

AUTOMATIC PLATE DISPENSER USING ARDUINO

Brindha.G, Girija.V, Gowri.M, Gowtham.S, Dr.K.Geetha

Department of Electronics and Communication Engineering

Rathinam Technical Campus, Coimbatore

Abstract— Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. In this paper we have used thumb impression for the purpose of voter identification or authentication. As the thumb impression of every individual is unique, it helps in maximizing the accuracy. A database is created containing the thumb impressions of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is employed the elections would be fair and free from rigging. Thanks to this system that conducting elections would no longer be a tedious and expensive job.

Keywords: *EVM electronic voting machine . EPIC Election photo identity card MEMS micro-electro-mechanical systems, AFIS - automatic fingerprint identification, UIDAI - unique identification authority of india*

I. INTRODUCTION

Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. In this paper we have used thumb impression for the purpose of voter identification. As the thumb impression of every individual is unique, it helps in maximizing the accuracy. A database is created containing the thumb impressions of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is employed the elections would be fair and free from rigging. Thanks to this system that conducting elections would no longer be a tedious and expensive.

II. FINGERPRINT SENSOR:

Finger print devices for voting machines and different existing identity documents are mentioned and enforced during this project. The user should show his voter ID card whenever he goes to the booth to poll his vote.

This is often a time consuming method because the person needs to check the voter ID card with the list he has, make sure it as an authorized card and then enable the person to poll his vote. Thus, to avoid this type of issues, designed a finger print based voting machine wherever the individuals no ought to carry his ID which contains his entire details. The person at the booth should show his Finger. This Finger print reader reads the details from the tag. This information is passed to the controlling unit for the verification. The controller reads DATA from the reader and compares this data with the already existing data. If the data matches with the already stored information is allowed to poll his vote. Person LCD is allowed to poll his vote. If not, a message is displayed on LCD.

The polling mechanism carries out manually using the switches. the and therefore the person employed to display the related messages. An appropriate security level is always a compromise between usability and strength of security method.

The secured e-voting process can be done by linking the voting machines with the Aadhar an Indian citizen identification data base with a unique identification number for every citizen. The Aadhar based EVM can result in secured e-voting process. As a result of no two or more voter's data can match as this system uses biometrics. Illegal votes and repetition of votes is checked for in this system. Hence if this system is utilized the elections would be truthful and free from rigging.

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan.

This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, Piezo resistivity, ultrasonic, piezoelectric, MEMS. This is an overview of some of the more commonly used fingerprint sensor technologies.

III. FINGER PRINT

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the Eccrine sweat gland that are present in epidermal ridges. These are sometimes referred to as "Chanced Impressions" In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand.

A print from the sole of the foot can also leave an impression of friction ridges. Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers. Human fingerprints are detailed, presumed to be nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity.

They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster. Fingerprint analysis, in use since the early 20th century, has led to many crimes being solved. This means that many criminals consider gloves essential. In 2015, the identification of gender by use of a fingerprint test has been reported.

IV. BIOMETRIC

A friction ridge is a raised portion of the epidermis on the digits (fingers and toes), the palm of the hand or the sole of the foot, consisting of one or more connected ridge units of friction ridge skin.

These are sometimes known as "epidermal ridges" Which are caused by the underlying interface between the dermal papillae of the dermis and the inter papillary ridges of the Epidermis. These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges may also assist in gripping rough surfaces and may improve surface contact in wet conditions.

V. EXISTING SYSTEM

An EVM consists of two units namely Control Unit and 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 Ballot Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his/her vote by pressing the blue button on the Ballot Unit against the candidate and symbol of his/her choice. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer.

No one (including the manufacturer) can change the program once the controller is manufactured. EVMs can cater to a maximum of 64 contesting candidates. There is provision for only 16 candidates in a BU if the total number of candidates exceeds 16, then a second BU is to be linked parallel to the first BU. Similarly, if the total number of candidates exceeds 32, then a third BU is to be connected and if the total number of candidates exceeds 48, fourth BU is to be connected to cater to a maximum of 64 candidates. As the process is faster and more reliable, the EVMs save considerable amount of time, money, and paper and man power. Actual process of identifying the voter has to be done by the polling officer. For casting of votes with EVMs, the voters have to produce their Election Photo Identity Card (EPIC) issued by the Election Commission.

The polling officer needs to verify the EPIC with the official list he has, then he needs to confirm whether it is an authorized card or not and he allows the voters to cast their votes. Therefore EVMs depend upon manual verification of the EPIC. Consequently, this slows down the voting process. This limitation is overcome with the help of fingerprint identification module. The second limitation is the number of contesting candidates available in the EVM.

The EVMs can cater to a maximum of 64 candidates with the use of one CU and four BU. If the number of contestant candidates exceeds 64, then the polling officer needs to carry one more set of EVM that necessitates more material and additional manpower.

VI. APPLICATIONS

1. Industrial application: “Fingerprint based security system” project can be used by the employees, staff or workers in various industries like Automobile industries, manufacturing industries, Software development companies.
2. Home or domestic application: This project can be used to automate the door locking process at our home, so the user need not to carry the door lock keys along with him, he can just use his/her finger to open the door .
3. Bank Lockers or security safes: Many of the banks use key based or password based locks for their lockers or safes. We can implement Fingerprint based bank locker system using this project.

