ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 11, Issue 1, pp: (1-10), Month: January - March 2024, Available at: www.paperpublications.org

Fingerprint Authentication Voting System using Arduino

Nganso Keupnou Romuald Peguy[1], Mbonyineza Roger[2],
Tinashe Valentine Gnerwande[3]

[1,2,3] College of Energy and Electrical Engineering, Hohai University, Nanjing 211106, China

Corresponding Author: Nganso Keupnou Romuald Peguy

DOI: https://doi.org/10.5281/zenodo.10566691

Published Date: 25-January-2024

***Abstract:* This study explores the use of Arduino to construct a fingerprint authentication voting system in order to improve electoral security and efficiency. By incorporating biometric technology, the method guarantees each voter's identification is distinct and verifiable. It reduces the hazards connected with conventional techniques and encourages a more trustworthy electoral process by utilizing fingerprints. In examining the system's technical features, security protocols, and sociological ramifications, the article highlights biometrics' crucial role in preserving democratic norms.**

***Keywords:* Biometric identification, Digital identity, Fingerprint, Voting system, Arduino Uno, liberal democracy.**

I. INTRODUCTION

In recent years, advancements in technology have revolutionized traditional voting systems, giving rise to innovative approaches aimed at enhancing the integrity and security of electoral processes. One such paradigm shift is the introduction of the "Fingerprint Authentication Voting System." This cutting-edge electoral technology leverages biometric authentication, specifically fingerprints, to ensure a more robust and tamper-resistant voting experience. By integrating biometric identifiers into the voting process, this system not only addresses concerns related to identity verification but also strives to create a more inclusive and streamlined democratic exercise[1] [2].

Nearly everyone in the world is born with a fingerprint that is unique and often are not affected by current (mental) conditions such as stress or illness [3]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae[4], and for this reason, the fingerprint has turned to be a useful part of biometric security. In electoral process, fingerprint identification is required during two phases: Firstly, for voter registration in order to establish the right to vote and afterwards. Secondly, at voting time, fingerprint allows a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication)[5] .

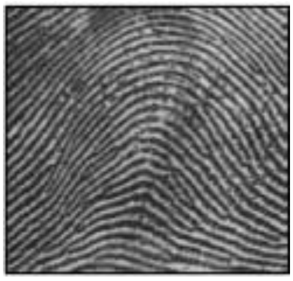


Figure 1: sample fingerprint

II. LITERATURE REVIEW

Over the years, the advent of technology in electoral systems has ushered in an era of innovative solutions aimed at enhancing the security, efficiency, and inclusivity of the voting process. Among these advancements, the Fingerprint Authentication Voting System has garnered significant attention. This literature review aims to explore existing research and literature on the subject, shedding light on the evolution, challenges, and potential implications of implementing fingerprint authentication in voting systems. The integration of biometrics, particularly fingerprint authentication, into voting systems is a response to the increasing need for robust identity verification mechanisms[6].

Early studies[7] discuss the historical evolution of biometric voting systems, highlighting the transition from traditional methods to technologically sophisticated approaches. Fingerprint authentication emerges as a frontrunner due to its reliability, ease of use, and widespread acceptance in various applications. One of the primary motivations behind adopting fingerprint authentication in voting systems is to enhance security and safeguard the integrity of the electoral process.[8][9] emphasizes the cryptographic protocols and security measures embedded in fingerprint-based voting systems. The analysis of potential vulnerabilities and countermeasures contributes to a comprehensive understanding of the system's resilience against fraudulent activities.

