International Journal of Research in Engineering, Science and Management
Volume-3, Issue-3, March-2020
www.ijresm.com | ISSN (Online): 2581-5792

Design of Secured Biometric Voting Machine

M. Madhu Mohan[1], M. Prakash[2], M. Madhuseelan[3], A. Kishore Kumar[4]
[1,2,3]*UG Scholar, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Coimbatore, India*
[4]*Associate Professor, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Coimbatore, India*

***Abstract*: Being one of the largest democratic countries in the world, it has always been a hard task for the election commission to conduct free and fair polls in India. In India, voting is one of the basic rights of every Indian citizen. By utilizing the right of the voting, people elect their most appropriate leader who will lead them. In recent years where technology is being used in every aspect of life, election is a place to apply the best technology. Huge amount has been spent on this to make sure that the elections are free from any illegal activities. Even though highly alerted and strict election is conducted fake votes has been casted by some local influential people. To avoid the fake votes and fake voters, design of secured biometric voting machine using embedded technology is proposed. In this proposed system we make use of the thumb impression of the individuals, as we know that the thumb impression of every human being is unique. In this proposed system we have used Arduino uno and Finger Print Scanner that can identify each voter, count votes and can avoid fake votes. The proposed system is highly secured, technology-based system.**

***Keywords*: Biometric, Arduino Uno, GSM module.**

1. Introduction

The biometric is a technology of measuring; science and it analyze the biological data. In the modern communications approximately it has accessible electronically, users of computer technology, it has increment in electronic services and with the security system. It improves in the election system with the help of new technologies in voting process. The information about election data is stored, recorded and processed the above information as a digital information. As a pre-poll procedure, a database consisting of the thumb impressions of all the eligible voters in a constituency is created. During elections, the thumb impression of a voter is entered as input to the system. During casting of vote only if the fed input matches the thumb impression of the voting person the vote will be cast. In case of repetition, access to cast a vote is denied. So, this can help in conducting a fair poll.

In this system we have used thumb impression for voter identification or authentication. Every person has an individual unique thumb impression and it helps with accuracy. In a constituency the thumb impression of the database is created for all the voters through this the illegal and repetition of votes is checked.

2. Components

- Arduino Uno
- Fingerprint scanner
- GSM module
- Buzzer
- LCD display
- Buttons

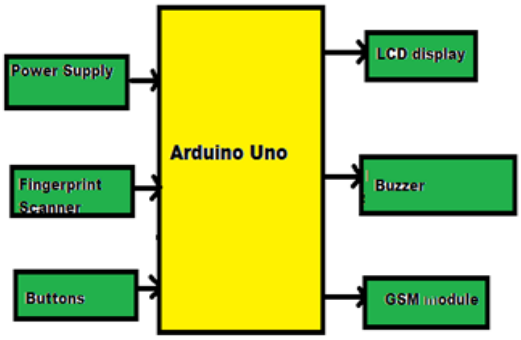

Fig. 1. Block diagram of biometric voting machine

3. Specification of components

A. *Arduino Uno*

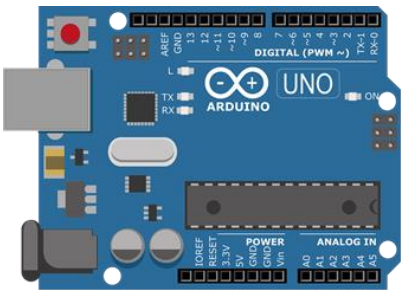

Fig. 2. Arduino Uno

The Arduino Uno is a microcontroller board based on the ATmega328. It has 20 digital input/output pins (of which 6 can be used as PWM outputs and 6 can be used as analog inputs), a 16 MHz resonator, a USB connection, a power jack, an in-circuit system programming (ICSP) header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. There is a

reset button given which is used to restart the program running in the Arduino Uno. There are two ways to restart the whole program. We can use the default reset button. We can connect our own reset button at the pin labeled as Reset. Different Arduino boards have different microcontrollers. It can be said that is the main component in the overall Arduino board. The main IC is a bit different in different Arduino Uno boards. The microcontrollers used basically are of ATMEL Company.

B. Fingerprint scanner

A fingerprint scanner is a type of electronic security system that uses fingerprints for biometric authentication to grant a user access to information or to approve transactions. There are two main ways of scanning fingers. An optical scanner works by shining a bright light over your fingerprint and taking what is effectively a digital photograph.

If we have ever photocopied our hand, we know exactly how this works. Instead of producing a dirty black photocopy, the image feeds into a computer scanner. The scanner uses a light-sensitive microchip (either a CCD, charge-coupled device, or a CMOS image sensor) to produce a digital image.

Fig. 3. Fingerprint scanner

Another type of scanner, known as a capacitive scanner, measures your finger electrically. When your finger rests on a surface, the ridges in your fingerprints touch the surface while the hollows between the ridges stand slightly clear of it. In other words, there are varying distances between each part of your finger and the surface below. A capacitive scanner builds up a picture of your fingerprint by measuring these distances.

