



International Journal of Intellectual Advancements and Research in Engineering Computations

Electronic voting machine based on fingerprint and iris authentication

G.Prabhakaran¹, T.Dharshini priya², N.Janani³, R.Deepan raj⁴, P.Elavarasan⁵.

¹Assistant Professor, ²³⁴⁵Final year UG students.

Department of Electronics and Communication Engineering.

Nandha Engineering College, (Autonomous), Erode.

Email id:¹prabhakaran.govindaraj@nandhaengg.org, ²dharshinidharsh96@gmail.com,
³jananinataraj1997@gmail.com.

Abstract-Biometrics is the science and innovation of estimating and investigating natural information. In data innovation, biometrics alludes to advancements that measure and break down human body qualities, for example, DNA, fingerprints, eye retinas and irises, voice designs, facial examples and hand estimations, for validation purposes. In this paper we have utilized iris acknowledgment and thumb impression with the end goal of voter distinguishing proof or verification. As the iris and thumb impression of each individual is remarkable, it helps in boosting the precision. A database is made containing the iris and thumb impressions of the considerable number of voters in the supporters. Unlawful votes and redundancy of votes is checked for in this framework. Henceforth if this framework is utilized the races would be reasonable and free from gear.

Keywords-Electronic voting machine; Fingerprint and Iris recognition.

I. INTRODUCTION

The goal of voting is to enable voters to practice their entitlement to express their decisions in regards to particular issues, bits of enactment, national activities, sacred alterations, reviews as well as to pick their legislature and political delegates. It has dependably been a cumbersome assignment for the decision commission to gather information in our nation, the biggest popular government on the planet. A great deal of cash has been spent on this to ensure that the races are sans frenzy. Be that as it may, now-a - days it has turned out to be exceptionally normal for a few powers to enjoy fixing which may in the long run prompt an outcome in opposition to the genuine decision given by the general population. Keeping in mind the end goal to give cheap answers for the over, this task will be executed with biometric

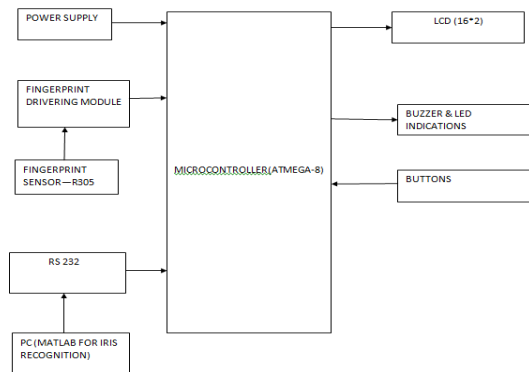
framework i.e. unique finger impression filtering and Irish identification. This is utilized to guarantee the security to keep away from phony, rehashed voting and so on. It additionally improves the precision and speed of the procedure. The framework utilizes thumb impression and a camera based iris location unit for voter ID as we realize that these parameters of each individual has a one of a kind example. In this way it would have an edge over the present day voting frameworks. The motivation behind such framework is to guarantee that the voting rights are gotten to just by a true blue client and nobody else.

In this, formation of a database comprising of the thumb impressions and iris of all the qualified voters in a supporters is done as a pre-survey strategy. Amid races, the thumb impression of a voter is entered as contribution to the framework took after by iris examining and recognition. This is then contrasted and the accessible records in the database. On the off chance that the specific example matches with any one in the accessible record, access to make a choice is conceded. Be that as it may, in the event that the example doesn't coordinate with the records of the database or in the event of reiteration, access to make a choice is denied or the vote gets rejected. The outcome is momentary and checking is finished. The general cost for directing decisions gets lessened thus does the upkeep cost of the frameworks.

II. SYSTEM DESIGN

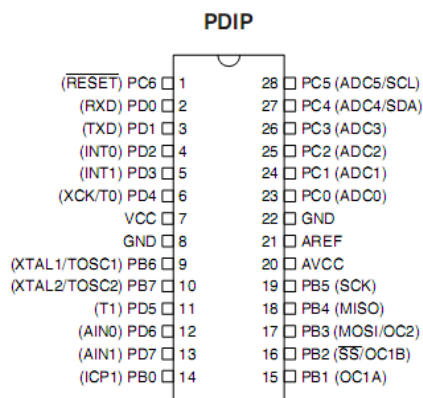
A biometric system is fundamentally a case affirmation structure that works by getting biometric data from an individual, removing a

rundown of capacities from the picked up data, and taking a gander at this rundown of abilities against the design set in the database. Dependent upon the application setting, a biometric system may work either under wraps mode or recognizing confirmation mode. Moreover, not the same as the manual approach for iris affirmation and one of a kind check affirmation by authorities, the iris ID is done by techniques for a camera. the exceptional stamp affirmation here is suggested as AFRS (Customized Finger impression Affirmation System), which is program-based.



III. ATMEGA8

The primary element of Atmega8 Microcontroller is that, every one of the pins of the Microcontroller bolster two signs aside from 5-pins. The Atmega8 microcontroller comprises of 28 pins where pins 9,10,14,15,16,17,18,19 are utilized for port B, Pins 23,24,25,26,27,28 and 1 are utilized for port C and pins 2,3,4,5,6,11,12 are utilized for port D.



