

Advanced Electronic Voting Machine Using Arduino

Bennet Prabha¹, A. Murali Krishna², V. Gokul³, S. Devanand⁴

¹Professor, Dept. of Computer Science and Engg., SRM Institute of Science and Technology, Chennai, India

^{2,3,4}Student, Dept. of Computer Science and Engg., SRM Institute of Science and Technology, Chennai, India

Abstract—The fingerprint-based voting strategy is an application recognized by the user through its fingerprint [9]. Since every person is different, the voter may be easily recognized. The system allows the voter to vote through his fingerprint. The fingerprint is used to identify the user as a symbol. Each person has different types of fingerprinted properties. Fingerprint is used as voter recognition. The voter will be able to vote for a second time and the computer candidate does not allow him to vote. The system administrator will allow the candidate to include the name and candidate photo. The administrator only has the right to add a candidate name and a nominated photo. The voter will register the voter when the voter is checked. The user will authenticate the administrator by verifying the identity, then the administrator will record the voter. Number of candidates added to the system. The admin must add the date. Once the user ID and administrator receives the password, the user can sign up and vote for the nominated candidate. Allows the system to vote for the single candidate. The system allows the user to vote for a specific time. The administrator can add any candidate when the new election is announced. Using the identity of the test can be seen by the administrator end. Even if the user chooses, the user can see it.

Index Terms—arduino, fingerprint, sensor, fingerprint sensor, biometric, EVM, minutiae

I. INTRODUCTION

A machine which is used during elections for the purpose of collecting and counting the votes casted by the common people. This machine actually replaces the traditional way of collecting votes through boxes consisting of voting papers. This method is called as paper ballot. Slowly, this system has changed or altered into a new technical and mechanical system which uses electronic voting machines in order to avoid misconceptions. Even though this voting machine is fast and accurate, this system needs more manpower and also it is not much more reliable. To increase the reliability of the voting, many algorithms have been introduced. One of the major idea of developing the system is to use the person's identity. The major unique identity of the each and every person is his fingerprint, Iris etc. So one of the cheapest way of recognition is fingerprint recognition. Not only the developers use this biometric, the government also has taken necessary steps to collect the biometric data and stored into a database. The government also issued aadhar card to identify the person's unique identity. Using the aadhar card, we can easily make the voters to cast the

vote without difficulty. Due to the advancements in upcoming technologies, we can also able to collect and count the votes in a faster manner and the counting process starts simultaneously as soon as the voting process ends.

II. 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 BUs. 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.

Advantages of EVM:

EVMs are powered by an ordinary 6 volt alkaline battery manufactured by Bharat Electronics Ltd., Bangalore and Electronic Corporation of India Ltd., Hyderabad. This design enables the use of EVMs throughout the country without interruptions because several parts of India do not have power supply and/or erratic power supply. It is not possible to vote more than once by pressing the button again and again. As soon as a particular button on the Ballot Unit is pressed, the vote is recorded for that particular candidate and the machine gets locked for next voter. Even if one presses that button further or any other button, no further vote will be recorded. This way the EVMs ensure the principle of "one person, one vote". Bogus voting can be greatly reduced by the use of EVMs. In case of ballot paper system, a bogus voter can stuff thousands of bogus ballot papers inside the ballot box because of manual process. But, an EVM is programmed to record only five votes in a minute.

III. PROPOSED SYSTEM

Fingerprint Biometric Human fingerprints are unique to each person and can be regarded as a sort of signature, certifying the person's identity. Fingerprints [6] are the oldest and most widely used form of biometric identification. A fingerprint is formed from an impression of pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. The minutiae which are the local discontinuities in the ridge flow pattern, provide the features that are used for identification.

Fingerprint Recognition [7] It is an active research area nowadays. An important component in fingerprint recognition systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: fingerprint verification algorithms and fingerprint identification algorithms. The aim of fingerprint verification algorithms is to determine whether two fingerprints come from the same finger or

Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller.