C. GSM module

Fig. 3. GSM Module

GSM is combination of TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) and Frequency hopping. Initially, GSM use two frequency bands of 25 MHz width: 890 to 915 MHz frequency band for up-link and 935 to 960 MHz frequency for down-link. Later on, two 75 MHz band were added. 1710 to 1785 MHz for up-link and 1805 to 1880 MHz for down-link. Up-link is the link from ground station to a satellite and down-link is the link from a satellite down to one or more ground stations or receivers. GSM divides the 25 MHz band into 124 channels each having 200 KHz width and remaining 200 KHz is left unused as a guard band to avoid interference.

D. Buzzer

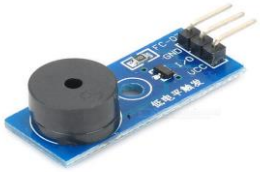

Fig. 5. Buzzer module

An active buzzer has a built-in oscillating source, so it will make sounds when electrified. But a passive buzzer does not have such source, so it will not tweet if DC signals are used; instead, you need to use square waves whose frequency is between 2K and 5K to drive it. The active buzzer is often more expensive than the passive one because of multiple built-in oscillating circuits. A 5V Active Alarm Buzzer Module for Arduino is an audio signaling device, which may be mechanical, electromechanical, or piezoelectric. Typical uses of buzzers include alarm devices, timers, and confirmation of user input such as a mouse click or keystroke.

E. LCD display

A liquid crystal display or LCD draws its definition from its name itself. It is combination of two states of matter, the solid and the liquid. LCD uses a liquid crystal to produce a visible image. Liquid crystal displays are super-thin technology display screen that are generally used in laptop computer screen, TVs, cell phones and portable video games. LCD's technologies allow displays to be much thinner when compared to cathode ray tube (CRT) technology. Liquid crystal display is composed of several layers which include two polarized panel filters and electrodes. LCD technology is used for displaying the image in notebook or some other electronic devices like mini computers. Light is projected from a lens on a layer of liquid crystal. This combination of colored light with the grayscale image of the crystal (formed as electric current flows through the crystal) forms the colored image. This image is then displayed on the screen.

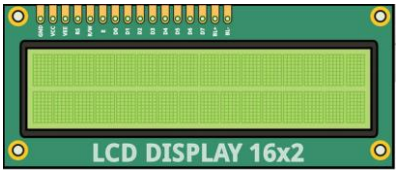

Fig. 6. LCD display

Liquid crystal display technology works by blocking light. Specifically, an LCD is made of two pieces of polarized glass (also called substrate) that contain a liquid crystal material between them. A backlight creates light that passes through the first substrate. At the same time, electrical currents cause the liquid crystal molecules to align to allow varying levels of light to pass through to the second substrate and create the colors and images that you see.

4. Working

In the case of biometric voting machine our biometry (Finger impression) is fed as input and stored in the voting machine. A fingerprint scanner is also connected with the Arduino Uno. During the time of voting the voter is made to register his fingerprint. Only if the finger print that was already fed matches the biometry of the voter vote will be cast. The machine is programmed in such a way that even if the same person tries to cast vote for two people will also be identified and the vote will not be registered. As GSM module is also connected message will be sent to the respective voter as such that their vote has been cast. If any attempt is made to cast a fake vote message will be sent to nearby police station. For the purpose of voter indication LCD display and buzzer is connected.

5. Conclusion

The proposed system is used to enhance security by overcoming counterfeit voting and vote duplication using fingerprint based authentication. In Biometric voting machine, we are actually using the unique identity (finger print) of humans. As a huge amount of capital is being used to conduct a fair election, with this proposed technique the expense for conducting election could be reduced. The number of fake votes will be reduced and the public will also have a trust that the election is conducted in an accurate manner. The proposed system can be contrived simply as well as low-priced and casting vote becomes easier by this process of voting.

References

[1] A. H. Feras, K. H. Mutaz, and M. A. Khairall. “New applied e-voting system,” Journal of Theoretical and Applied Information Technology, 25(2):88-97, 2011.
[2] B. Madan Mohan Reddy, D. Srihari, “RFID Based Biometric Voting Machine Linked to Aadhaar for Safe and Secure Voting, vol. 7, April 2015.
[3] M. Sudhakar, B. Divya Soundarya Sai, “Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller,” Jan.-Feb. 2015.
[4] S. Sridhar CH. Manjulathal "Electronic Voting Machine Using Finger Print," International Journal of Professional Engineering Studies, vol. 7, no. 4, pp. 274-277, 2016.
[5] P. Dayaker, Y. Madan Reddy, M. Bhargav Kumar, “A Survey on Applications and Security Issues of Internet of Things (IoT),” International Journal of Mechanical Engineering & Technology, vol. 8, no. 6, pp. 641-648, July 2017.
[6] B. Divya Soundarya Sai, and M. Sudhakar, "Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller," IOSR Journal of Electronics and Communication Engineering (IOSR-JECE).
[7] R. Karpagavani, M. Mangai, D. Meena, E. Poonguzhali, Chitravalavan, "Aadhaar Identity Based Electronic Voting Machine with Instant Result Announcement,", i-manager's Journal on Embedded Systems, vol. 4, pp. 26, 2015.
[8] J. Deepika, S. Kalaiselvi, S. Mahalakshmi, S. Agnes Shifani, "Smart electronic voting system based on biometric identification survey," Science Technology Engineering & Management (ICONSTEM), 2017, Third International Conference on, pp. 939-942.