Fingerprint authentication offers a promising avenue for addressing concerns related to inclusivity in the electoral process. Studies [10],[11]delve into the accessibility aspects of fingerprint-based voting, exploring how this technology can facilitate participation for individuals with disabilities and those in remote areas. The potential to create a more inclusive democracy is a crucial aspect that warrants further investigation. As with any technological innovation, public perception and ethical considerations play a pivotal role in the successful adoption of fingerprint authentication in voting systems. Research [12],[13]examines the attitudes of voters toward biometric authentication, addressing concerns related to privacy, consent, and trust in the electoral process. Despite the promising prospects, the literature also acknowledges challenges associated with implementing fingerprint authentication in voting systems. Studies [14], [15]delve into issues such as scalability, cost, and the potential for technical glitches. Understanding these challenges is crucial for developing robust solutions that ensure the seamless integration of fingerprint authentication into electoral practices.

Summing up the above, the challenging problem we are trying to solve is how to establish an authentic fingerprint system for voting, which cost efficient and affordable for local areas use. To this end we propose a one-to-many match voter’s fingerprint mechanism for which an input can be compared with the database and the matching output can be allowed to cast a vote. The contributions of this paper mainly lie as follows:

1. We proposed fingerprint authentication to facilitate the voting system for local area use

2. A one-to-many match voter’s fingerprint mechanism was used to avoid fraud by matching the input voter to database registered fingerprints.

3. The Arduino software is incorporated in this system to ease the implementation and to restrain the costs

The rest of this article is organized as follows: Section 3 presents the Authentication voting Framework, and the specific hardware descriptions. Section 4 presents the implementation of the proposed mechanism and discusses the findings, while section 5 concludes the paper with future perspectives.

III. METHODOLOGY

A. Authentication voting Framework

Fingerprints are considered to be the best and fastest method for biometric identification. They are secure to use, unique for every person and does not change in one’s lifetime. This project aims at designing a fingerprint authentication voting system. For the voter’s identification, a fingerprint recognition-based identification system is used. The fingerprint module is used to sense fingerprints and provide the microcontroller for further processing. The system comprises the data base of eligible voters. The voting system tallies the recognized finger print against the ones stored in the database. If a match is found that person is allowed to vote. Once a vote is casted by that person his ID is marked as voted and rolled out for that voting process. This avoids double vote casting. It also gives allowance for a fingerprint to be deleted from the database. Thus, this system provides for a fully automated voting system with finger print based authentication.

B. Hardware Description

We considered a system: The fingerprint authentication voting system (FAVS) hardware mainly contains an Arduino Uno R3 board, a finger print module, an LCD display with potentiometer.

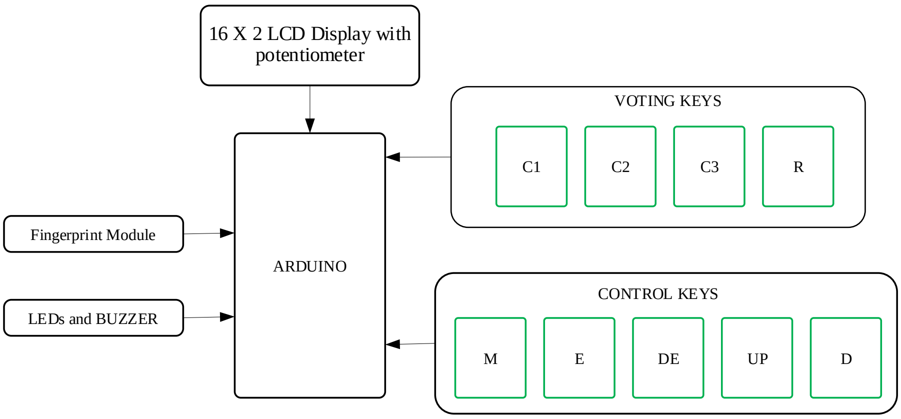


Figure 2: Fingerprint voting system design

C. Arduino UNO

Arduino UNO is the microcontroller that is used in this project. It is built based on ATmega328 in AVR 8 bit RISC architecture. It has 6 analog inputs, 14 digital input output port, a USB connection, 16MHz ceramic resonator, power jack and an ICSP connector. It consists of 1 KB of EEPROM memory which can be read and written. Communication in Arduino UNO is using UART TTL serial communication. Contains 32KB flash memory of which 0.5KB is used as bootloader with a clock speed of 16MHz [1].

