Secured Electronic Voting System using Biometrics

Karthik G Maiya , Vineesha. T, Veena G and Sujay S.N.
Dept. of TCE, K S Institute of Technology,
Bangalore-109

***Abstract*—In India voting procedure strictly follows the principle of electronic voting machine (EVM) which has simple design, reliability and fast accessing characteristics. Unfortunately, due to hardware problems in EVM's, malfunctioning officer's and illegitimate voter's invalid votes are being casted. This paper provides conceptual solution through multimodal biometrics which helps in enhancing security, eradicating the fraud and provides high level authentication. High accuracy is obtained by fusion of face and finger print recognition system.**

***Key words* — Electronic voting machine, multimodal biometrics, face recognition, finger print recognition**

I. INTRODUCTION

Voting has evolved over years [1] from purely manual process to more electronic means. The use of electronic devices in voting is known as electronic voting. According to electronic voting we should be able to ensure that authenticity of cast ballot can be verified and transaction should be untraceable.

Current voting system is based on a ballot machine where, when we press the button with the symbol the voting is done. Here there is a security risk, the person who votes may be fake person voting. The people there might not know that a person is using fake voting card, this may cause problems.

Electronic voting system security can be enhanced using Biometrics. Biometrics is the measurement and statistical analysis of a person's unique physical and behavioral characteristics. There are many techniques in biometrics like Face recognition, Finger print, iris recognition, hand geometry, palm veins, palm print etc.

In this technique, Face recognition and Finger print is used. A facial recognition is a biometric method of identification of an individual by comparing live capture or digital image data with the stored image data for that person. Finger print recognition refers to the method of identification and confirmation of the identity of a person based on comparison of two Finger prints (finger print in database and sensed finger print) and used for authenticating in computerized systems.

II. EXISTING VOTING SYSTEM

The existing voting procedure follows the principle of electronic voting machine (EVM) which has simple design, reliability and fast accessing characteristics. Unfortunately, due to hardware problems in EVM's, malfunctioning officer's and illegitimate voter's invalid votes are being casted, and the same person can vote multiple times. Voting system must provide results quickly, but existing voting system takes much time to produce the result.

In unimodal biometrics like Finger print has many draw backs like the Finger print will be taken with which the dirt inthe Finger, greases and other contaminated content will be recorded and there will be chances of finger print getting rejected. When the person has some marks on the finger or if he has cut on his finger the person will be considered an invalid voter [2].

This paper provides the conceptual solution for fraud voting procedure through multimodal biometrics which helps in enhancing the security, eradicating the fraud which provides high level authentication and consumes less time to provide results. Multi model biometrics is the fusion of two or more types of biometrics. High accuracy will be achieved by fusion of Face and Finger print recognition systems compared to present EVM system.

III. PROPOSED /PROTOTYPE DESIGN

The proposed EVM system has two inputs, one of the inputs is Face image and another is Finger print. Initially, in the Face recognition part, web camera captures the face image and it is processed as shown in figure. 1. The face region will be detected using the Viola and Jones algorithm[3], which contains three types which are Haar-like feature[4][5], AdaBoost and Cascading. The face features are extracted from the detected face image using HOG algorithm. The HOG algorithm[6][7] consists of two methods they are Intensity based method and Feature based method. Intensity based method is used to extract the face intensity features and feature based method is used to extract the magnitude and angle of face.

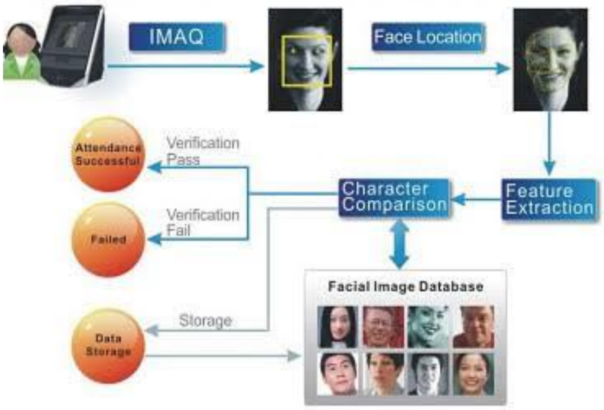


Fig.1. Face recognition verification process

The formulae to calculate magnitude and angle are given as

$$Magnitude = \sqrt{(I_x^2 + I_y^2)} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ 1$$

$$Angle = tan^{-1}(Y/X) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 2$$

I_x and I_y are intensity values written in rows and columns of a matrix that represents the image. Euclidean distance matcher is used for Face and Finger print modalities[8].

