International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 6 ǁ 2022 ǁ PP. 932-936

Electronic Voting Machine with Fingerprint and Facial Recognition

Kanagaraj G 1st, Ajay R 2nd, Bharath G 3rd, Kalaiarasan MK 4th, Mubarak Ali SY 5th
1st Head of the Department, 2nd, 3rd, 4th, 5th UG Scholar (B.E), Department Electronics and Communications Engineering, AVS Engineering College, Salem.

Abstract: *This project main objective is to attempt to make developed and more secured electronic voting machine using fingerprint and facial recognition technology. The double authentication system provides security of the voting process and almost eliminate the chances of a corruption and manipulation in election process. The facial recognition process uses the Local Binary Pattern Histogram and Support Vector Machine process to scan, store and recognize faces effectively. The fingerprint recognition has capturing of multiple 2D images technology and Highly Sensitive Pixel Amplifier to provide better quality of the images to scan the fingerprint. Visual Basic is used for easy voting process. A secured server is used for storing both user data and the election voting results. This minimize the chances of external manipulation of the election process.*

Key Words: *Fingerprint, Voting machine, Facial recognition, Arduino UNO, Capacitive touch.*

Date of Submission: 02-06-2022 Date of acceptance: 14-06-2022

I. INTRODUCTION

Biometrics is the method of measuring and analyse the biological data using science and technology. In IT field, biometrics refers to technologies that used to measure and analyse the human body structures, such as DNA, eye retinas, voice data, facial data and leg & hand measurements, for authentication purposes. In this project we have used finger impression for the purpose of voter identification and authentication. The finger impression of every individual is different and unique, it helps in improving the accuracy and provide security. A database is created which contains the facial data of all the voters. Illegal votes, repetition of votes and manipulation of votes are checked in this system. Hence if this system is implemented the voting would be fair and free from corruption of votes. This system also provides simplicity of the voting process and require fewer human resources also provide security.

1.1.1 Facial Recognition

Facial recognition is the method of identifying or finding an individual's face data using their image of their face. This system can be used to find people in photos, videos, or in real time web cameras. It is a category of biometric security which uses face structure. Some other biometric authentication software includes speech recognition, fingerprint recognition and iris recognition. This technology is mostly used for high security applications, even though the use of this system is wider.

1.1.2 Working of Facial Recognition

Facial recognition technology working is based on four important parameters which is fall under the software. The parameters which act as key to the facial recognition as follows:

i. Face detection
ii. Face analysis
iii. Converting the image to data
iv. Finding a match

II. LITERATURE SURVEY

Hanady Hussien, Hussien Aboelnaga, entitled "Design of secured E-voting systems"
This project is able to desire with the innovation and use of computers and embedded systems which makes work easier for the humans. Security is the crucial problem which should be considered as important factor in such systems. This project proposes a advanced electronic-voting system that has the security requirements of e-voting. This electronic voting machine is based on homomorphic property and blind signature plan. It is

implemented by using embedded system which act as a voting machine. The RFID module is used to store all instructions that given with the moral of the government to check user eligibility in this system.

Daniel petcu, Dan Alexandru stoichescu entitled "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 so he proposed a system which has combination of voter identification and fingerprint authentication to provide and enhance security in the election.

M.Venkata Rao, Venugopal Rao Ravula, Pavani Pala entitled "Development of Antirigging Voting System Using Biometrics Based on Aadhar card Numbering"

Now a day's voting process is mainly based on and exercised by using EVM (Electronic voting machine). In this project implementation and execution, the progress of anti corruption voting system using finger print. The objective of this project and implementation is to include a secured and good environment to the voters is to electing the candidates by using the FINGER PRINT identification technology. Here in this project we are going supply the at most security because it is using the FINGERPRINTS as the authentication for EVM.

III. EXISTING SYSTEM

Electronic Voting Machines (EVM), which idea are motivated by the Chief Election Commissioner in 1977. The EVMs in India were initially 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 present day EVMs are now manufactured by the above two undertakings. EVM has two main units, one is Control Unit and the other one is Balloting Unit. These two units are connected or else joined by a five-meter cable. The Control Unit is with a Polling Officer and the Balloting Unit is placed inside the voting compartment and both are combined working as whole voting machine.