Figure 3: Arduino UNO

D. The fingerprint module (R305)

This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through **MAX232** / USB-Serial adapter. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. Fingerprint processing includes two steps: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). *When enrolling, user needs to enter the finger two times*. The system will process the two-time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure [16]. At power on, it takes about 500ms for initialization. During this period, the Module can't accept commands for upper computer. The specifications of the fingerprint module (R305) used in this work are detailed below.

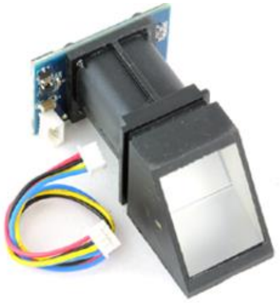


Figure 4: Fingerprint module (R305)

Fingerprint sensor type: Optical , Sensor Life: 100 million times, Static indicators: 15KVBacklight: bright green, Interface: USB1.1/UART(TTL logical level), Communication Baud rate: (9600*N)bps, N=1～12 (default N=6）, Dimension: 55*32*21.5mm, Image Capture Surface: 15—18(mm), Verification Speed: 0.3 sec, Scanning Speed: 0.5 sec, Character file size: 256 bytes, Template size: 512 bytes, Storage capacity: 250, Security level: 5 (1,2,3,4,5(highest)), False Acceptance Rate (FAR) :0.0001%, False Rejection, Rate (FRR): 0.1%, Resolution 500 DPI, Voltage :3.6-6.0 VDC, Working current: Typical 90mA, Peak 150Ma, Matching Method: 1:1 and 1: N, Operating Environment Temperature: -20 to 45° centigrade [4].

E. LCD Display Module

The LCD display panel is used to display status messages and error messages for example, to display the vote casted and also the eligibility of a voter. The most used LCD display type is the **16×2 LCD**, which is so named because; it has 16 Columns and 2 Rows [3]. The LCD can work in two different modes connected to a 5V supply, namely the 4-bit mode and the 8-bit mode. In **4 bit mode** we send the data nibble by nibble, first upper nibble and then lower nibble (a nibble is a group of four bits), so the lower four bits (D0-D3) of a byte form the lower nibble while the upper four bits (D4-D7) of a byte form the higher nibble. This enables us to send 8 bit data. Whereas **in 8 bit mode** we can send the 8-bit data directly in one stroke since we use all the 8 data lines. The 8-bit mode is faster and flawless than 4-bit mode and so it is used in this project. But the major drawback is that it needs 8 data lines connected to the microcontroller.

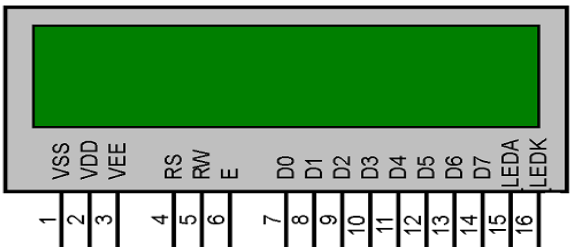


Figure 5: 16 X 2 LCD Display with pins

IV. IMPLEMENTATION, RESULTS AND DISCUSSION

A. Voting Process Explanation

First of all, user needs to enrol finger or voters (in this code max limit of the voter is 25) with the help of push buttons/keys. To do this user need to press ENROLL key and then LCD asks for entering location/ID where finger will be a store. So now user needs to enter ID (Location) by using UP/DOWN keys. After selecting Location/ID user needs to press an OK key (DEL key). Now LCD will ask for placing finger over the finger print module. Now user needs to put his finger over finger print module. Then LCD will ask to remove the finger from finger print module and again ask for placing the finger. Now user needs to put his finger again over finger print module. Now finger print module takes an image and converts it into templates and stores it by selected ID in to the finger print module’s memory. Now voter will be registered and he/she can vote. Now if the user wants to remove or delete any of stored ID then he/she need to press DEL key, after pressing DEL key, LCD will ask for select location means select ID that to be deleted. Now user needs to select ID and press OK key (same DEL key). Now LCD will let you know that finger has been deleted successfully.

