modules.

TABLE II. VERTEX DEFINITION

Vertex	Modul
V_1	New user
V_2	Voter & Application User
V_3	Android Application
V_4	Server
V_5	Java Client
V_6	Database
V_7	Vote

TABLE III. EDGES DEFINITION

Edg	Input/out
E_1	Register for new user
E_2	Giving user data to Java client
E_3	Fetching Server
E_4	Storing Data in Database
E_5	Acknowledgement to User
E_6	Generate New User
E_7	Fetching Application
E_8	Entering Vote
E_9	Sending Vote to Server

Let Fe be a rule of E into V such that for given edge; it returns vertices.

$Fe(E) \mapsto V$

$F(E1) = \{V1\}: V1$ is called using $E1$ for registration of new user.

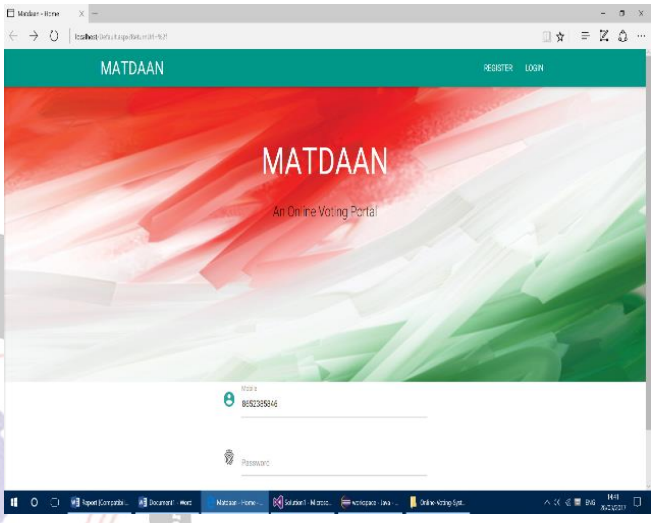
$F(E2) = \{V5\}$: User data is passed to $V5$ using $E2$ to verify user documents.

$F(E3) = \{V4\}$: User data is passed to $V4$ using $E3$ to fetch server.

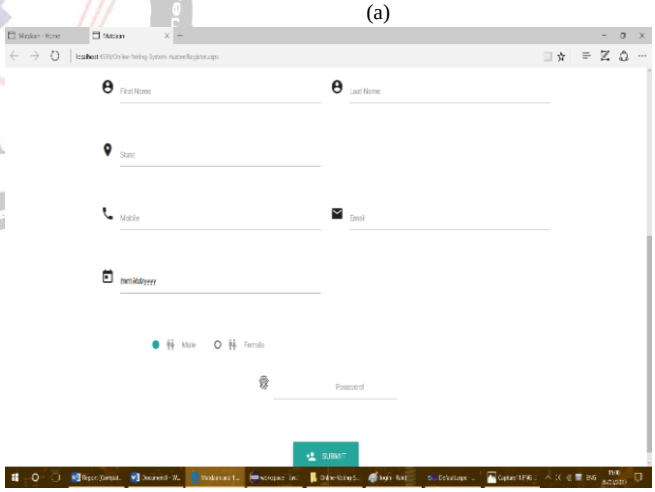
$F(E4) = \{V6\}: V6$ Is called using $E4$ to store data in database.

$F(E5) = \{V1\}: V1$ is called using $E5$ for giving acknowledgement to the user.

