Voter ID Card and Fingerprint-Based E-voting System

Rajesh Kannan Megalingam, Gaurav Rudravaram, Vijay Kumar Devisetty, Deepika Asandi, Sai Smaran Kotaprolu, and Vamsy Vivek Gedela

Abstract Voting is a fundamental right given to every citizen of a democratic country, with a minimum age requirement set by the respective countries. As such, one would expect the procedure for voting to be on the cutting edge of technology in terms of security and adhere to the highest standards. This paper proposes and discusses a method of E-voting based on dual-factor authentication in the form of unique identification (UID) number and the fingerprint of the voter for verification purposes. An algorithm for fingerprint recognition is also discussed in the paper along with the efficiency of the algorithm in CPUs of different computing powers. We created a website with the proper focus on securing the personal data of the constituents while also making it legible for the election officials to keep track of the progress of the election and avoid dual/multiple vote casting. The additional security provided by biometric authentication ensures that the system we propose meets the safety standard set by the Information Technology Act, 2000. Based on the experiments and results, we believe that the proposed anti-fraud E-voting system can bring confidence in voters that their vote is secured.

R. K. Megalingam (✉) · G. Rudravaram · V. K. Devisetty · D. Asandi · S. S. Kotaprolu
Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India
e-mail: rajeshm@am.amrita.edu

G. Rudravaram
e-mail: gauravrudravaram@am.students.amrita.edu

V. K. Devisetty
e-mail: devisettyvijaykumar@am.students.amrita.edu

D. Asandi
e-mail: asaideepika@am.students.amrita.edu

S. S. Kotaprolu
e-mail: ksaismaran@am.students.amrita.edu

V. V. Gedela
Department of EE, University of Cincinnati, Cincinnati, OH, USA
e-mail: gedelavv@mail.uc.edu

S. Smys et al. (eds.), *Inventive Computation and Information Technologies*, Lecture Notes in Networks and Systems 336, https://doi.org/10.1007/978-981-16-6723-7_8

Keywords Electronic voting machine (EVM) · Fingerprint recognition · Unique identification (UID) · Hashing · Secure voting · Authentication · Biometric matching system (BMS)

1 Introduction

The system of E-voting has been introduced in many countries and has been in use to date by most of these countries. E-voting systems have been observed to have more advantages than the traditional paper-based system in aspects such as the counting of votes time period, and the mistakes in counting votes can be drastically reduced using the E-voting system. The problem the E-voting system lacks is transparency and false voting. The problem of being non-transparent can be rectified by using voter-verified paper ballots (VVPBs); this device prints the vote that has been cast and displays it to the voter, and through this, the vote cast can be verified. In order to prevent malpractices like false voting (voting using the other citizen's data) can be reduced by introducing a dual-factor authentication system to verify the voter before the vote has been cast.

AADHAR card consists of a 12 digit number that is unique to each Indian citizen or passport holder of India. It even consists of information, biometric and demographic data of the respective residents of India. The Unique Identification Authority of India (UIDAI) is responsible for collecting the data. The UIDAI was established by the government of India in January 2009. This research work proposes a voting system based on UID card and fingerprint authentication to enable a safe and transparent election process. While this process of using the AADHAR card is relevant only in India, the same method of storing the citizen's biometrics in a government database and linking to a unique identification card can be applied in other countries as well to imitate similar results.

Biometric security methods are proven to be more secure than the use of one-time password (OTP)-based or PIN-based security methods. The biometric security methods include fingerprint scanning, where a person is identified based on his/her fingerprints. As the fingerprints are unique to each individual, only the respective person can access the system whose fingerprint matches the one in the database. The proposed system practices dual-factor authentication, that is, the verification of the UID Card and the fingerprint of the voter, and does not allow a constituent to cast more than one vote because it automatically updates the status of the vote of a constituent on a dynamically rendered website created by us.

Our proposed system authenticates a voter based on the UID number and the voter's fingerprints. If the authentication at any of the levels fails (the UID number or the fingerprints won't match with any of the data present in the pre-enrolled database), then the voter will be denied access to voting. This process can prevent other people from casting false votes, as the voter needs to scan their fingers to pass the second level of authentication. Once a voter passes both the levels of security, then the voter

can vote. Then, the vote is updated in the database and will not allow a second vote, hence preventing a person from voting more than one time.