Now when user wants to vote then he/she needs to press match key and then buzzer will beep and LED will also glow and LCD will ask for place finger over fingerprint module. Now Arduino will give you three attempts to put your finger. After placing a finger over fingerprint module fingerprint module captures finger image find its IDs is present in the system. If finger ID detected, then LCD will show authorized Voter. It means the user is authorized to vote. And then the system moves to next stage for voting. Now Green LED will glow it means now voter can vote for their candidates by pressing a relected key (from RED bread board in this demonstration). Now if the same voter wants to vote again then the system will show it *'Already Voted'*. Means same voter can't vote again and buzzer will beep for 5 seconds. If any Non-registered user wants to vote, then finger print module will not detect its ID into the system and LCD will show '*No Fingerprint Found'*.

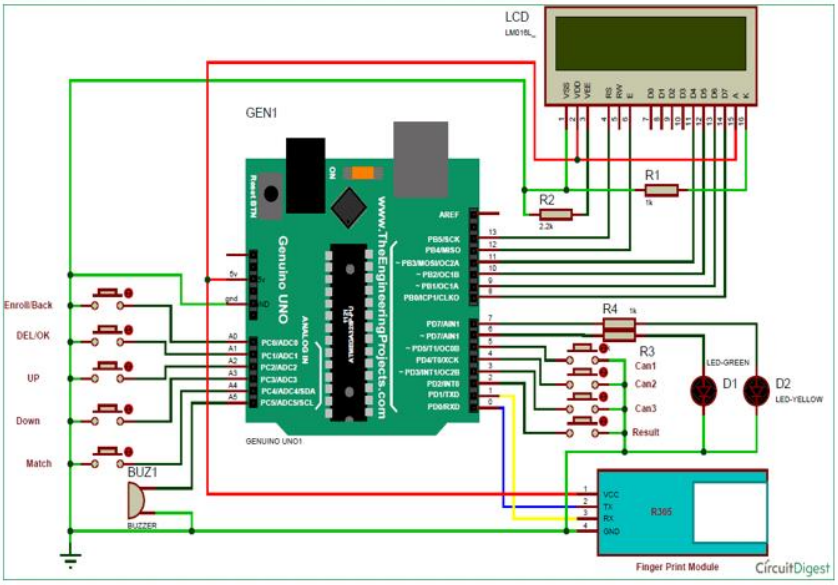


Figure 6: Circuit diagram of Arduino

The entire process for the fingerprint authentication voting system is described below

First the user has to confirm his/her identification before entering. For user identification finger print sensor is used. The user will first put her/his thumb on the sensor. Matching will be done from sensor data base. If match found then access will be granted and if match is not found, the user will need to enrol into the system with the help of push buttons. To do this user need to:

Step 1: Press ENROLL (E) key:

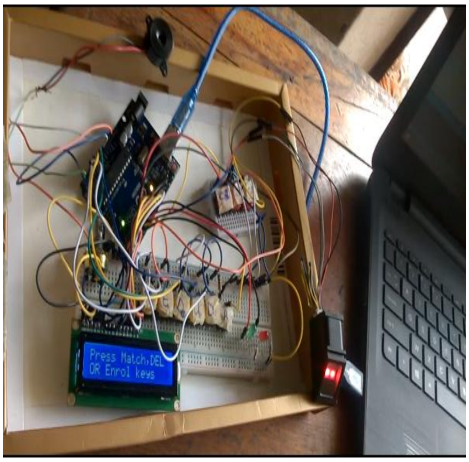


Figure 7: Enroll prompt

Step 2: The LCD will ask for entering location/ID where finger will be a store*:*