The Face images of individual are taken during enrollment time and that will be stored in the database. The database images and the captured image are compared and the result is taken.

Finger print [9] image is taken from the finger print module and compared with the finger prints which are stored in the database as shown in figure 2; finger print module stores the finger prints in its own memory. Finger print matching is done using Gabor filter using support vector machines[10] [11].

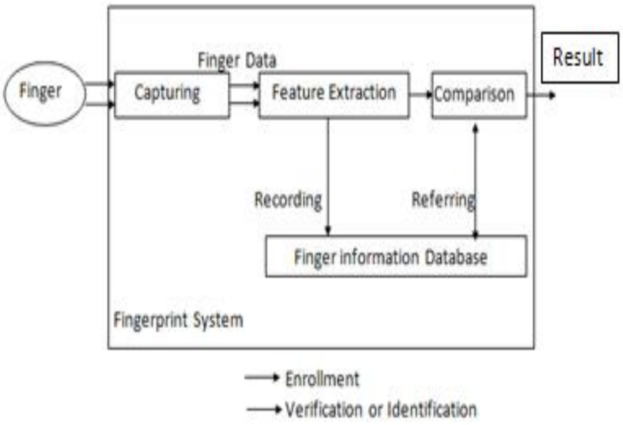


Fig. 1. Finger print verification

The features of the Face module and the Finger print module are fused as shown in figure 3and recognition result is given to the PIC18F458 microcontroller and the person is matched or not matched is displayed in the LCD display. Then the person, who is recognized, will be allowed to vote.

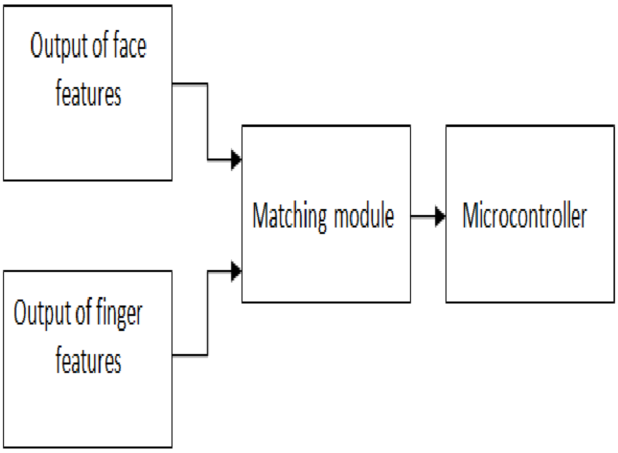


Fig. 2. Interfacing to microcontroller

LCD display is used to display the messages to the voter for example, select a candidate, vote accepted, matched, not matched etc. A buzzer is used to alert the user. The buzzer will turn on if the person comes again to vote, if the input does not match and if any malpractice takes place or if the person comes again for voting.

The below figure is the proposed block diagram for electronic voting system using biometrics.

