Electronic Voting Machine with fingerprint and facial recognition

Bharath G*
bharathganesh2001@gmail.com

Kalaiarasan M K*
kalaiarasanmayakesavan@gmail.com

Mubarak Ali S Y*
Mubarakmsd114@gmail.com

Ajay R*
Ajayr10052001@gmail.com

*** Department of Electronics and Communication Engineering**

*** AVS Engineering College, Salam, Tamil Nadu**

Abstract: In this project, an attempt has been made to the development of an authenticated electronic voting system using fingerprint and facial images. The two-fold authentication system improves the security of the voting process and reduces the chances of a corrupt election process. The facial recognition process utilizes the Local Binary Pattern Histogram and Support Vector Machine process to scan, store and recognize faces efficiently. The fingerprint recognition involves the capturing of multiple 2D images and High Sensitive Pixel Amplifier to improve the quality of those images to scan the fingerprint to provide the primary form of authentication. Visual Basic is used to develop a very easy to use User Interface that enables an easy voting process. A private server is used to store both the user data and the election results separately. This reduces the chances of external manipulation of the election results.

Key Words: Fingerprint, Voting machine, Facial recognition, ESP 32, Capacitive touch.

1. INTRODUCTION

The simple and cold truth is that everyone hates the problems and security flaws that are glaring at everyone's face. They are so apparent to ignore, as many witnesses these flaws straight on. Some of these flaws can be easily corrected and that is the main objective of this project, to rectify the flaws that can be rectified.

To list some of these so-called flaws, are a polling of proxy votes, polling of illegal votes, polling of votes under a stolen identity, external manipulation of the voting process pre and postelection, improper counting of votes. Electronic voting is both electronically casting a vote and an electronic means of counting votes. In our project, we are giving importance to the authentication process of our designed voting machine. The securities that are provided will totally eliminate the fraud in the voting system. As a total number of fraudulent votes that are cast are considerably reduced, the probability of obtaining a stable and working government is increased manifold. Also due to this, there is very minimal possibility of manipulation by external forces pre and post-election. When these elements are considered together, a nearly working voting system can be developed. Upon the elimination of these flaws, we can safely entail a safe and secure voting process, which results in the establishment of a stable and working government. The main objectives that are encompassed within this project are listed as, Fingerprint Confirmation as the Primary form of Verification, facial Recognition as the Secondary and Final form of Verification, two memory implementation for the prevention of manipulation, easy to use and an inviting UI for the better understanding of the voting process.

2. LITERATURE SURVAY:

1.Hanady Hussien, Hussien Aboelnaga, IEEE 2013. “Design of secured E-voting systems.” is able to desire with the widespread use of computers and embedded systems. Security is the essential problem should be considered in such systems. This paper proposes a new e-voting system that fulfils the security requirements of e-voting. It is based on homomorphic property and blind signature plan. The suggest system is executed on an embedded system which serves as a voting machine. The system employees RFID to store all conditions that comply with the rule of the government to check voter eligibility.

2.Daniel petcu, Dan Alexandru stoichescu, The International Symposium on Advanced topics in electrical engineering; May 7-9, 2015. “A Hybrid mobile Biometric- based E- voting system.” Information technology changes and gives shape to networked society all over the world today & its solutions are becoming main drivers in almost all field of human life activity.

3.M.Venkata Rao, Venugopal Rao Ravula, Pavani Pala. “Development Of Antirigging Voting System Using Biometrics Based On Adharcard Numbering”. Now a day’s voting process is exercised by using EVM (Electronic voting machine). In this paper we present and use implementation is to execute the progress of anti rigging voting system using finger print .The purpose of the project and implementation is to provide a safety and good environment to the customers is to electing the candidates by using the intelligent electronic voting machine by providing a rival naming to every user using the FINGER PRINT identification technology. Herein this project and satisfy we are going supply the at most security since it is taking the FINGER PRINTS as the authentication for EVM.