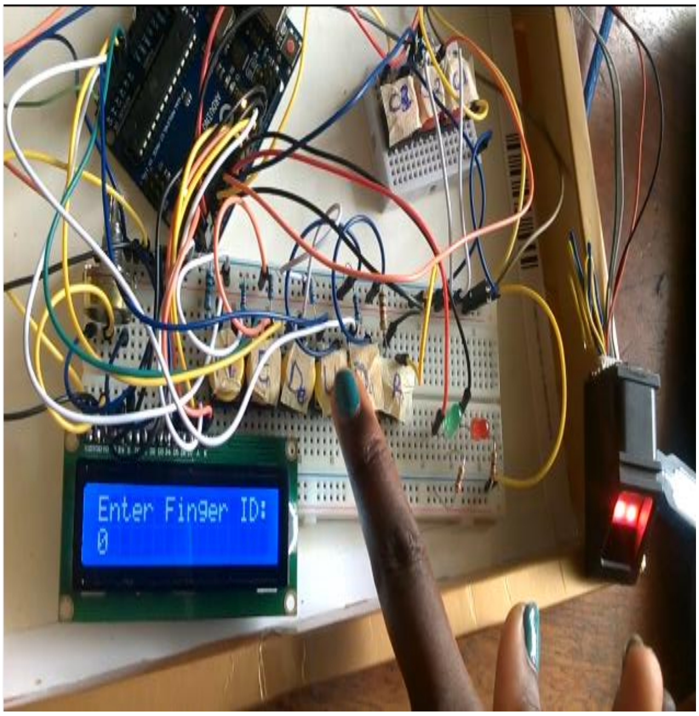


Figure 8: Finger ID

Step 3: Now user needs to enter ID (Location) by using UP /DOWN (D) keys.

Step 4: After selecting Location/ID user needs to press an OK key (DE key). The LCD will ask for placing finger over the finger print module

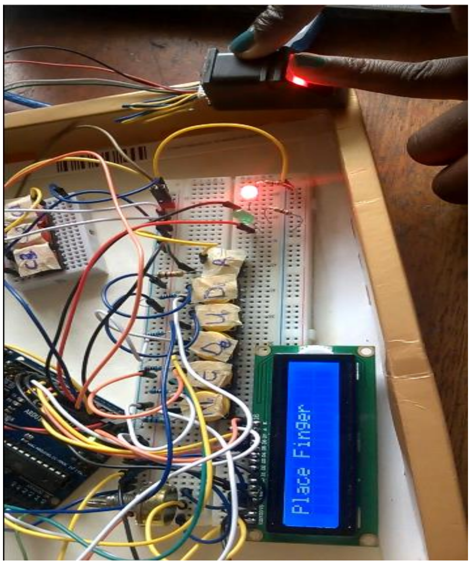


Figure 9: Place finger

Step 5: Now user needs to put his finger over finger print module. Then LCD will ask to remove the finger from finger print module and again ask for placing the finger.

Step 6: User then needs to put his finger again over finger print module. The finger print module will then take the image and convert it into templates and store it with the selected ID in to the finger print module's memory. The voter will be registered and they can vote. By same method all the voters can be registered into the system.

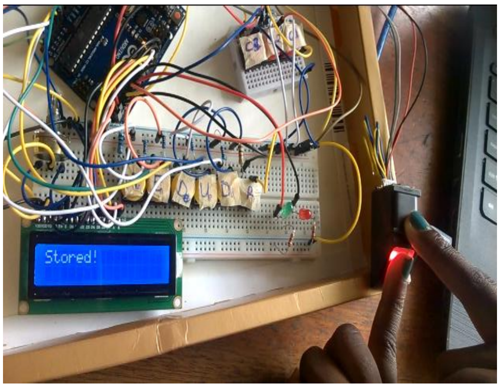


Figure 10: Fingerprint stored

Now when the user wants to vote, they will need to;

Step 7: Press match (M) key and then the buzzer will beep and LED will also glow and LCD will ask the user to place finger over fingerprint module. Now Arduino will give you two attempts to put your finger.