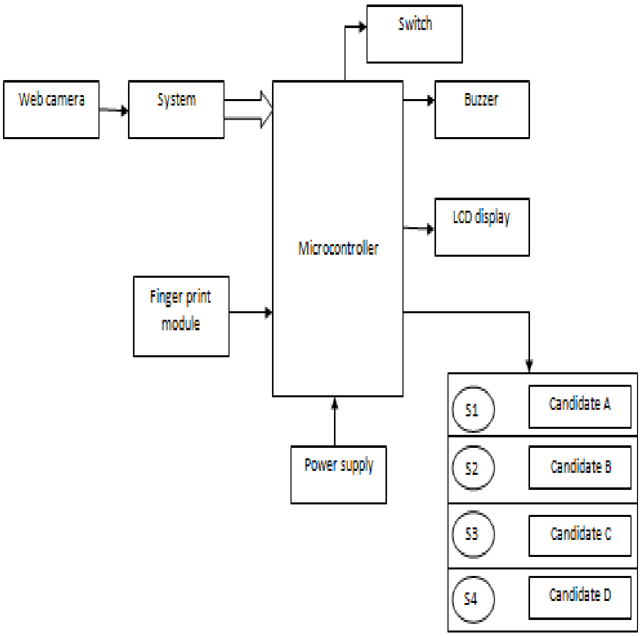


Fig. 3. Block diagram of proposed EVM

Switch can be operated in two modes which are mode A and mode B. Mode A indicates that switch is in voting mode and mode B indicates that switch is in counting mode. Votes will be accepted only when the switch is in the voting mode. S1, S2, S3 and S4 are the buttons used to represent the candidates. The voter should press any one of the button. If the voter will press more than one button at a time the buzzer will turn on or the first button pressed will be taken as the vote. The face recognition has been implemented using MATLAB[12].

IV. ALGORITHM FOR THE PROPOSED DESIGN

Algorithm for voting module:

Step 1: Keep the switch in voting mode
Step2: Capture the face and finger print using web camera and finger print sensor.
*Step 3:*If both the inputs are matched go to step (7)
Step4: If only one input will match and other does not match booth head will be given the authority to decide whether the user is the user is the right person or not
Step 5: Booth head will enter the secret key, if it is correct the he/she will check which biometry is not matching.
Step 6: If both the inputs does not alarm will turn on and LCD will display not allowed to vote
Step 7: The voter will be allowed to press in one of the buttons with candidates’ symbol and the votes will be stored in the memory.
Step 8: If voter will press more than 1 button then LCD will

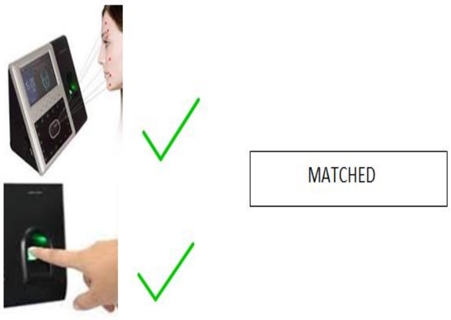
display to press any one button and go to step (7).

Algorithm for counting mode

Step 1: capture the face images and finger print using web camera and finger print sensor.
Step 2: If the inputs are matched, the authorized person will be allowed to access the votes and count them.
Step 3: If it doesn't matches go to step (1).
Step 4: The votes will be counted and displayed.

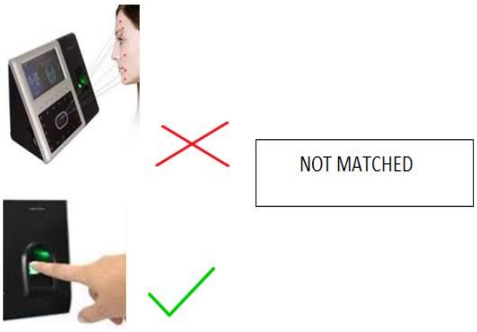
V. CASE STUDY

Case I: Both the inputs (face image, finger print) are matched



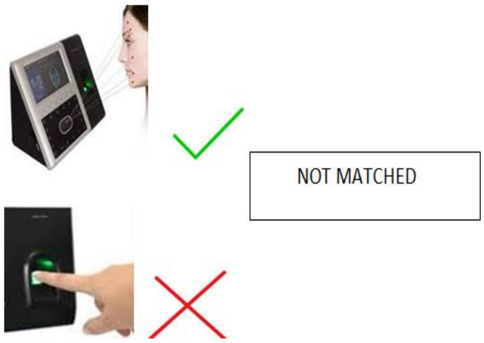
The LCD will display that the inputs are matched then it will ask the user to vote by displaying the candidates' profile.

Case II: Finger print is matched but face image doesn't match



The booth head will check whether the voter is the right person or not by checking the database. The voter will be allowed to vote if he/she is the right person.

Case III: Face image is matched but finger print doesn't match
The booth head will check whether the voter is the right person or not by checking the database.



The voter will be allowed to vote if he/she is the right person.

Case IV: Both the inputs doesn't match

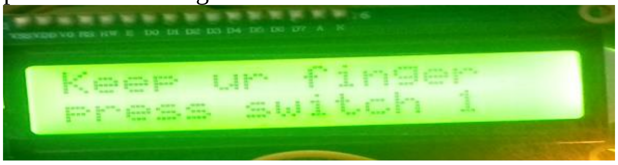
NOT MATCHED

The alarm will turn on and the user will not be allowed to access till the booth head will approve his/her identity

Case V: An unauthorized person comes to vote
The alarm will turn on to alert the officers that he is a fake person.

