



International Journal of Intellectual Advancements and Research in Engineering Computations

Fake Voter Identification System

**Dr.P.Sukumar¹, Mohanasundar.M², RamyaBharathi.B², Sandhiya.S²,
ThilaiNatarajan.K.S²**

¹Ass.Professor, Department of Electronic and Communication Engineering,
Nandha Engineering College [Autonomous]-Erode.

²UG Scholar Student Department of Electronic and Communication Engineering,
Nandha Engineering College [Autonomous]-Erode.

ABSTRACT

Voting is one of the fundamental rights of every citizen of a democratic country. By utilizing the right of the voting, people elect their most suitable leader who will lead them. In this modern era where technology is being used in every aspect of life, election is a place to apply the best technology. Bio-metric identification system to prevent and alert the authorities against fake voting and voting on behalf of absent voters during election and prevent rigging during election. In this proposed system we have used Arduino and Finger Print Scanner that can identify each voter and it can prevent fake votes. The proposed system is more digital, technology-based and secured system.

Index Terms: Voting, Electronic Voting Machine, Arduino, Finger Print Scanner, Biometric.

INTRODUCTION

In a voting system the random citizens elect a candidate by law who represents them and works for them for their welfare. If a wrong candidate is selected, it brings a disaster to the nation. EVM in next parliamentary election but this system also lacks from security. Considering these problems, in this project, a new system of voting is proposed based on electronic voting machine (EVM). The additional feature of this system is biometric security which will be realized by the fingerprints of the voters. In voting systems, the system should be easy to authenticate and verify, it also should have high accuracy rate and reliability. The system also has to be cost effective and unique. An advanced voting system is introduced where aadhar card was used but the system is complicated and the system is online. There are always some risks in online system. In this literature, the proposed system will identify each

voter by their fingerprint with help of fingerprint scanner (FPS). It is able to detect if someone is a registered voter or not and it will deny if someone tries to cast a second vote.

PROPOSED SYSTEM

The proposed system is based on electronic voting machine. The system is able to identify each voter by getting their fingerprint. Whenever the system will receive a fingerprint, it will match the fingerprint from the database. According to the information given by the database, the system will decide if the person is registered or not. System is also able to distinguish second vote. If a particular voter is not registered voter or tries to cast more than one vote, system will identify him and will restrict from voting. However, if neither case is applicable for a voter, it will allow the voter to cast the vote. The system is designed in such a way, if

Author for correspondence:

Department of Electronic and Communication Engineering, Nandha Engineering College [Autonomous]-Erode.

vote is given to a candidate mistakenly; the voter has the ability to change their decision but only once [1-5]. Furthermore, just like any other electronic voting machines, the device will count votes for each candidate. It is also able to show the result, after a certain period of time when the

voting is over. It has very high accuracy rate in case of identifying voter. Another advantage of the system is, it is completely offline system. For this reason, the data cannot be hacked. The flowchart of the system is given below.