Step 8: After placing a finger over fingerprint module fingerprint module captures finger image and checks if its ID is present in the system. If the finger ID is detected then the LCD will show authorized Voter. It means the user is authorized to vote. And then the system moves to next stage for voting.

Step 9: Now Green LED will glow it means that voter can vote for their candidates by pressing any of the candidate keys (C1, C2 or C3).

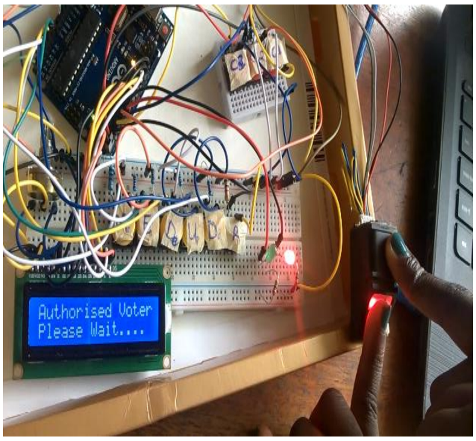


Figure 11: authorized voter

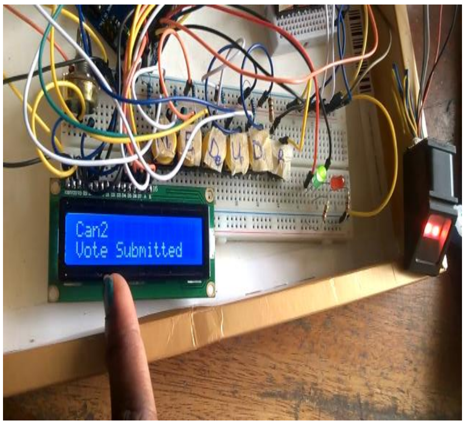


Figure 12: Vote submit

Step 10: If the same voter wants to vote again, the system will display 'Already Voted' on the LCD screen. This means same voter can't vote again and buzzer will beep for 5 seconds.

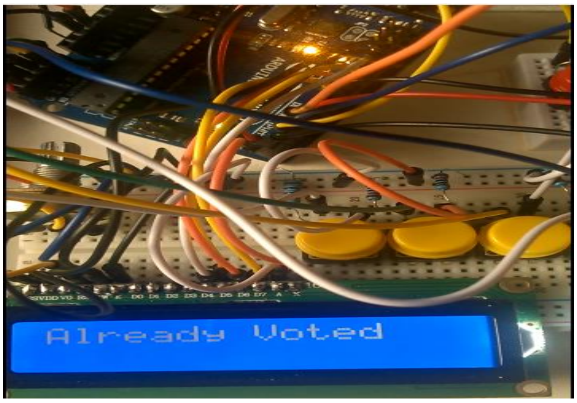


Figure 13: Double vote prevented

Step 11: If any Non-registered user wants to vote then the finger print module will not detect its ID in the system and LCD will show 'Finger Not Found, Try Later

