Implementation of Biometric Based Electoral Fraud Desisting System

Y.Sangamitra[1], M.Hemalatha[2], A.Indhuja[3], R.Irfana Fathima[4] and S.Kalaiyarasi[5]

[1]Assistant Professor, Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, India. Email: vcewec@gmail.com
[2]UG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, India. Email: aparna03madhu@gmail.com
[3]UG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, India. Email: indhujaarumugam@gmail.com
[4]UG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, India. Email: irfanairupu@gmail.com
[5]UG Scholar, Department of ECE, Vivekanandha College of Engineering for Women, Tiruchengode, India. Email: kalaiyarasiece8@gmail.com

ABSTRACT

India is one of the countries which has the electronic voting machine for parliamentary and assembly polls. But in every poll election commission is facing so much of troubles and various types of issues through the election. The most familiar issue which is faced by the election commission is, no proper acknowledgement regarding the confirmation of casting the votes, duplication or illegal casting of votes. In this project all these issues has been handled and overcome with the perfect solution. The main advantage of this project is handling of data by using biometric system such as finger print and face recognition (is done by masking technique). This is used to ensure the security to avoid fake and repeating voting. It also enhances the accuracy and speed of the process. The system performs with perfect recognition on a face and thumb impression of all the eligible voters in a constituency, which is done as pre-polled procedure. During election, thumb impression and face templates of voters is given as an input to the system. This is then compared with the already stored database and available records. If the particular pattern matches with the record then the voters are allowed to vote but incase if it doesn't match or in case of repetition, voters vote are denied or gets rejected. The result is instant and counting is done.

Keywords: Fingerprint module, PC, Face recognition and Masking technique.

1. INTRODUCTION

The pillar of Democracy country is its election system. The election process provides the rights to every citizen of a country to select a legitimate representative among themselves who can guide democratic system towards the welfare of the society. For the past few decades the voting system has observed many effective changes. By a step by step process voting system is improving. This project is designed for electronic voting machine by using the recognition of finger print and face template. Here the voters thumb impression and face templates are used for identification. During the voting the voters need to places their thumb and face for scanning, this system will check whether it matches with the pre-stored data in the database. If it matches, then the system will allow the voter to poll their vote otherwise it prevents the voter from polling.

2. PROPOSED SYSTEM

In our proposed system, we are going to create a database for all eligible voters with their biometric identifications. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. One touch data training is available, so that user can show their face and finger print once for proper detection. It can detect all the face in long-distance, also it can use many fingers. Multiple face detection functionalities are implemented here; all the faces will be detected under masking techniques. So face will be marked in a rectangle box for identity verification. After the verification user will get an acknowledgement message. All face and finger print data will be stored as a reference file in the data base, this method provides more security.
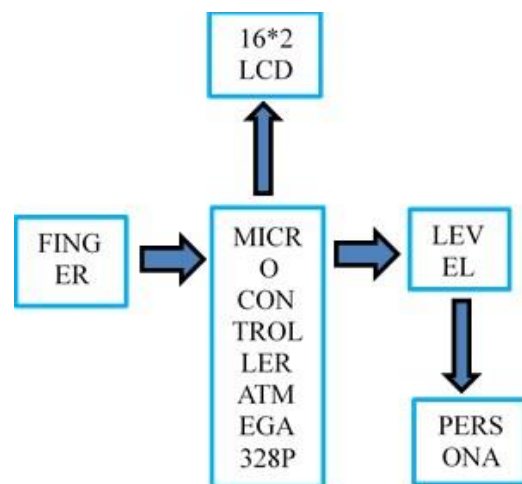
3. METHODOLOGY

Fig.1. Block Diagram

4. WORKING

The system mainly consists of four phases; Image acquisition, Face Detection, Feature Extraction, Face Recognition. The working of the system is depicted as follows:

1. User Creation.
2. Recognition and verification.
3. COMM Port communication.
4. Centralizing the data.
5. Face and finger Detection.

1. User Creation

This is the initial module of this project, here the admin is involved, for the data updating. The admin role is to create the user details with the camera interface. The basic details of the customer are the input data in the module, so that the admin will get the details of the voters name, personal details and etc. The voters face and finger print will be added while creating the account. This system will works according to the system timings.

2. Recognition and verification

Recognition of biometric systems like facial recognition, finger print or iris recognition, relating to their fundamental function. The generic term however does not necessarily imply verification of closed-set identification or open-set identification. Verification is the task where the biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. The concept of recognition and verification which is further illustrated by the picture below where the first image resembles the second image.

3. COMM port Communication

The Commercial input port of the computer, is useful in providing various data inputs and interactions. In computing, a COMM port is a serial communication physical interface through which information transfers in or out one bit at a time (in contrast to a parallel port). The term "COMM Port" usually identifies hardware more or less compliant to the RS-232 standard, intended to interface with a modem or with a similar communication device. Modern computers without COMM ports may require COMM-to-USB converters to allow compatibility with RS 232 serial devices. COMM ports are still used in applications such as industrial automation systems, scientific instruments, shop till systems and some industrial and consumer products. Server computers may use a COMM port as a control console for diagnostics. Network equipment (such as routers and switches) often use serial console for configuration. COMM ports are still used in these areas as they are simple, cheap and their console functions are highly standardized and widespread. A COMM port requires very little supporting software from the host system.

4. Centralizing the data

This is the most important module of the project; because the updating details will be stored in the centralized server and the sub servers. A prior admin will be allocated to access these details. They will be permitted to update the details too. All the centralized details will be available in the server so that user or admin can able to access the server anywhere at any time. There will be more security provided to the centralized server and high bandwidth will be allocated to access more number of users at a same time.