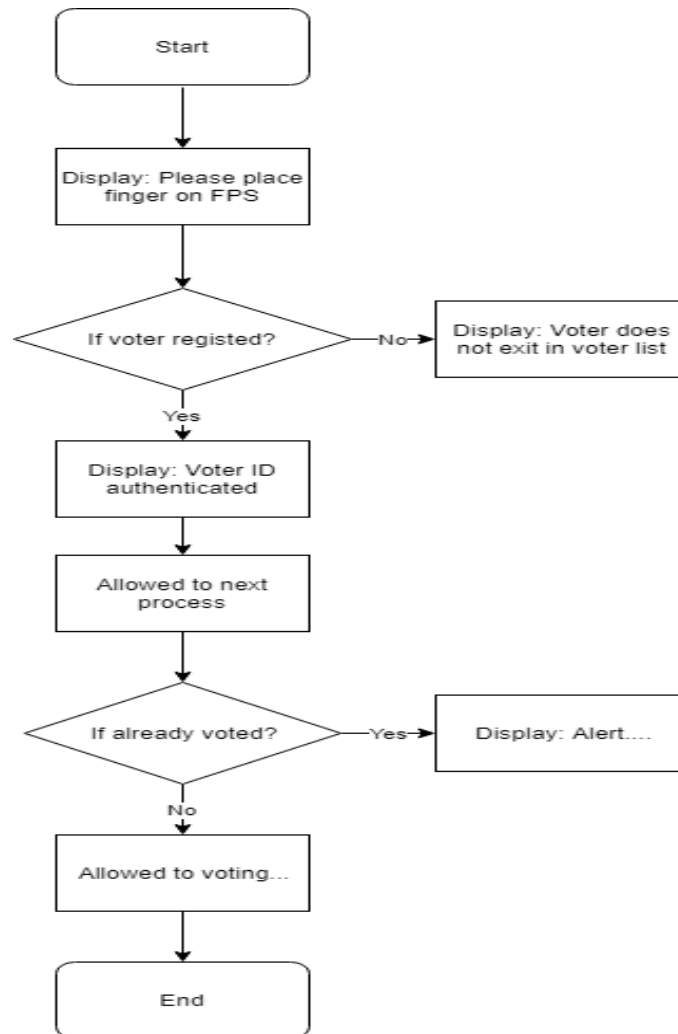


Fig. 1: Flowchart

HARDWARE

Controller Unit

The controller unit of the whole design is Arduino UNO R3 which is an open source microcontroller. The board is based on ATMEGA 328. The board is combined with Analog, Digital

and Pulse width modulation type signals. In this project, for communicating with the finger print scanner, one PWM pin and one digital pin was used. For voting pin purpose, the analog pins were used as digital means. The code can be downloaded with USB connector.

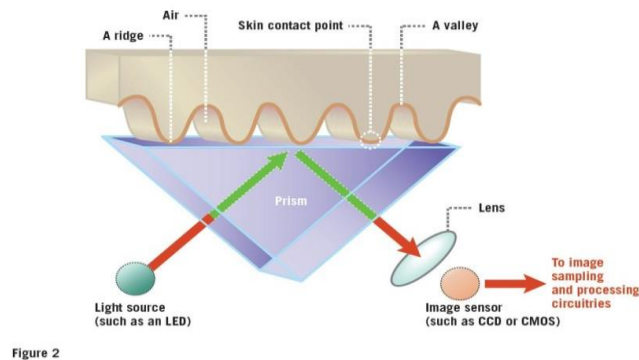
**Fig.2 Arduino**

Fingerprint Scanner Module

The Fingerprint scanner module used for this project. The device is able to capture fingerprint, save it, manipulate it, match fingerprint with the database. It has on board 64-bit CPU which accepts code [8, 9]. In this project, it is interfaced with Arduino. The module has 4 external wires, two of them which communicate with the arduino. Other two wires are biasing voltage and ground. The finger print scanner module's receiving pin

cannot handle more than 3.3 volts. That is why a voltage divider circuit was used so that the finger print scanner can get approximately 3.3 volts. Other wires were directly connected. Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current. The sensor is made up of one or more semiconductor chips containing an array of tiny cells.

An optical sensor.

**Fig. 3: Fingerprint Scanner**

SOFTWARE

For controlling the controller unit, which is arduino UNO R3 with ATMEGA 328 microcontroller, the software from arduino developer is used. The arduino board can be programmed with this software. UNO was selected from Tools>Board menu and ATMEGA 328 was

selected for microcontroller. In case of controlling the fingerprint scanner a library file was used created and developed by Josh Hawley [10]. The header file from this library was used to interface the scanner with arduino and for controlling it. The language used in the header file is C++.

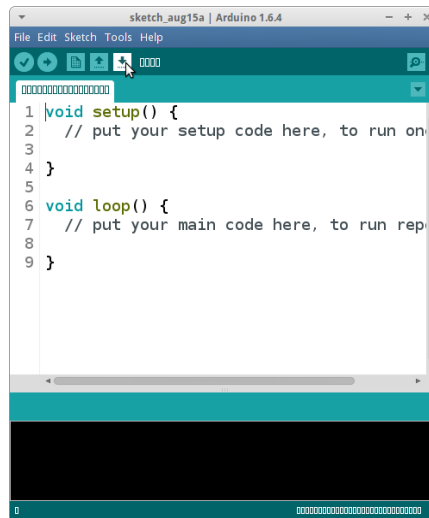


Fig.4 Software

WORKING PROCESS

Authenticity of the Voting Process and Privacy of the Voter Rights.