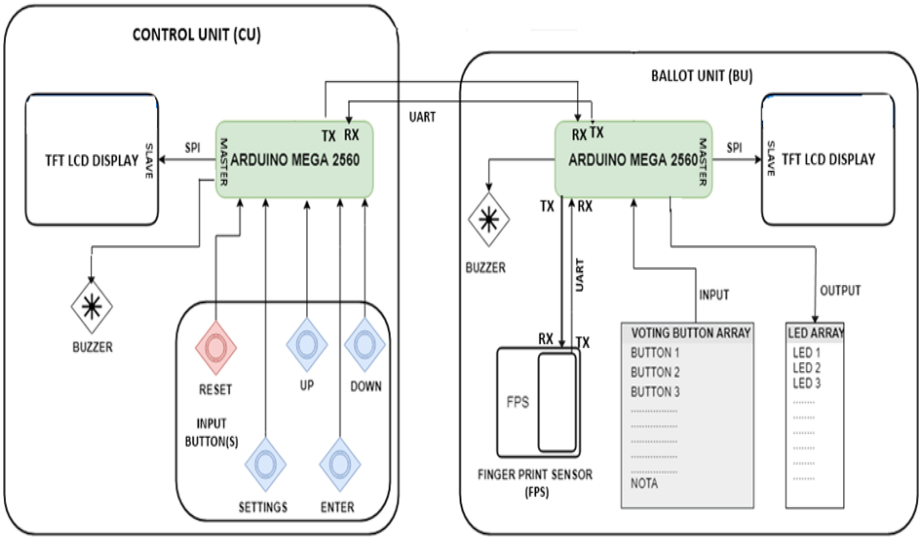

Fig 3.1.1 Flow Diagram of Existing Method

3.2 Two types of main problems with EVM which used in present day are:

1. Security Problems - One can change the program installed in the EVM and tamper the results after the polling. By changing a small part of the machine with a similar component that can be stealthily instructed to steal a percentage of the votes in favor of a desired candidate. These instructions are operated by the malicious person who can be sent wirelessly from a mobile phone.

2. Illegal Voting (Rigging) - The very commonly known problem, Manipulation which is faced in every electoral procedure. One candidate casts the votes of all other people or members or few amounts of members in the electoral list illegally without identified. It results in the loss of votes for the other opposing candidates who are participating and also increases the number votes to the candidate who performs this action. This process was done externally at the time of voting.

IV. PROPOSED SYSTEM

This project includes various advanced technologies used such as that used technologies are compatible with one other and have no interfering problems with each other. And also, they must fall under the budget limit so it can be implemented throughout the country without any problem. The different technologies and tools which are used in this project are listed below Python Development Environment Software (PDE), Linux Interfacing Engine (LIE) and, Visual Basics. The PDE is used for developing the working program for the authentication devices and the LIE is used for converting it to Linux compatible code for execution. Here, the python development environment is a combination of a text editor or notepad and with the Python interpreter. The text editor or the notepad allows user to write the code.

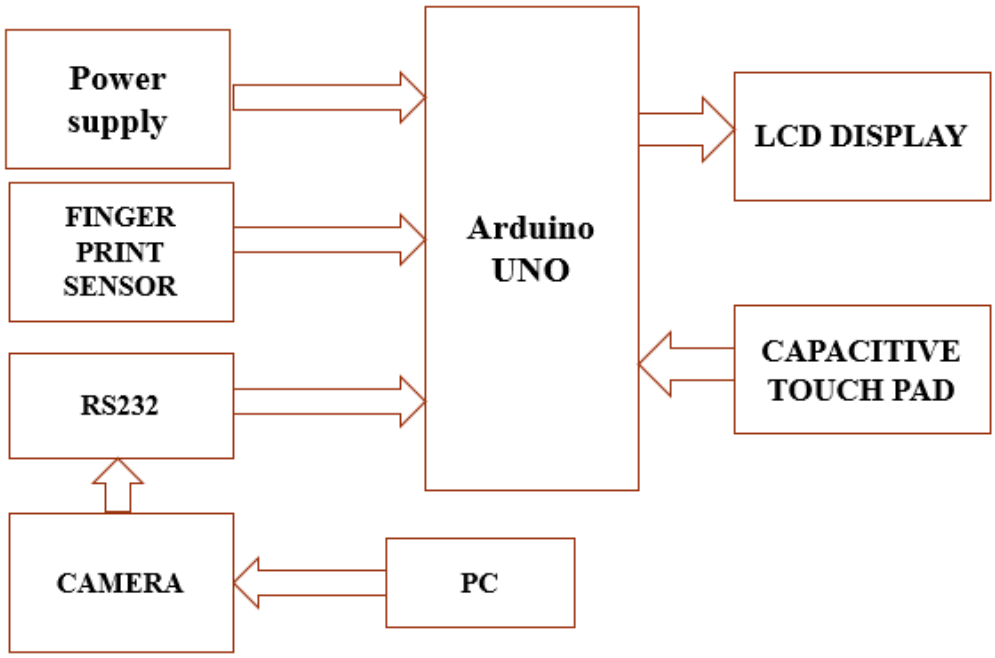

Fig 4.1.1 Flow Diagram of Proposed Method

The interpreter gives a way to execute and run the code which the user written. A text editor can be as simple as the inbuilt or installed third party Notepad on Windows or more advanced and complicated as integrated development environment (IDE) such as PyCharm and Eclipse and so on, which runs on any most of the operating system. An application programming interface (API) is a set of codes that specifies how one piece of code or software interacts with another, specifically an application program with an operating system like Windows, Linux and so on. A main purpose is to give a set of generally-used functions, like to draw windows or icons on the screen. The PDE is used in this project to develop the working of the program for the authentication devices. The capacitive fingerprint sensing feature is one type of fingerprint sensor used in this project which can store 2D image of the fingerprint. Instead of creating a traditional or normally used image of a fingerprint, capacitive fingerprint scanners use arrays of tiny or small capacitor circuits to collect data about the fingerprint of the candidate or voter. As all the capacitors can store electrical charge, joining them up to conductive plates on the surface of the scanner allows them to be used to track more details of a fingerprint rather than traditional method. The facial recognition uses Local Binary Pattern Histogram and Support Vector Machine algorithms as base for its highly secured functioning.