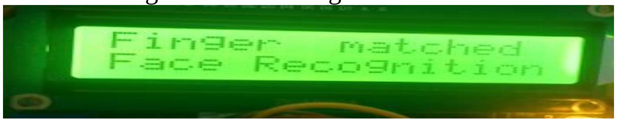
VI. RESULTS AND DISCUSSION

To create database:
To enroll person's database, initially we will take his/her finger print and face images.



Keep ur finger
press switch 1

Finger print recognition:
To take the finger print the LCD will display to keep the finger and press switch 2 and if it matches LCD will display as finger matched and go with face recognition.



Finger matched
Face Recognition

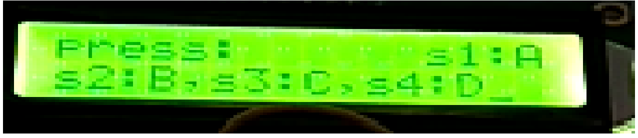
Face recognition:
To take the face images the LCD will display that face is

matched and the person is allowed to vote.

Voting phase:
Any one of the four switches will be pressed and LCD will display that the vote is accepted.

vote accepted

Counting phase:
The Authorized person will count the votes by using his finger print and results will be displayed.



Press: s1:A
s2:B,s3:C,s4:D_

The prototype design is as shown in figure 5

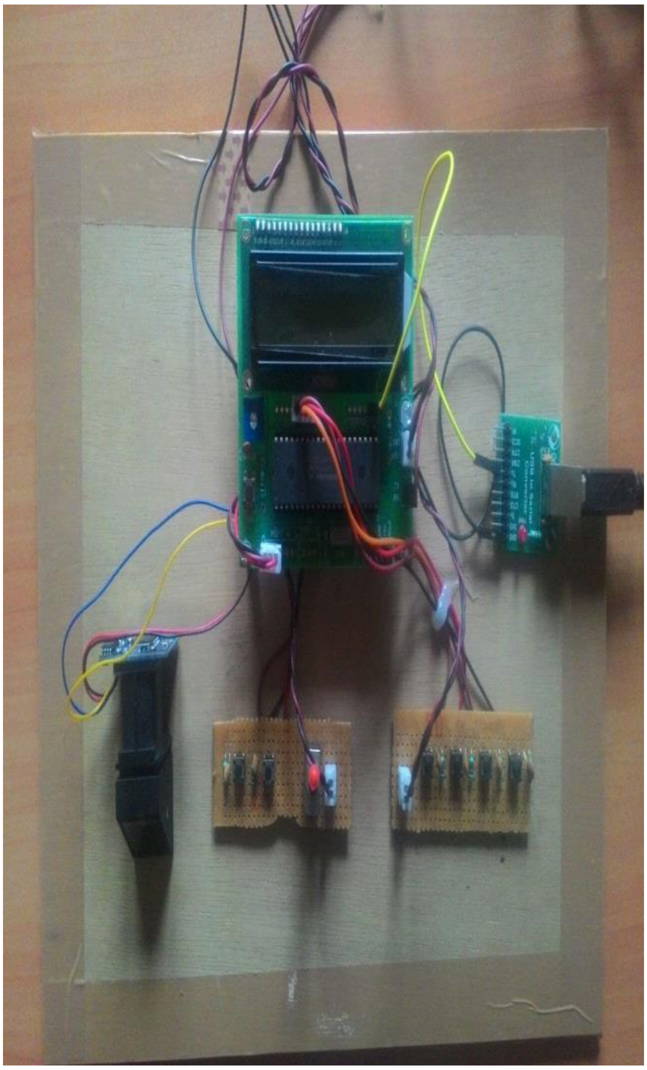
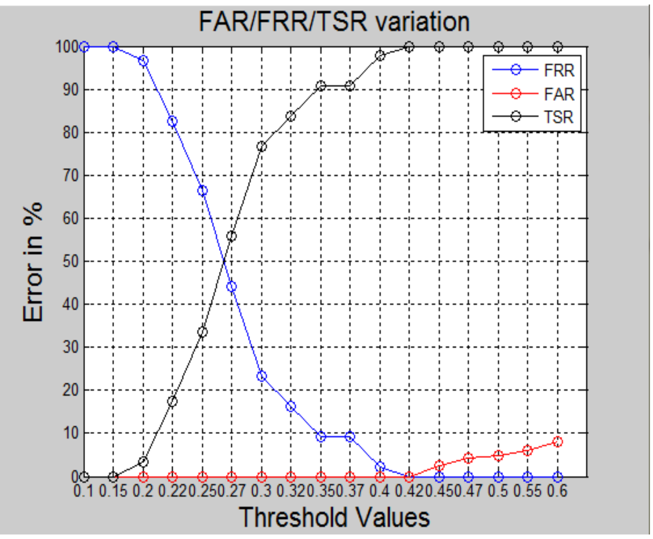