5. Fingerprint and face Detection

A. Finger print: The system consists of a finger print reader that captures the impressions of the voter and sends it to the image pre-processing. It creates an ID and goes for face detection.

B. Face Detection: This process separates the facial area from the rest of the background image (i.e., the length of eyes, nose and lip are measured). The faces and the finger templates are stored in the database.

C. Feature Extraction: Feature extraction is done for distinguishing faces of different student. In this system, eyes, nose and mouth are extracted along with the finger templates. Feature extraction is helpful in face and fingerprint detection and recognition.

D. Face and Finger Recognition: The face image and the fingerprint templates are then compared with the stored image. If the face image and finger print are matched with the stored database then the voters are allowed to poll the vote for their desired party. The counting is instant and time conscious for polling and counting.
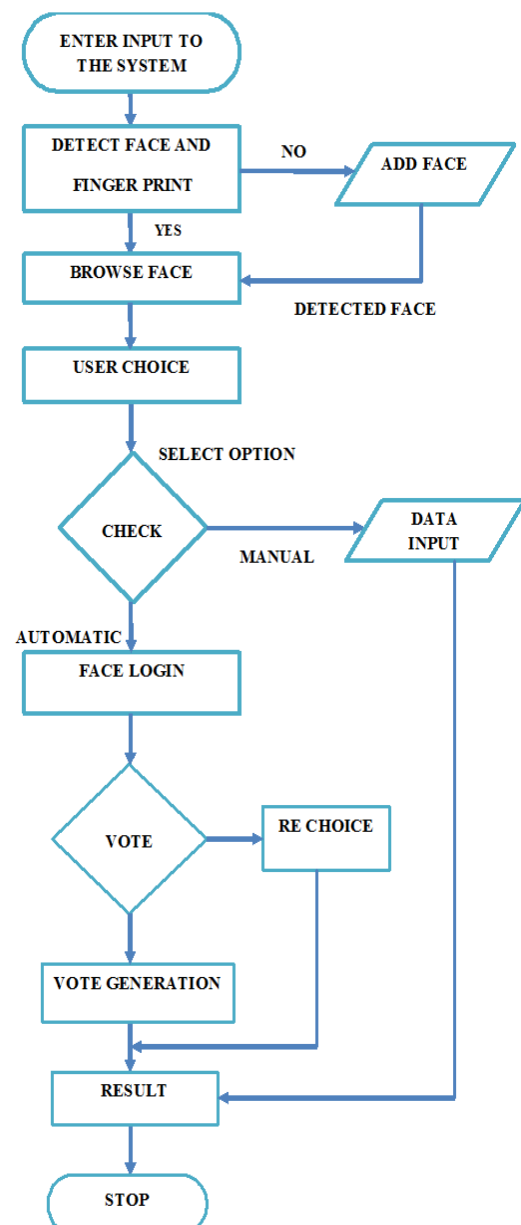
5. FLOWCHART

Fig 2. Flowchart for Face Recognition Technology

6. CONCLUSION

The current developed project is found to be working accurately. It is tested for its effectiveness, flexibility, accuracy and user friendly. The system is found to be running under the single window system. The programming techniques used in the design of the system provides a scope for further expansion and implementation of any changes which may occur in future. The system has been tested with all sample data covering all possible options for each function. Its performance is satisfactory and the system is successfully implemented.

7. FUTURE SCOPE

The system has been designed and developed according to the current requirement. At the same time the system is very flexible and extensible. Hence, future enhancement can be made without much difficulty. Thus new applications can be developed and it can be integrated with the existing one very easily. The following future enhancements may be worthwhile to make the tool usable to a wider section of users. It could be interfaced with the printer to get the hard copy of the result. Once the result is on the server it could be relayed on the network to various office of the election conducting authority. Memory of the fingerprint module can be expanded. Audio output can be introduced to make it user friendly for illiterate voters. We can use Iris technology for higher resolution.

ACKNOWLEDGEMENT

REFERENCES

[1] Patil Ragul H., Tarte Babita B., Wadekar Sapana S., Zurunge Bhakti S., "A Secure E-voting System Using Face Recognition And Dactylogram", *International Engineering Research Journal (IERJ)*-April 2016.

[2] Sudhakar.M,Divya Soundarya Sai, "Biometric System Based Electronic Voting Machine using ARM9 Microcontroller", *IOSR Journal of Electronics and communication engineering(IOSR-JECE)*-Feb 2015.

[3] Avier Galbally, Sebastian Marcel and Julian Fierrez, "Image Quality Assessment for Fake Biometric Detection: application to Iris, Fingerprint and Face Recognition" -2014.

[4] Sanjay Kumar, Manpreet Singh, "Design a Secure Electronic Voting System Using Finger Print Technique"-2013.

[5] Nikita Sharma, D.S.Singh, "A Survey on Various Features Extraction Techniques for Face Recognition", *IJCA*-2012.

[6] S.Kumar and E.Walia, "Analysis of Electronic Voting System in Various Countries", I*nternational Journal on Computer Science and Engineering*-2011.

[7] Tadayoshi Kohno, Adam Stubblefield, Aveil D.Rubin and Dan S.Wallach, "Analysis of an Electronic Voting System"-2004.

[8] Alaguvel.R, Gnanavel.G, "Offline and Online E-voting System with Embedded Security for Real Time Application", *International Journal of Engineering Research.*