The website we designed can be personalized by the government or third-party contractors to be made to enlighten the average citizen on the process and security of the voting system. The website is also connected to a database and renders a complete list of the constituents and their status of voting, both of which are encrypted in a local database by hashing the data in it to secure them from the prying eyes. Hashing is used to map data of any size to a fixed length. This is called a hash value. Encryption is a two-way function whereas hashing is a one-way function. While it is technically possible to reverse-hash something, the computing power required makes it unfeasible. The election official can access this list by using the credentials issued to him/her, and it is up to their discretion whether or not to make this list public. In this way, the proposed system in this research paper ensures a safe and reliable election procedure with the utmost transparency so as not to raise any questions about rigged elections or false votes.

2 Problem Statement

The centerpiece of any successful democracy is the peaceful transition of power from one government to another. And this is only made possible by the process of voting. As the most powerful non-violent tool a citizen has in a democracy, the process of voting has to be without any flaws. There should not be any questions about the safety or reliability of the voting system in the mind of any citizen or constituent. While technology has greatly impacted every aspect of our life, the process of voting has, unfortunately, not undergone many changes since it was first proposed. There are 167 democratic countries in the world out of which around 34 countries have some sort of electronic voting system. Among these countries, only India, despite its population of 1.36 billion, has a 100% electronic voting system. When dealing with large democracies like India, the efficiency of EVMs during the voting process becomes extremely important. The 2019 parliamentary elections in India had a voter turnaround of 67%, nearly 900 million registered voters across 542 parliamentary constituencies came out to vote. Some countries still rely on ballots to carry forward the voting procedure. The ballot system has many disadvantages such as long waiting lines, questions about authenticity of the ballots due to the votes not being transparent enough as there is no way for an individual to be sure the candidate they voted for received the vote with absolute certainty. To avoid questions about authenticity and safety of the voting process and to ensure the safety of the election officials, we present a new idea for implementing the process of voting.

3 Related Works

Paper [1] proposes a system which uses a biometric authentication system and additionally provides a facility to users to cast a vote using mobile phones. The first way is for the smartphone users, one-time password (OTP) is used. For other users who do not have smartphones, biometric methods such as fingerprint recognition is used as authentication. The main objective is to cast a vote from anywhere anytime. A large population of people is not aware of using smartphones even though they have one and it will be a huge task to educate voters. In the voter ID card and fingerprint-Based E-voting system, a person is allowed to vote if the fingerprint of a person is matched with his/her fingerprint stored in the database. No other electronic devices are needed for the voter to vote. A system which takes complete control over child vaccination status and monitors child vaccination schedules is proposed in paper [2]. It uses the fingerprint of the child from the database and performs fingerprint processing and classifies it. In e-vaccination, the fingerprints of the infants are taken, the accuracy is hard to verify. This drawback can be rectified by considering the fingerprints of their parents/guardians and applying the same system as discussed in this paper. Paper [3] takes measures to allow the voter to vote only if the voter logs into the system by using the right credentials which are generated by merging the two sets of credentials in the form of black and white dotted images generated by the computer and encrypted using a video cryptography scheme. Accessibility or voter education—Many people are not aware of how to use an email and how to log in and this gives rise to hackers. In the voter ID card and fingerprint-based E-voting system, there is no need for the voter to log into a system, only the voter's fingerprint is required. Paper [4] proposes a multifaceted online e-voting system. The requirements embedded in the design of the respective system permits well-secured authentication processes for the voter using combined simple biometrics. There are possible attacks such as: replay attacks, denial-of-service and session hi-jack which can be minimized by the use of the system proposed in this paper which uses a cloud-based database encrypted through salting and hashing.

A voting system based on an advanced RISC machines (ARM) processor and fingerprint sensor is proposed in the research paper [5]. The authors have used a simple liquid crystal display (LCD) display for user interface and a keypad for entering the information about the voters. This suffers the drawback of limited constituent enrolling due to limitations of the sensor memory. The research paper [6] give us an idea on how to proceed with the fingerprint recognition by providing an in depth explanation about two different image processing algorithms namely, scale invariant feature transform (SIFT) algorithm which is used for local feature matching and the fast library for approximate nearest neighbors (FLANN) which is applied to match the query image and reference image in dataset. In paper [7], the authors have implemented a secured platform for remote health monitoring services. They have used a Raspberry Pi to keep track of the health data. For security purposes, they came up with a password authentication key exchange mechanism based on hashing and zero-knowledge password proof. Paper [8] proposes a women security system

based on GPS modules and foregoes the need of a smartphone instead opting for a completely portable system based on microcontroller. The system communicates via Wi-Fi and transmits data in real time.