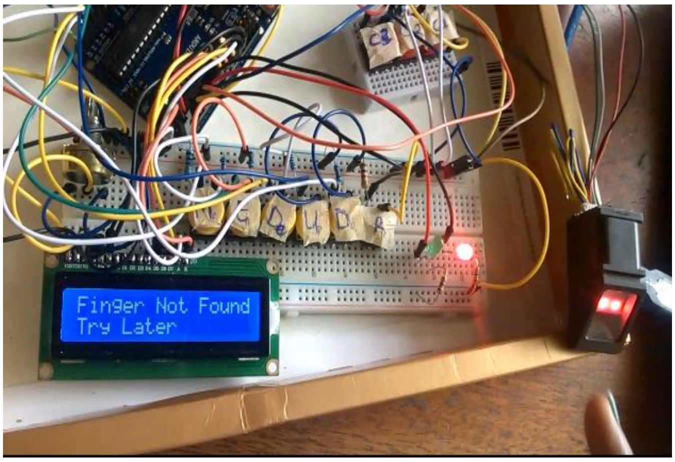


Figure 14: Finger not found

B. Result check

The results of the elections can be checked by the following steps

Step 1: Pressing the Match key

Step 2: The entering the fingerprint with fingerprint sensor

Step 3: And finally, by pressing the Result (R) button

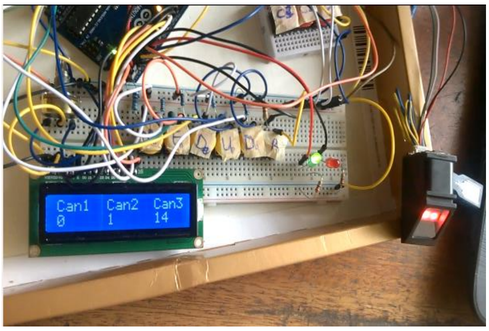
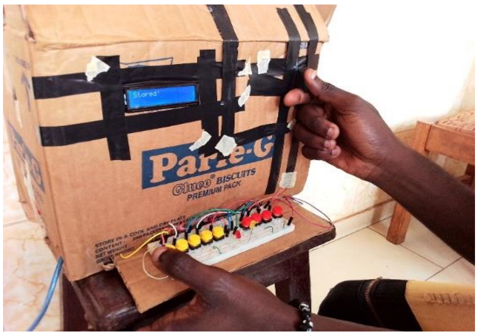
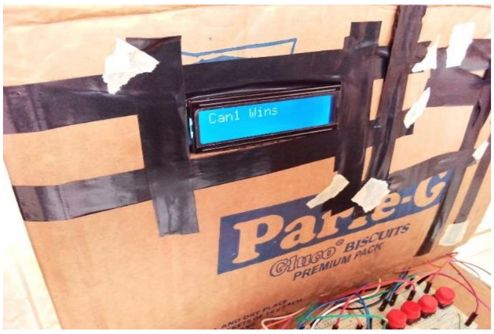


Figure 15: result

The winner of this election is displayed accordingly. This system also provides allowances for a voter to be deleted from the database hence the delete key. This system also provides allowances for a voter to be deleted from the database hence the delete key. Finally, we see on this picture that CANDIDATE 1 has won.





The fingerprint authentication voting system was expected to prevent unauthorized voting and double casting of votes. From the results illustrated from **figures 11** and **12,** these expectations were fully realized.

V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

In conclusion, the positive findings of a fingerprint authentication voting system underscore its potential to enhance electoral processes. By providing a secure and efficient means of verifying voter identity, this technology promotes transparency, reduces fraud, and ensures the integrity of the democratic system. Additionally, the user-friendly nature of fingerprint authentication contributes to increased accessibility, fostering a more inclusive and participatory voting experience. As we embrace technological advancements, the implementation of such systems holds promise for reinforcing the foundations of fair and reliable elections.

B. Future Scope

This work was implemented with a limited number of eligible voters of 25 but the fingerprint module can take up to about 256 IDs in its database [1]. Hence this project can be used in a simple class election with just one fingerprint module. In the case where a much larger number of voters is required like during presidential elections, many more fingerprint modules will be required. And the number of candidates can also be increased. An online database can also be created and integrated into the system so that it can be readily accessible to all users regardless their location. This system can be upgraded in a way as to RESET, in case the electoral period is over and the next is to begin.

REFERENCES

[1] M. Odden, “BIOMETRIC CRISIS: LEGAL CHALLENGES TO BIOMETRIC IDENTIFICATION INITIATIVES.” [Online]. Available: https://searchsecurity.techtarget.com/definition/biometrics

[2] M. Smith and S. Miller, “The ethical application of biometric facial recognition technology,” AI Soc, vol. 37, no. 1, pp. 167–175, Mar. 2022, doi: 10.1007/s00146-021-01199-9.