Figure 5 prototype design

False acceptance ratio is very less and false rejection ratio is very high. So, the system is time efficient.



VII. CONCLUSION

In the proposed work, the number of person’s faces and finger print are considered for performance analysis. Face features are extracted from hog algorithm. Finger print is taken from R303a finger print sensor. The fusion of face and finger print recognition is done. The recognized person is allowed for voting. Voting module is implanted using microcontroller PIC18F458.The results show proposed method provides highly secured voting technique.

VIII. FUTURE SCOPE

In the proposed voting prototype model, less number of finger prints can be stored in the finger print module which can be increased. This electronic voting machine can be interfaced with the machines at different places for the state elections so that votes can be counted easily. Time stamp can be provided so that no malpracticing takes place and provide more
security.

REFERENCES

[1]J. Deepika, S.Kalaisevi, S.Mahalakshmi,S.Agnes Shifani “Smart electronic voting system based on biometrie identification survey*” IEEE third international conference on science technology engineering & management (ICONSTEM)* 2017,pp939-949

[2]Vidyasree .P.dr. s.Viswananda Raju and Dr.G.Madhavi “Desisting the fraud in India”s voting process through multi modal biometrics”,*IEEE 6th international conference on advanced computed* pp.488-491,2016

[3]Dr.S.Ravi, Dattatreya P.Mankame “Multimodal Biometric Approach Using Fingerprint,Face and enhanced Iris features Recognition”*International Conference on Circuits,power and Computing Technologies 2013pp1143-1150*

[4] M. Satiyam.R Nagrajan “Recognition of facial expression using Haar-like feature extraction method*” IEEE International conference on intelligent and advanced syatems* 2010 pp1-4

[5]Kamal Nasrollahi, Thomas B. Moeslund “Haar-like features for robust real time face recognition” *IEEE International conference on image processing2013*pp3073-3077

[6]Rupali L.Telgad, P. D. Deshmukh, Lmas M.N.Siddiqui”Combination approach toscore level fusion for multimodal Biometricsystem by using

face and finger print" *International Conference on Recent Advances andinnovations in Engineering(ICRAIE) 2014,pp1-6*

[7]J. Kulandai Josephine Juliana, T.Sree Sharmila "Facial recognition using Histogram of Gradients and support vector machines" *International Conference on Computer, Communication and Signal Processing(ICCCSP)2017* pp1-5

[8]Zheng Xiang, Hengliang Tan,Wengliang Ye" the excellent properties of pa dense grid based HOG feature on face recognition compared to Gabor and LBP" *IEEE early* access 2018,pp1-1

[9] M.Faheem Rana, Ayesha Altaf, Syed Zagham Naseem"Enhanced real time system of evoting using Finger print" *IEEE International conference on Electronics, Computer and Computation(ICECCO) 2013,*pp297-300

[10] M.Slavkovic, B.Reljin,A. Gavrovska, M.Milivojevic"Face Recognition using Gabor filters,PCA and neural networks*" IEEE 20th International conference on systems,signals and image processing(IWSSIP) 2013,* pp35-38

[11] Jiang Li –Li, Liang Kun,Ye Shuang"Face Recognition based on support vector machine"*IEEE Fifth International symposium on computational Intelligence and design2012* pp115-119

[12] Sanjay Thakre, Ambikesh Kumar Gupta, Shilpi Sharma"Secure Reliable Multimodel Biometric Fingerprint and Face Recognition" *International Conference on Computer Communication and Informatics(ICCCI) 2017* pp1-4