Paper [9] proposes a voting mechanism which identifies the voter based on his/her fingerprint image taken from a fingerprint sensor. In this model, encryption of the database is not done. In our model, the database encryption is done by hashing and salting. Paper [10] proposes a dual authentication one using iris recognition and the other is comparing fingerprints. The comparison technique used for iris recognition is hamming distance and for comparing fingerprints is Euclidean distance. This technique is not optimum for voting because the time taken for dual authentication is higher. In paper [11], the authors propose a model aimed at retrieving images from the database based on the context in the given image. The major steps involved are object recognition and image retrieval. Object recognition includes training phase and is done using SIFT, SURF (speed-up robust features), HOG (histogram of oriented gradient), and color Histogram. In image retrieval, similar images are selected based on rank of similarity. Paper [12] proposes a method in which voter has to place his/her voter ID which has a unique radio-frequency identification (RFID) tag. If the tag matches from the one in database, then the voter must verify his/her fingerprint. If the fingerprint verification is successful, the voter is eligible to cast his/her vote.

Paper [13] focuses more on the implementation of the EVMs, making the voting process more transparent. It also introduces the term 'Voting Status Flag' which plays a role in the authentication. In order to prevent malpractices during the election process, Kerberos (computer network protocol) is used. Our proposed system uses a security system that verifies the voter before casting the vote. We have even designed a website which improves the user interface. The EVM proposed in Paper [14] is built using LPC2148 which is the core of the ARM-7 processor. Here in the first stage of authentication, the card given is scanned using RFID and later the fingerprints are taken. Using RFID tags might become expensive and less secure while dealing with a large population, and considering this factor, our system uses a fingerprint sensor as the second stage, which is more secure than using RFID tags. In Paper [15], the authors explained about the fingerprint recognition algorithms. They explained the enrollment, matching, and extracting phases in the fingerprint algorithm. In our proposed model, the run-time of the fingerprint recognition algorithm can be reduced as we will be using 1:1 matching, using the unique identity number of each voter. Paper [16] gives more insight into fingerprint recognition. Biometric authentication systems has two modes, enrollment and recognition. The identity of the fingerprint is based on invariance and singularity. This paper discusses the process of recognition of fingerprints using image preprocessing, feature extraction stages etc.

Paper [17] states the advantages of using biometric methods such as fingerprint recognition as a mode of authentication. It even gives information about the method (Chaotic Arnold transform) used for recognizing the fingerprints. Our proposed system has a dual-security system where we take the unique identification number of a voter first, then the fingerprint of the individual will be compared with the one from the database with the ID entered initially. This will reduce the run-time of the algorithm. Paper [18] deals with the transparency of the E-voting system and

the advantages of E-voting. It provides various methods such as using voter-verified paper ballots (VVPBs) which helps the voter to verify the vote casted. In our proposed system, we introduced a biometric authentication level (fingerprint sensor) which can reduce malpractices such as false voting and multiple voting.

4 System Architecture

In the system we propose as shown in Fig. 1, the constituent first has to enter his voter ID number (the number assigned to him/her by the government) into a keypad connected to a processor. We have tested two processors for this project, namely Broadcom BCM2711 and Intel Core i7-9750H. The processor then verifies the number with the list of UID numbers stored in the external database and finds the related fingerprint based on this unique identification number in the form of voter ID. After successfully finding the number and verifying its status of voting, the fingerprint module is activated and asks the constituents to verify their fingerprint with the one stored in its database.

We have written a fingerprint algorithm which verifies whether or not they are matching and sends a message to the microcontroller to activate the ballot box if the fingerprints are matching. Once the microcontroller is activated after the verification process is completed, the constituent can cast their vote with the help of the ballot box. Once the constituent selects their candidate, the ballot box immediately deactivates and informs the microcontroller. The microcontroller in turn sends this information back to the processor which updates its database for preventing the constituent from voting again. The updated database is rendered in real time in a website under secure authentication which will be handled by the government either by establishing secure