Stick - 1 is the RST (Reset) stick and applying a low level flag for a period longer than the base heartbeat length will deliver a RESET.

Stick 2 and stick 3 are utilized as a part of USART

for serial correspondence

Stick 4 and stick 5 are utilized as an outside intrude. One of them will enact when an interfere with hail bit of the status enlist is set and the other will actuate as long as the barge in condition succeeds.

Stick 9 and stick 10 are utilized as a clock counters oscillators and also an outer oscillator where the precious stone is related straightforwardly with the two pins. Stick 10 is utilized for low-recurrence precious stone oscillator or gem oscillator. In the event that the inward balanced RC oscillator is utilized as the CLK source and the non concurrent clock is permitted, these pins can be used as a clock oscillator stick.

Stick 19 is utilized as an Ace CLK o/p, slave CLK I/p for the SPI-channel.

Stick 18 is utilized as Ace CLK I/p, slave CLK o/p.

Stick 17 is utilized as Ace information o/p, slave information I/p for the SPI-channel. It is utilized as an I/p when enabled by a slave and is bidirectional when permitted by the ace. This stick can likewise be used as an o/p contrast and match o/p, which helps as an outside o/p for the clock/counter.

Stick 16 is utilized as a slave decision I/p. It can likewise be utilized as a clock or counter1 relatively by orchestrating the PB2-stick as an o/p.

Stick 15 can be utilized as an outside o/p of the clock or counter analyze coordinate A.

Stick 23 to Pins28 have utilized for ADC (computerized estimation of simple information) channels.

Stick 27 can likewise be utilized as a serial interface CLK and stick 28 can be utilized as a serial interface information

Stick 12 and stick 13 are utilized as a Simple Comparator I/ps.

Stick 6 and stick 11 are utilized as clock/counter sources.

Memory: It has 1Kbyte Interior SRAM, 8 Kb of Blaze program memory and 512 Bytes of EEPROM.

I/O Ports: It has three ports, in particular port-B, port-C and port-D and 23 I/O line can be achieved from these ports.

Intrudes on: The two Outside Interfere with sources

are situated at port D. Nineteen unique interferes with vectors supporting nineteen occasions created by inside peripherals.

Clock/Counter: There are 3-Inside Clocks are available, 8 bit-2, 16 bit-1, introducing various working modes and supporting interior/outer timing.

Serial Fringe Interface (SPI): ATmega8 microcontroller holds three coordinated specialized gadgets. One of them is a SPI, 4-pins are assigned to the Microcontroller to actualize this arrangement of correspondence.

USART: USART is a standout amongst the most capable correspondence arrangements. Microcontroller ATmega8 underpins both synchronous and offbeat information transmission plans. It has three pins distributed for that. In numerous correspondence ventures, USART module is broadly utilized for correspondence with PC-Microcontroller.

Two Wire Interface (TWI): TWI is an another specialized gadget which is available in ATmega8 microcontroller. It grants planners to set up a correspondence b/n two gadgets utilizing two wires alongside a common GND association, As the o/p of the TWI is made by methods for open gatherer o/ps, accordingly outside draw up resistors are mandatory to make the circuit.

Simple Comparator: This module is fused in the incorporated circuit that offers differentiate office between two voltages connected to the two contributions of the comparator through Outer pins related with the Microcontroller.

ADC: Inbuilt ADC (simple to computerized converter) can modify a simple I/p motion into advanced information of the 10-bit determination. For a most extreme of the low-end application, this much determination is adequate.

IV. FINGERPRINT RECOGNITION SYSTEM

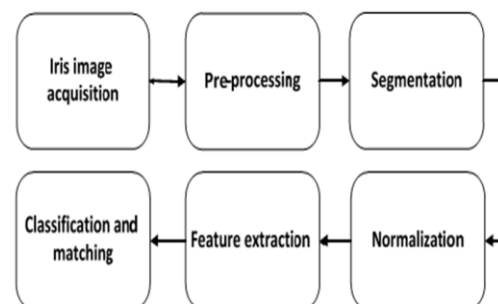
Unique mark distinguishing proof (now and then alluded to as dactyloscopy or palm print recognizable proof is the way toward looking at addressed and known rubbing skin edge impressions (see Details) from fingers or palms or even toes to decide whether the impressions are from a similar finger or palm. The adaptability of grinding edge skin implies that no two finger or palm prints are ever precisely similar (never indistinguishable in everything about), two impressions recorded quickly after each other. Unique mark distinguishing proof (additionally

alluded to as individualization) happens when a specialist (or a specialist PC framework working under limit scoring rules) discovers that two rubbing edge impressions started from a similar finger or palm (or toe, sole) to the avoidance of all others.

A known print is the deliberate account of the grinding edges, for the most part with dark printers ink moved over a differentiating white foundation, normally a white card. Grinding edges can likewise be recorded carefully utilizing a method called Live-Output. An idle print is the shot proliferation of the rubbing edges stored on the surface of a thing. Inactive prints are regularly fragmentary and may require concoction techniques, powder, or elective light sources with a specific end goal to be pictured.