3. EXISTING SYSTEM

Electronic Voting Machines ("EVM"), Idea mooted by the Chief Election Commissioner in 1977. The EVMs were devised and designed by Election Commission of India in collaboration with Bharat Electronics Limited (BEL), Bangalore and Electronics Corporation of India Limited (ECIL), Hyderabad. The EVMs are now manufactured by the above two undertakings. An EVM consists of two units, i) Control Unit, ii) Balloting Unit. The two units are joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment.

There are two types of problems with EVM which is currently in use:

1. Security Problems - One can change the program installed in the EVM and tamper the results after the polling. By replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favor of a chosen candidate. These instructions can be sent wirelessly from a mobile phone.
2. Illegal Voting (Rigging) - The very commonly known problem, Rigging which is faced in every electoral procedure. One candidate casts the votes of all the members or few amounts of members in the electoral list illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.

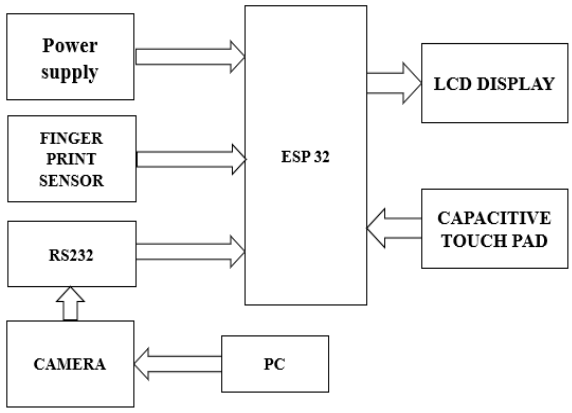
This project will eliminate these above mentioned problems.

4. PROPOSED SYSTEM

The various technologies used are selected such that they are compatible with one other and have no interfacing problems. Also, they must fall within the budget limit such that compromises shall not be made. The different technologies and tools used are listed below Python Development Environment, Linux Interfacing Engine and, Visual Basic. The PDE is used to develop the working program for the verification devices and the LIE is used to convert it to Linux compatible code. Here, a development environment is a combination of a text editor and the Python interpreter. The text editor allows you to write the code. The interpreter provides a way to execute the code you've written. A text editor can be as simple as Notepad on Windows or more complicated as a complete integrated development environment (IDE) such as PyCharm which runs on any major operating system. An application programming interface (API) is a set of specifications that define how one piece of software interacts with another, particularly an application program with an operating system. A primary purpose is to provide a set of commonly-used functions, such as to draw windows or icons on the screen, thereby saving programmers from the tedium of having to write code for everything from scratch. The PDE is used to develop the working program for the verification devices and the LIE is used to convert it to Linux compatible code. The capacitive fingerprint sensing is the type of fingerprint sensor used in the project. Instead of creating a traditional image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint.

The facial recognition uses Local Binary Pattern Histogram and Support Vector Machine algorithms for its functioning. Finally visual basic is used to develop the user friendly user interface of the project.

BLOCK DIAGRAM



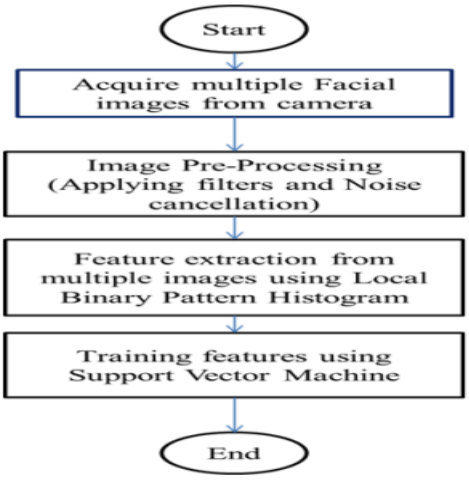
METHODOLOGY

The order of execution of the project requirements is done so as to achieve an optimal solution within the shortest possible timeframe. The overall workflow is such that the most difficult to execute is done first and foremost, and the easiest is done at the last. This is so that, enough time is available for the testing process and some additional time, in the case of sudden, unprecedented emergencies [1]. The overall workflow can be classified into two phases; they are the Development Phase and the Testing Phase. In the development phase, the design of the circuit, purchasing of the components, developing the security detail, final integration of all the details into one and fabrication of components to make the final product look appealing is completed. Secondly, the testing phase involves the testing of the final, finished product for the various contingencies and areas of problems. When these tests are carried out, faults and defects are found out and they are rightly corrected.