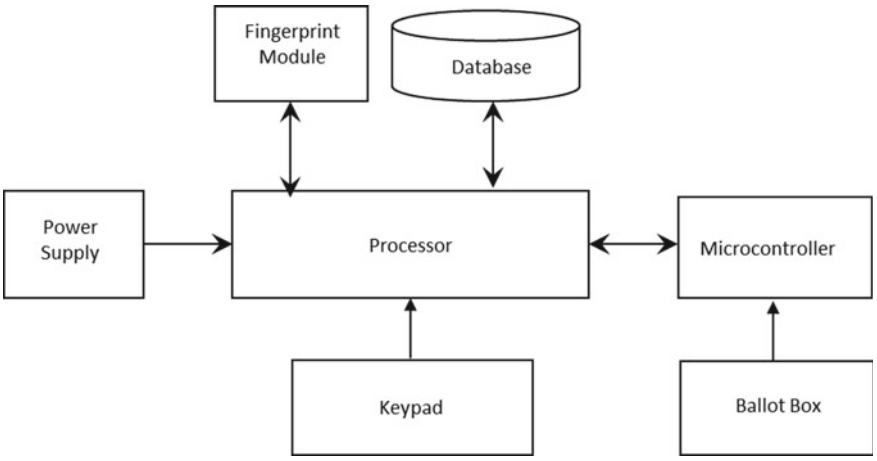

Fig. 1 System architecture

servers for handling the data influx or by hosting the website on a trusted third-party server system. This system of using a duality of processor and microcontroller can be made simpler by using a micro-processor such as Raspberry Pi, but it was decided against that due to drawbacks which we will discuss later in the paper.

5 Design and Implementation

5.1 System Flow Architecture

Figure 2 shows the control flow of the system from the point of input entry to the point of termination. There are two levels of authorization to be passed in order for the voter to cast his/her vote. The first authorization level includes the verification of the voter ID which can be inputted through a keypad. Once this level is cleared, the fingerprint module accepts the fingerprint of the voter. The verification of the