On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger. Despite the widespread use of fingerprints, there is little statistical theory on the uniqueness of fingerprint minutiae. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from the fingerprint images. However, fingerprint images are rarely of perfect quality. They may be degraded and corrupted due to variations in skin and impression conditions. Thus, image enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations. Straightforward matching [8] of the to-be-identified fingerprint pattern against many already known fingerprint patterns would not serve well, due to the high sensitivity to errors in capturing fingerprints (e.g. due to rough

fingers, damaged fingerprint areas or the way a finger is placed on different areas of a fingerprint scanner window that can result in different orientation or deformation of the fingerprint during the scanning procedure). A more advanced solution to this problem is to extract features of so called minutiae points (points where the tiny ridges and capillary lines in a fingerprint have branches or ends) from the fingerprint image and check matching between these sets of very specific fingerprint features. The extraction and comparison of minutiae points requires sophisticated algorithms for reliable processing of the fingerprint image, which includes eliminating visual noise from the image, extracting minutiae and determining rotation and translation of the fingerprint. At the same time, the algorithms must be as fast as possible for comfortable use in applications with a large number of users. Many of these applications can run on a PC, however some applications require that the system be implemented on low cost, compact and/or mobile embedded devices such as doors, gates, handheld computers, cell phones etc.). For developers who intend to implement the fingerprint recognition algorithm into a microchip, compactness of algorithm and small size of required memory may also be important

IV. ADVANTAGE

- Cost is less, because human interventions are less in the system.
- Due to real time approach counting of votes could be done at the same time while voting.
- Time take to cast vote is less.
- Due to use of fingerprint scanner the cross voting is cannot be done.
- Due to use of encryption and decryption technique the hacking is not possible.
- The overall system installation is effortless.

V. FUTURE SCOPE

- For getting more details we can use aadhar card in future.
- For storing fingerprint images the external memory can be provided then later it can be access the fingerprint images.
- To make it user friendly the audio output can be used for illiterate voters.
- In future, making the voting system online this advanced system will be referred.

VI. CONCLUSION

This system enables all the citizens of the country to give his/her vote over the internet and avoid proxy vote or double voting and provide highly secure, quick to access and easy to maintain all information of voting ,highly efficient and reliable due to the use of fingerprint scanner it reduce or remove unwanted human error. In addition this voting system is capable of handling multiple modules in various centers and provide better scalability for large election.

REFERENCES

- [1] Timaadeepkaurameja, Jasleenkarubassi, D amanjeet kaur" Implementation of electronic voting machine through FPGA" International journal of soft computing and artificial intelligence vol. 2, no. 1.
- [2] Hari K. Prasad J. Alex haldermanRopGonggrijp "security analysis of India's electronic voting machine,"proc.17th ACM Conference on computer and communication security (CCS'10).
- [3] Salil Prabhakar, 2001. "Fingerprint Classification and matching using filter bank.
- [4] DavideMaltoni, Anil K. Jain, 2009,"Handbook of fingerprint Recognatio 2nd edition.
- [5] Ashok Kumar .D., Unmalsariba Begum T.,"A novel design of electronic voting system using fingerprint", International Journal of Innovative Technology & creative Engineering, vol1 no 1.pp:12 19, January 2011.
- [6] Junichsakamoto, 2008 "Hybrid fingerprint Recognition.
- [7] <http://nevonprojects.com/fingerprint-voting-system-project-2/>
- [8] J. Deepika, S. Kalaiselvi, S. Mahalakshmi and S. A. Shifani, "Smart electronic voting system based on biometric identification-survey," *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, Chennai, 2017, pp. 939-942.
- [9] S. M. Hasan, A. M. Anis, H. Rahman, J. S. Alam, S. I. Nabil and M. K. Rhaman, "Development of electronic voting machine with the inclusion of Near Field Communication ID cards and biometric fingerprint identifier," *2014 17th International Conference on Computer and Information Technology (ICCIT)*, Dhaka, 2014, pp. 383-387.
- [10] D. Gentles and S. Sankaranarayanan, "Biometric secured mobile voting," *2011 Second Asian Himalayas International Conference on Internet (AH-ICI)*, Kathmandu, 2011, pp. 1-6.