Certain factors play out big in a given voting process in any particular country. Culture itself and the underpinning social factors/values largely determine the rules and regulations that govern any voting process. In countries, where election results are determined through the voter counts that are tallied by directly depositing specially designed voting cards into the voting boxes, there are tendencies that electoral votes can get misappropriated in many ways; some voters would tend to attempt to vote more than the number of times permissible by law for a given candidate; other voters may try to vote in lieu of other illegible voters so that the voter count would weigh favorably towards one candidate or another, to mention just a few. Counterfeit/Malice is yet another issue that can jeopardize the integrity of an election process. Automating an election process,

while relying on state-of-the-art in computer and ICT technologies, can significantly mitigate many of the factors that would hamper a healthy progress of an election process. Nonetheless, relying totally on available information technologies can only warrant the authentication/validation of the identity of a given voter, but, still, would not have the capacity to block any attempted abuse of the voting system, viz., those voters who simply try to vote on behalf of others (fraud). Without additional measures, the integrity of a voting process, within the proper context, is far from any acceptable standard/s; the incorporation of biometrics would definitely have an added value towards achieving the required levels of election integrity. Present day applications, including banking applications, guarding of high-security establishments, monitoring of passengers across border posts, amongst many others are witnessing increasing levels in the use of biometric technologies and devices.

Biometrics is best defined as measurable physiological and / or biological characteristics that can be utilized to verify the identity of an individual. They include fingerprints, retinal and iris scanning, hand geometry, voice patterns, facial recognition, Gait recognition, DNA and other techniques. They are of interest in any area where it is important to verify the true identity of an individual. Initially, these techniques were employed primarily in specialist high security applications; however, we are now seeing their uses and proposed uses in a much broader range of public facing situations. Essentially, a biometric system follows two characteristic traits: identification and verification. The former involves

identifying a person from all biometric measurements collected in a database. The question that this process seeks to answer is: “who is this?” It, therefore, involves a one-compared-to-many match. Verification involves authenticating a person’s claimed identity from his/her previously enrolled pattern.

“Is this who he claims to be?” is the question that this process seeks to answer. This involves a one-to-one match [6, 7]. Verifying the identity of a person against a given biometric measure involves five phases that the system needs to go through. At the beginning, input data is read from the person through the reading sensors.

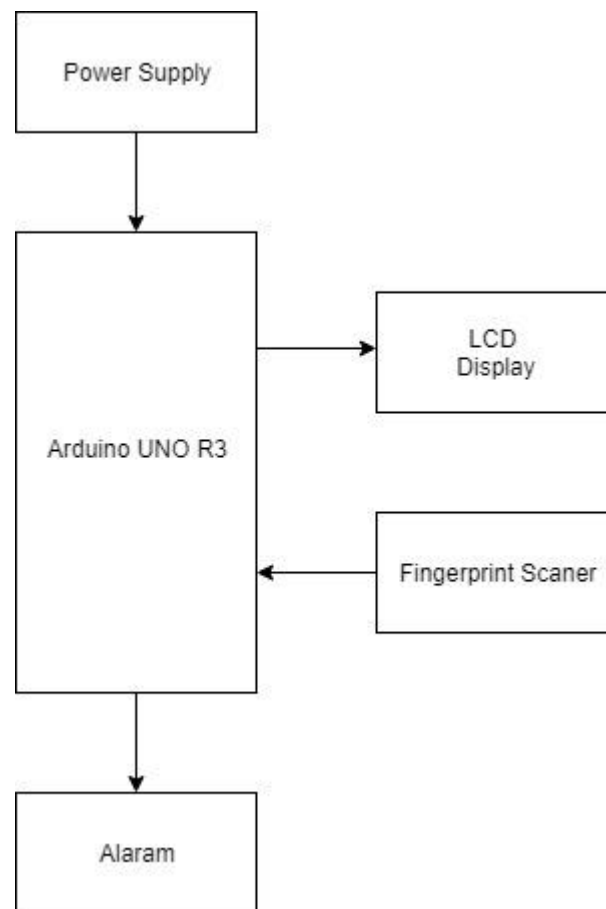


Figure: 6 Block Diagram

Collected data is, then, sent across a network to some central database hosting a biometric system. The system will, then, perform identity matching

using standardized and/or custom matching techniques. Figure 5 illustrates data flow in a typical biometric identification process.