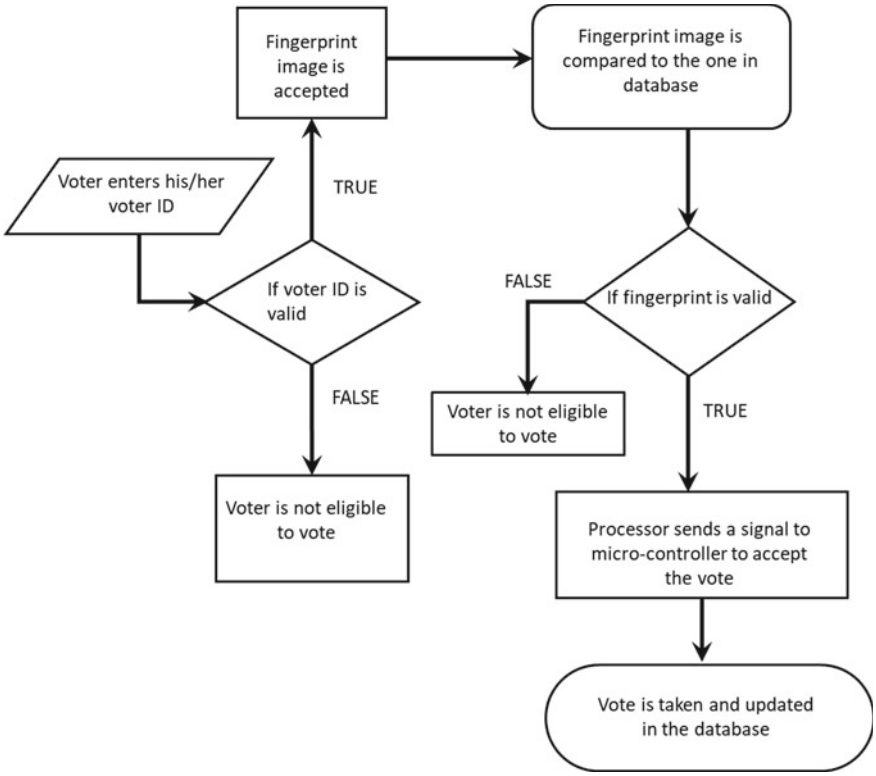

Fig. 2 System flow architecture

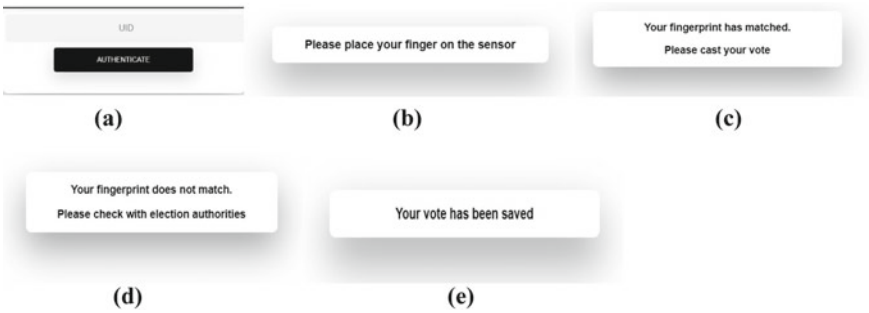

Fig. 3 User interface with respect to system flow outcomes

voter's fingerprint comes under the second level of authorization. After the voter is successfully verified to be legitimate through both their voter ID and fingerprint, a signal is sent to the microcontroller which accepts the vote and sends the input back to the processor to be updated in the database.

Figure 3a is the main page where the voter has to enter their voter ID. If the voter ID is valid, then Fig. 3b is rendered in the webpage prompting the voter to give their fingerprint as the input through the fingerprint sensor. When the voter fingerprint image is taken, it is compared to the one in database. If the fingerprint is matched Fig. 3c is rendered in the webpage, if the fingerprint does not match Fig. 3d is rendered in the webpage. After the vote is cast, Fig. 3e is rendered and the vote is added to the database.

5.2 Hardware Used

Processor For the experimentation process, we have used two processors. We will discuss the advantage and disadvantage of both in the Experimentation and Results section.

i. *Broadcom BCM2711.* This is the processor used in Raspberry Pi 4 and uses a 1.5 GHz 64-bit quad-core Arm Cortex-A72 CPU.
ii. Intel Core i7-9750H. This is a 6 core, 12 threaded CPU with a base frequency of 2.6 GHz and Max Turbo frequency of 4.5 GHz.

Fingerprint-Sensor R307-TTL UART The R307 Fingerprint Module is a sensor that is used to scan fingerprints. It even includes transistor–transistor logic (TTL) and universal asynchronous receiver transmitter (UART) interfaces. The fingerprint data can be stored in the module and can be configured as 1:1 mode or 1: N mode for authentication. 1:1 matching is when a person uses either 'Card + Fingerprint' or 'User ID + Password' mode of authentication. Initially, the data (such as User ID) is entered, and once the data with the respective ID is found, it is matched

with the second input (such as the fingerprint). 1: N authentication is more user-friendly as no specification is needed. In this method of authentication, using the data entered by a person (like a fingerprint), one template from a list of up to a thousand pre-enrolled templates is picked. A 3.3 V or 5 V microcontroller can be directly interfaced using the fingerprint module. In order to create an interface with a PC serial port, a level converter like MAX232 is needed. R307 Fingerprint Module consists of a high-performance fingerprint alignment algorithm and a high-speed DSP processor. It even has other hardware which facilitates its performance, image processing, template storage, and other functions. Since the fingerprint sensor R3-07 is a module with a TTL UART interface, it is connected with a USB-TTL UART module to communicate with the computer. Interfacing with fingerprint sensor is achieved by using pyfingerpint library; this library allows the sensor to interface with Raspberry Pi and other Linux-operated machines and send data to them.

Microcontroller Arduino Uno is a development board based on the ATmega328p microcontroller. It has 20 general purpose input/output pins (GPIO), out of which 14 are digital input/output pins (6 pins are used as PWM output pins) and the remaining pins are 6 analog input pins. It includes a USB connection to program the microcontroller, a power jack, an in-circuit serial programming (ICSP) and a 16 MHz ceramic resonator. Arduino is connected to the computer via USB, and it is interfaced using pyserial library in python; this allows the processor to send or receive data from Arduino through a serial port.

Hardware requirements The hardware requires no GPU. It is recommended to have a minimum memory of 2 GB and CPU of base frequency 1.5 GHz.

Interfacing the Various Components The fingerprint sensor R3-07 is a module with a TTL UART interface, and it is connected with a USB-TTL UART module to communicate with the computer. Interfacing with fingerprint sensor is achieved by using pyfingerpint library. This library allows the sensor to interface with Raspberry Pi and other Linux-operated machines and send data to them. Arduino is connected to the computer via USB, and it is interfaced using pyserial library in python; this allows the processor to send or receive data from Arduino through a serial port. The hardware requires no GPU. It is recommended to have a minimum of 2 GB RAM.