At the point when grating edges interact with a surface that is open to a print, material on the edges, for example, sweat, oil, ink, and so on can be exchanged to the thing. The elements which influence rubbing edge impressions are various, along these lines expecting analysts to experience broad and target think about with a specific end goal to be prepared to competency. Malleability of the skin, affidavit weight, slippage, the framework, the surface, and the improvement medium are only a portion of the different variables which can make an inert print show up uniquely in contrast to the known account of a similar grinding edges. Undoubtedly, the states of rubbing edge testimony are one of a kind and never copied. This is another motivation behind why broad and target contemplate is vital for analysts to accomplish competency.

V. IRIS RECOGNITION SYSTEM



STEPS TO FOLLOW FOR IRIS RECOGNITION:

A biometric arrangement of iris acknowledgment in unconstrained conditions in which each piece's capacity is quickly examined as takes after:

1. Picture securing: in this stage, a photograph is taken from iris.
2. Pre-preparing: including edge location, differentiate alteration and multiplier.
3. Division: including restriction of iris inward and external limits and confinement of limit amongst iris and eyelids.
4. Standardization: including change from polar to Cartesian directions and standardization of iris picture.
5. Highlight extraction: including commotion expulsion from iris picture and creating iris code.
6. Grouping and coordinating: including contrasting and coordinating of iris code and the codes effectively spared in database.

With respect to actuality that in an unconstrained domain iris may have impediments caused by upper or lower eyelids or eyes may move left and rightwards, as the paper goes on, these squares are presented and such issues are explained.

VI. CONCLUSION

Subsequently, here a voting framework is talked about considering unique mark and iris coordinating procedure. Additionally unique systems are broke down. It is discovered that the unique finger impression and iris based voting framework is best reasonable in planning a proposed design. Thus, a proposed framework will actualize a voting framework with protection and security. This task can be utilized for voting since it beat all the downsides of standard voting machine likewise give extra security. Its primary leeway is that since biometric information of each individual is exceptional and thus this framework totally diminishes the shot of invalid votes. The framework can be fabricated just and also shoddy.

VII. REFERENCES

- [1] G. S. Heiberg, P. Laud & J. Willemson, "The application of i-voting for Estonian parliamentary elections of 2011." *E-Voting and Identity*: Springer Berlin Heidelberg, Vol.7187, pp. 208–223, 2012.
- [2] I. V. Blankenship, "Trusting the Machine: Inherent Problems with Electronic Voting Systems", *Global Information Assurance Certification Paper*, 2004.
- [3] Bellis, "The History of Voting Machines - History of the Voting System Standards Program", *About.com Inventors*, 2015. [Online]. Available: <http://inventors.about.com/library/weekly/aa111300b.htm>.
- [4] S. Everett, "The Usability of Electronic Voting Machines and How Votes Can Be Changed without Detection," PhD dissertation, Rice University, 2007.
- [5] C. Burton, C. Culnane, J. Heather, T. Peacock, P. Y. A. Ryan, S. Schneider, S. Srinivasan, V. Teague, R. Wen and Z. Xia "A supervised verifiable voting protocol for the Victorian Electoral Commission", *Proc. 5th International Conference on Electronic Voting*, 2012.
- [6] Davis and S. Thomas, "Direct recording electronic voting machine and voting process", US5583329 A, 1996.
- [7] F. S. Wood, "Electric voting-machine", U.S. Patent 616,174, Granted Dec. 20, 1898.
- [8] J. Fried and A. Lee, "Study On Open Source Voting Systems", Draft Report, San Francisco Local Agency Formation Commission, 2015.
- [9] Wikipedia, "Electronic voting", 2015. [Online]. Available: https://en.wikipedia.org/wiki/Electronic_voting
- [10] A. Boyle, 'Pentagon launches Internet voting effort for overseas Americans', *MSNBC*, 2003.
- [11] D. Jefferson, A. Rubin, B. Simmons, and D. Wagner. "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)". Technical report, 2004.
- [12] GIAC Security Essentials Certification, "Trusting the machine: inherent problems with electronic voting systems", *Global Information Assurance Certification Paper*, 2004.
- [13] CNN WB, 'Pentagon halts Internet voting system', 2015.
- [14] L. Landes, 'Internet Voting -- The End of Democracy?', *Dissident Voice*, 2003.
- [15] D. A. Gritzalis, "Secure electronic voting.", Dordrecht: Kluwer Academic Publishers, 2003.
- [16] M. M. Sarker and M. N. Islam, "Management of sustainable, credible and integrated electronic voting (E-Voting) system for Bangladesh," *Management of Sustainable Development*. Vol. 5, pp. 15–21, 2013.
- [17] P. G. Neumann "Security criteria for electronic voting", *Proceedings of the 16th*

National Computer Security Conference, pp.478–481 1993.

[18] R. Newman, “Security and Access Control Using Biometric Technologies: Application, Technology, and Management” (1st ed.), Course Technology Press, Boston, MA, United States. 2009.

[19] S. Hasan, A. Anis, H. Rahman, J. Alam, S. Nabil and M. 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), 2014.