Figure 5: Biometric System Data Flow

The incorporation of biometric technologies can be as simple as using a single biometric. However, a single biometric measure is always subject to security breaches, if not properly attended and administered. This naturally includes security passwords, fingerprints, and signatures, all of which can be spoofed when applied in a non-properly attended environment. This is significantly alleviated and system security enhanced with the proper application of combined simple biometric measures. The application of combined weak biometrics leads to systems that are less complex and more robust in terms of the security levels attained. There are strong single biometric measures which involve retinal and iris scans that are rather hard, if not impossible, to breach, but usually lead to more complex systems which, in turn, slow down the underlying biometric matching process due to the amount of data processing involved. For these reasons, amongst others, the type of biometrics addressed in this work is of the former type that involves combined biometrics of the weak types.

APPLICATIONS

The proposed system can be used at various levels of public elections in our country. This system can be used even in the committee board election.

ADVANTAGES AND DISADVANTAGES

Advantages

- Cost effective.
- It is economical.
- Low power consumption.
- Less manpower required.
- This system allows only authenticated voting than the existing equipment as the person is identified based on his Fingerprint which is unique to each individual.
- Avoids invalid voting as it prevents unregistered voters from voting.
- Ease of transportation due to its compact size.
- Convenient on the part of voter.

Disadvantages

- Before voting the user has to enroll first.

CONCLUSION

Proposed system provides best possible solution to problems associated with the Indian voting system. Since this system includes Biometric Authentication, it ensures that vote can't be casted by unauthorized persons. This system allows voters to cast their votes remotely which help senior citizens, disabled, patients and migrants which intern increases voting percentage. This system will make India to have sophisticated and transparent voting system in the world.

REFERENCES

- [1]. Afrina Ali, "Is Bangladesh going for e-voting?" Available: <http://www.thefinancialexpress-bd.com/2017/02/06/61143/Is-Bangladesh-going-for-e-vote>, 2017.
- [2]. P Sukumar, RK Gnanamurthy "Computer aided detection of cervical cancer using pap smear images based on adaptive neuro fuzzy inference system classifier", 2016.
- [3]. Remmert, M.: "Toward European Standards on Electronic Voting", The Council of Europe, 2017.
- [4]. S Ravi, VitaliyMezhuyev, K IyswaryaAnnapoorani, P Sukumar "Design and Implementation of a Microcontroller Based Buck Boost Converter as a Smooth Starter for Permanent Magnet Motor", 2016.
- [5]. Bhuvanapriya R., RozilBanu S., Sivapriya P. and Kalaiselvi V. K. G., "Smart voting" , 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, 2017, 143-147.
- [6]. Prabhakher. S, P. Sukumar "Performance Analysis of Rotation Invariant parts Based Object Detection in High-Resolution Images" International Journal of Engineering Science Invention, 2015.
- [7]. "GT-511C3 datasheet" [Online] Available: [https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C3_datasheet_2\(1\)](https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C3_datasheet_2(1)), 2017, 20161025.
- [8]. P.Sukumar S.Tamilselvi "Clock Power Reduction using Multi-Bit Flip-Flop Technique"IRACST – Engineering Science and Technology: An International Journal, 2014.
- [9]. K Tamilselvan, R Krishnaraj, P Sukumar, T Jayakumar "Security Method for Human Finger and Palm Images Identification"International Journal of Emerging Technologies in Engineering Research (IJETER), 2016.
- [10]. "Fingerprint_Scanner-TTL" [Online] Available: https://github.com/sparkfun/Fingerprint_Scanner-TTL.