[3] L. H. Adamu and M. G. Taura, “Embryogenesis and Applications of Fingerprints- a review,” International Journal of Human Anatomy, vol. 1, no. 1, pp. 1–8, Jan. 2017, doi: https://doi.org/10.14302/issn.2577-2279.ijha-17-1539.

[4] W. Zafar, T. Ahmad, and M. Hassan, “Minutiae based fingerprint matching techniques,” 17th IEEE International Multi Topic Conference 2014, pp. 411–416, 2014, [Online]. Available: https://api.semanticscholar.org/CorpusID:27847944

[5] A. C. S. Sheela and G. F. Ramya, “E-voting system using homomorphic encryption technique,” in Journal of Physics: Conference Series, IOP Publishing Ltd, Apr. 2021. doi: 10.1088/1742-6596/1770/1/012011.

[6] V. Baraskar, “FINGER PRINT BASED BIOMETRIC AUTHENTICATION SYSTEM FOR ATM SYSTEM,” Asian Journal For Convergence In Technology (AJCT) ISSN -2350-1146, vol. 4, no. I, Apr. 2018, [Online]. Available: https://asianssr.org/index.php/ajct/article/view/502

[7] J. Liu, T. Han, M. Tan, B. Tang, W. Hu, and Y. Yu, “A Publicly Verifiable E-Voting System Based on Biometrics,” Cryptography, vol. 7, no. 4, 2023, doi: 10.3390/cryptography7040062.

[8] N. B. Kintu, A SECURE E-VOTING SYSTEM USING BIOMETRIC FINGERPRINT AND CRYPT-WATERMARK METHODOLOGY. [Online]. Available: https://www.researchgate.net/publication/329116213

[9] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, “Blockchain-Based E-Voting Systems: A Technology Review,” Electronics (Basel), vol. 13, no. 1, p. 17, Dec. 2023, doi: 10.3390/electronics13010017.

[10] R. V. Adiraju, K. K. Masanipalli, T. D. Reddy, R. Pedapalli, S. Chundru, and A. K. Panigrahy, “An extensive survey on finger and palm vein recognition system,” Mater Today Proc, vol. 45, pp. 1804–1808, 2021, doi: https://doi.org/10.1016/j.matpr.2020.08.742.

[11] M. Nalayini, K. Vishnupriya, A. Dhivyabharathi, and H. Yuvapriya, “Biometric based Mobile Voting Application,” Journal of Information Technology and Digital World, vol. 5, no. 2, pp. 159–168, Jun. 2023, doi: 10.36548/jitdw.2023.2.006.

[12] Z. Acemyan, P. Kortum, and F. L. Oswald, “The Trust in Voting Systems (TVS) Measure,” International Journal of Technology and Human Interaction, vol. 18, no. 1, 2022, doi: 10.4018/IJTHI.293196.

[13] Lancelot Miltgen, A. Popovič, and T. Oliveira, “Determinants of end-user acceptance of biometrics: Integrating the ‘big 3’ of technology acceptance with privacy context,” Decis Support Syst, vol. 56, no. 1, pp. 103–114, Dec. 2013, doi: 10.1016/j.dss.2013.05.010.

[14] M. Kumar, “Fingerprint Recognition System: Issues and Challenges,” Int J Res Appl Sci Eng Technol, vol. 6, no. 2, pp. 556–561, Feb. 2018, doi: 10.22214/ijraset.2018.2080.

[15] S. Zhao, D. Ge, J. Zhao, and W. Xiang, “Fingerprint pre-processing and feature engineering to enhance agricultural products categorization,” Future Generation Computer Systems, vol. 125, pp. 944–948, 2021, doi: https://doi.org/10.1016/j.future.2021.07.005.

[16] T. Keerthi, M. C. Chinnaiah, A. Kumari, P. Asharani, D. Harikrishna, and G. Divyavani, “Real Time Implementation of Biometric-based EVM System for Distinct Verification,” Procedia Comput Sci, vol. 230, pp. 407–416, 2023, doi: https://doi.org/10.1016/j.procs.2023.12.096.