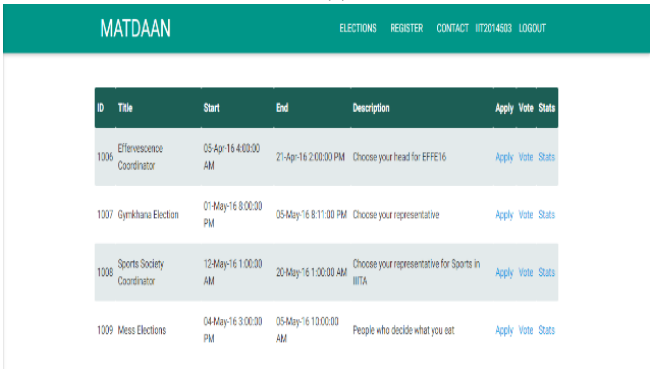
VI. RESULTS



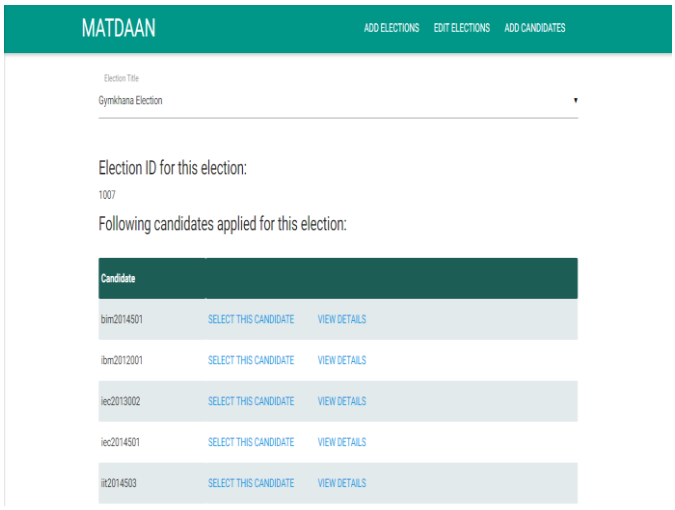
(a)



(b)



(c)



(d)

(f)

Fig 4: The whole ***E***-Voting procedure

(***a***):***The*** Sign-In procedure for voters.

(b): If voter is not registered then voter have to fill their details and then face is captured.

(c): Election details is displayed.

(d): Candidates list is displayed.

(e): Voter select the candidates.

(f): Voting is done.

Figure 4(a) shows the Sign-In procedure for voters. If the voter is already registered, then Sign-In using the given username and password. In Figure 4(b) if the voter is not registered then voter have to fill their detailed information such as name, age, address, username and password. Then click on face capture button, will capture the face of the voter. Figure 4(c) provides the detail information about the election, such as election name, election date, and election ward and election disc. Figure 4(d) provides the list of the candidates. In Figure 4(e), the voter is free to vote for the particular candidate. Figure 4(f) displays the message that the voting is done successfully.

VII. CONCLUSION

We have tried to implement the paper Ms. Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane "Mobile based facial recognition using OTP verification for voting system" IEEE 2015 and according to the implementation the conclusion is this is a Novel technique that will give us best results to get better understanding of online voting systems through facial recognition and OTP verification.

This paper has successfully introduced a new design of E-voting application using Internet Platform. This paper concisely explains the design and working of this application, which delivers remote voting ability, precision, greater privacy, good interface and reliability towards the entire election process. The utilization of modern technologies like face recognition using template matching mechanism, OTP generation ensures that the application uses latest advances in technology and thus gives better performance.

REFERENCES

[1] Hari K. Prasad, J. Alex Haldermany, Rop Gonggrijp, Scott Wolchoky, Eric Wustrowy, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, *"Security Analysis of India's Electronic Voting Machines*", April 29, 2010.

[2] Sheifali Gupta, O.P. Sahoo, Ajay Goel, Rupesh Gupta, *"A New Optimized Approach to Face Recognition Using EigenFaces*", Global Journal of Computer Science and Technology Vol. 10 Issue 1, April 2010.

[3] S. Ravi, S. Wilson, *"Face Detection with* Facial Features and Gender Classification Based *on Support Vector Machine*", 2010 Special Issue - International Journal of Imaging Science and Engineering.

[4] Hemlata Sahu, Anupam Choudhray, "Polling System Using GSM Facility", International Journal of Scientific & Engineering Research. Volume 2, Issue 10, Oct-2011.

[5] Mr. Mayur Patil, Mr. Vijay Pimplodkar, Ms. Anuja R. Zade, Mr. Vinit Vibhute, Mr. Ratnakar Ghadge, *"A Survey on Voting System Techniques"*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013 ISSN: 2277 128X.

[6] Feng-Li Lian, Yi-Chun Lin, Chien-Ting Kuo, and Jong-Hann Jean, *"Voting-Based Motion Estimation for Real-Time Video Transmission in Networked Mobile Camera Systems"*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 9, NO. 1, FEBRUARY 2013.

[7] Gomathi.B, Veena priyadarshini.S. S, *"Modernized Voting Machine using Finger Print Recognition*", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[8] Dr. Aree Ali Mohammed, Ramyar Abdolrahman Timour, *"Efficient E-voting Android Based System"*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, 2013 November.

[9] Sanjay Kumar, Manpreet Singh, *"Design a Secure Electronic Voting System Using Fingerprint Technique*", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, 2013.

[11] Ganapatikrishna P. Hegde1, M. Seetha, *"Real Time Voting System Using Face Recognition for Different Expressions and Pose Variations*", IJRET: International Journal of Research in Engineering and Technology, ISSN: 2319-1163.

[12] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari and S. N. Mugunthan, *"Highly Secured Online Voting System over Network*", Indian Journal of Science and Technology.