4.2 Fingerprint Recognition

Fingerprint recognition is one of the traditional and most used authentication technology in researched fields of biometrics.

Biological principles related to fingerprint recognition to work as follows:

- Epidermal ridges and furrows of different people have different characteristics for different fingerprints, this creates the foundation for fingerprint recognition.
- Types of the configurations are individually different, but thee variations are within limits that allow for systematic classification and identification.
- Details and configurations of furrows and ridges are permanent and unchanging.

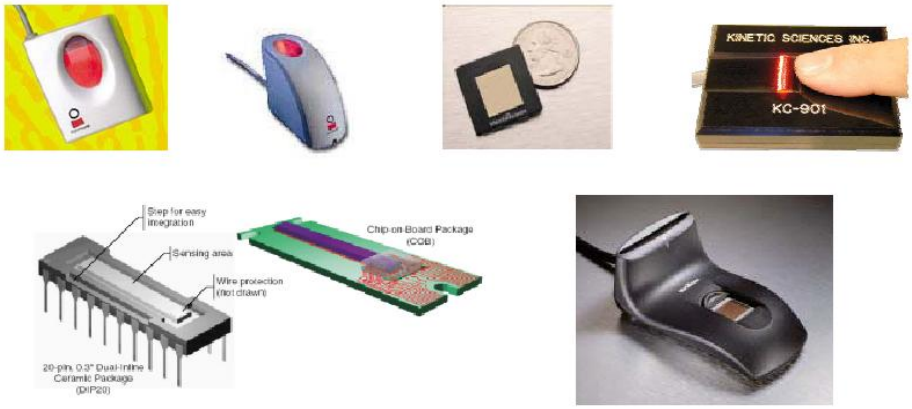

Fig 4.2.1 Fingerprint Sensors

4.3 Facial Recognition

The human brain has millions of numerous highly interconnected neurons which used for some specific tasks, can outperform any supercomputers in this world. A child can accurately identify a face without an ease, but for a computer, it is a very cumbersome task. Therefore, the main idea of face recognition is to engineer a system that can emulate what a child can do in this case recognition of faces. Early used face recognition algorithms used simple geometric models, but recently these recognition process has now matured into mathematical representations and matching processes which is more accurate than early facial recognition technology. This system can be used to find people in photos, videos, or in real time web cameras. It is a category of biometric security which uses face structure. Some other biometric authentication software includes speech recognition, fingerprint recognition and iris recognition. This technology is mostly used for high security applications, even though the use of this system is wider.

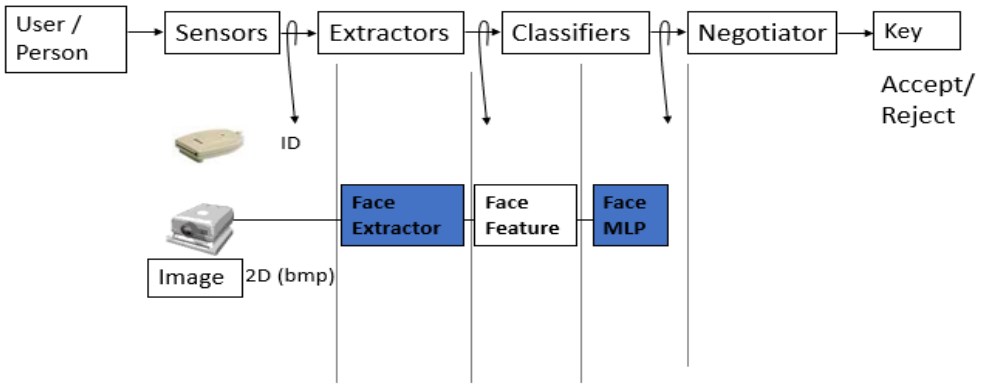

Fig 4.2.1 Facial Recognition Block Diagram

V. CONCLUSION

The working of this model is very easy to understand for all the people. The fingerprint scanner scans and then stores the fingerprint data of the voter and after that sends the output to the microcontroller for authentication or verification. The microcontroller then pairs the scanned data with the data in the database and retrieves the information about the voter. The camera scans the face of the voter and checks whether it is same or similar to the face of the voter's face data that is paired with the fingerprint in the database. There are many manipulation and illegal activities that are happening in regards to the present voting process or system. With these problems in mind, the electronic voting machine is developed with two-fold authentication of fingerprint and facial recognition. This dual authentication system reduces the chances of the above mention problems and so it can improve 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).