VII. PROPOSED SYSTEM

1. Power Supply (12V)
2. Microcontroller
3. Personal computer
5. Fingerprint sensor (R307)
6. Relay module
7. Solenoid valve

VIII. ARDUINO

Arduino: “arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. it's intended for artists, designers, hobbyists and anyone interested in creating interactive objects or environments1” Since Arduino is Open Source, the CAD and PCB design is freely available. Everyone can buy a pre- assembled original Arduino board2 or a cloned board from another company. You can also build an Arduino for yourself or for selling.

Although it is allowed to build and sell cloned Arduino boards, it’s not allowed to use the name Arduino and the corresponding logo. Most boards are designed around the Atmel Atmega328.



IX. SYSTEM ANALYSIS

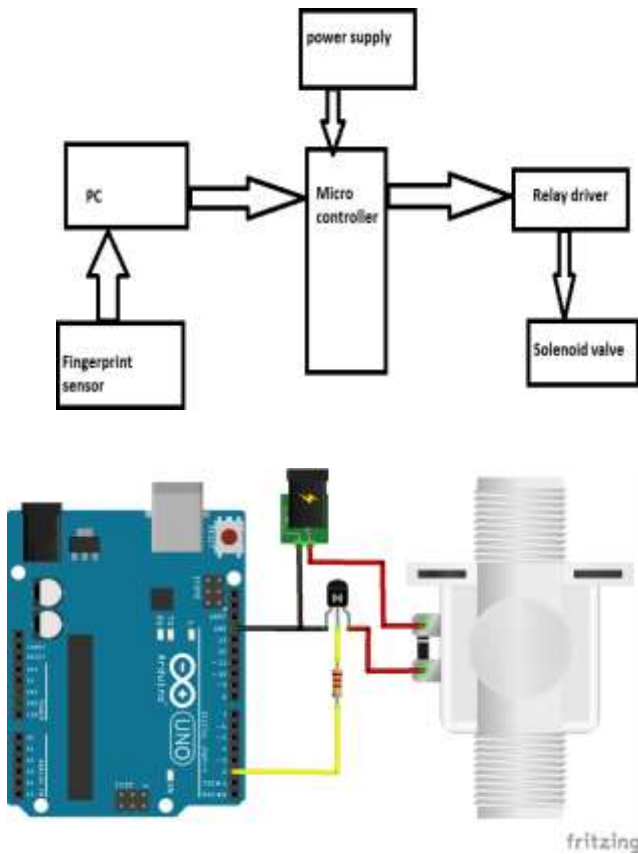
Following are the important blocks of this system:

- 1) Fingerprint sensor: We have used 4500 Finger Print Sensor. It has an Optical biometric fingerprint reader. It also has inbuilt flash memory. It performs the function of image processing and gives out data on its output pin.
- 2) Microcontroller: This is the CPU (central processing unit) of our project. We are going to use a microcontroller of PIC family. The various functions of microcontroller are like: I. Reading various digital input signals from fingerprint sensor II. Sending this data to LCD so that the person operating this project should understand the status. III. Giving the respective signal to the various output devices. Relay and DC motor for valid access and buzzer for the invalid access. IV. Sending the data to the computer using serial port. This data consist of the status of valid or invalid access.

Various keys are following,

- ✓ Add fingerprint entry.
- ✓ Search fingerprint.
- ✓ Empty the database of fingerprint module.

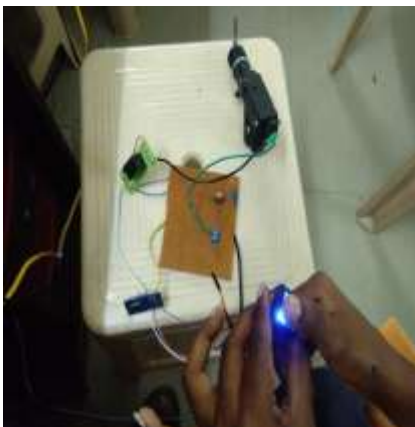
X. ARDUINO SOLENOID VALVE CONTROL CIRCUIT



```
COM4 (Arduino/Genuino Uno)

Adafruit finger detect test
Found fingerprint sensor!
Sensor contains 3 templates
Waiting for valid finger...
Found ID #3 with confidence of 55
Found ID #2 with confidence of 71
Found ID #2 with confidence of 85
Found ID #2 with confidence of 149
Found ID #3 with confidence of 109
Found ID #3 with confidence of 90
Found ID #3 with confidence of 63
Found ID #3 with confidence of 62
```

OUTPUT:



CONCLUSION

We found major security vulnerabilities that could compromise the confidentiality, integrity, and availability of the voting process.

The results of our study suggest that there is a need for a drastic change in the way in which electronic systems are designed, developed, and tested. Researchers, practitioners, and policy makers need to define novel testing approaches that take into account the peculiar information flow of these systems, as well as the combination of computer security mechanisms and physical procedures necessary to provide a high level of assurance. Electronic voting software is not immune from security concerns.

REFERENCES

- [1]. Schurmann, C.; IT Univ. of Copenhagen, Copenhagen, Denmark. —Electronic Elections: Trust Through Engineering, First international workshop Requirements Engineering for e-Voting Systems (RE-VOTE), 2009.
- [2]. Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.
- [3]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2003.
- [4]. Anil K. Jain and David Maltoni, Handbook of Fingerprint Recognition, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
- [5]. Tadayoshi Shikohno, Adam Stubblefield, Aviel Rubin. Wallach Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004.
- [6]. Y. A. Zuev and S. Ivanov, —The voting as a way to increase the decision reliability, in Proc. Foundations of Information/Decision Fusion with Applications to Engineering Problems, Washington, DC, Aug. 1996, pp.206–210