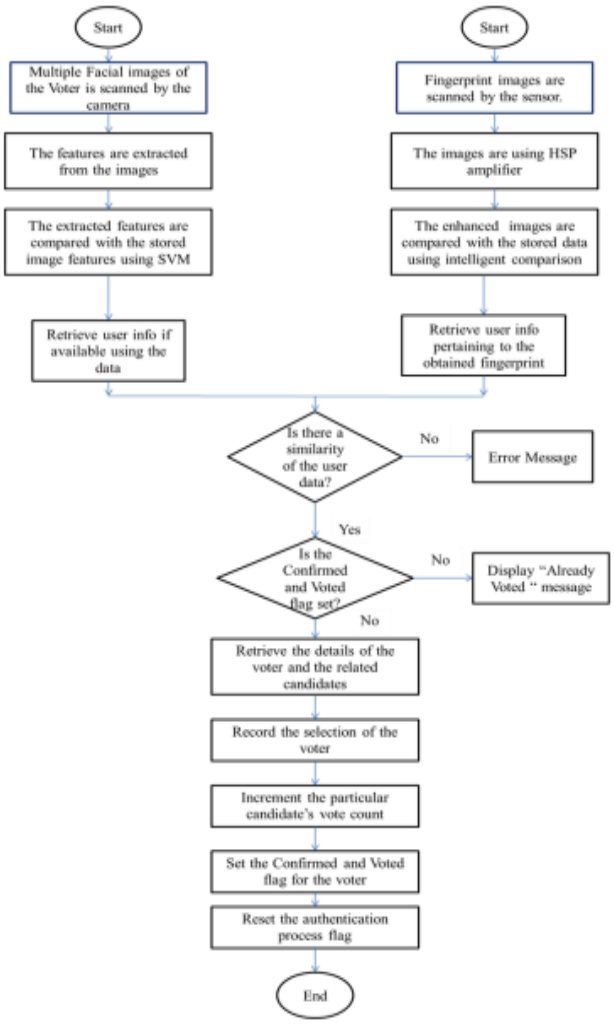
FLOW CHART

The overall flow of the project can be illustrated and understood from the below flowchart.

ACQUISITION



AUTHENTICATION



5. CONCLUSION

The working of this model is very straightforward and very easy to understand. First, the fingerprint reader scans the fingerprint of the voter and sends the output to the microcontroller. The microcontroller then pairs the scanned data with the data in the database and retrieves the information about the voter. Now, the camera scans the face of the voter and checks whether it is similar to the face of the voter's face data that is paired with the fingerprint.

There are many fraudulent and illegal activities that are happening in regards to the current voting process. With these problems in mind, the electronic voting machine is developed with fingerprint and facial recognition. This dual authentication system reduces the chances of the above mentioned problems and so it has improves the security and efficiency of the voting process.

REFERENCES

[1] Phillips, P., Grother, P., Micheals, R.J., Blackburn, D.M., Tabassi, E., Bone, J.M.: Face recognition vendor test 2002 results. Technical report (2003).

[2] Zhao, W., Chellappa, R., Rosenfeld, A., Phillips, P.J.: Face recognition: a literature survey. Technical Report CAR-TR-948, Center for Automation Research, University of Maryland (2002) Phillips, P.J., Wechsler, H., Huang, J., Rauss, P.: The FERET database and evaluation procedure for face recognition algorithms. Image and Vision Computing 16, 295–306 (1998).

[3] Turk, M., Pentland, A.: Eigenfaces for recognition. Journal of Cognitive Neuroscience 3, 71–86 (1991).

[4] Etemad, K., Chellappa, R.: Discriminant analysis for recognition of human face images. Journal of the Optical Society of America 14, 1724–1733 (1997).

[5] Moghaddam, B., Nastar, C., Pentland, A.: A bayesian similarity measure for direct image matching. In: 13th International Conference on Pattern Recognition, pp. II: 350–358 (1996).