5.3 Fingerprint-Recognition Algorithm

As we can see from Fig. 4, after downloading the fingerprint image from using the inbuilt library inside the sensor R3-07 fingerprint sensor, we store it in a separate database.

The fingerprint algorithm is explained in the following steps. We apply the contrast-limited adaptive equalization (CLAHE) algorithm from the opencv2 library in python. CLAHE is a variant of adaptive histogram equalization which takes care

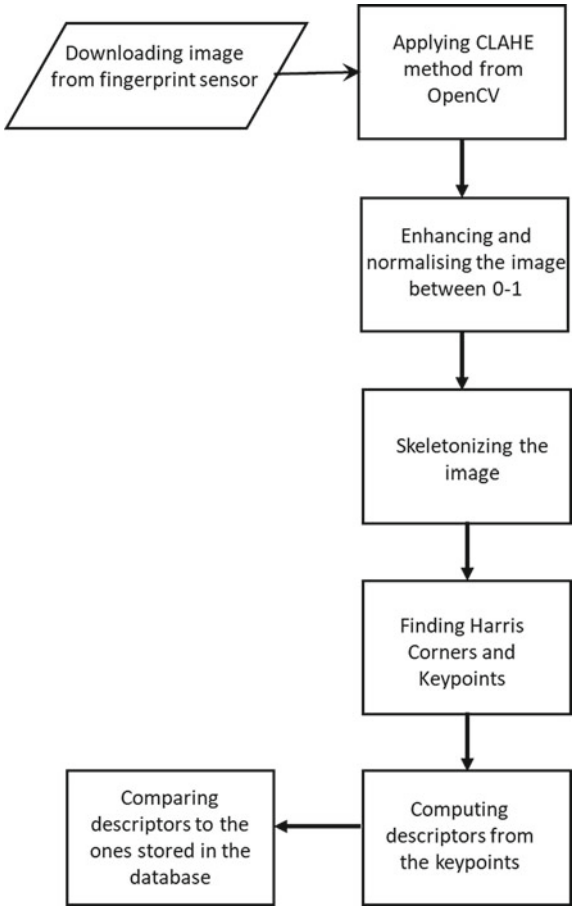

Fig. 4 Algorithm for fingerprint recognition

of over-amplification of contrast. It will operate by selecting small regions of an image, the respective region is called tiles. The surrounding tiles are later combined using bilinear interpolation to remove artificial boundaries. Applying CLAHE to our original images equalizes it and improves its contrast. We then proceed to enhance the image. The image enhancement part of the algorithm draws heavy influence from [17] and improves the overall accuracy of the algorithm.

This enhanced image is further normalized and skeletonized. Skeletonization reduces the image into 1-pixel wide representation. In 1-pixel wide representation, the value of the pixel is either 0 or 1 indicating whether the pixel corresponds to the foreground of the image or background of the image. This is useful for feature extraction. The next part includes extracting corners and inner features of the image using the Harris Corners method. The final part of the algorithm includes extracting the key points of the image and computing their descriptors using oriented fast and rotated (ORB) which is a fast-robust feature detector in the cv2 library.

5.4 Software Used

Fingerprint-Recognition For the fingerprint recognition algorithm, we used Python because of its ease of coding as well as fast prototyping. Python is open source and can be integrated with Web frameworks easily which is very important for this project.

Backend We have used Node.js for handling all the data and event listeners since its processing speed is very fast as compared to other Web frameworks as it is an event-based model. Non-blocking input/output and asynchronous request handling which is a unique feature of Node.js makes it capable of processing requests without any delays.

Database As for the database we have picked MongoDB because it is very easy to integrate with Node.js. It is based on document-oriented storage and handles big data much more efficiently.

Simulation Environment The proposed model has been simulated in a Linux environment. We used the following python libraries: Numpy—1.17.3, OpenCV—4.5.1.48, Scikit image—0.18.1, Scipy—1.6.0, Pandas—1.22, pyfingerprint—1.5 while developing the fingerprint comparing algorithm.

6 Experiment and Results

6.1 Testing the Images for Fingerprint Recognition

All the experiments mentioned below were conducted in lighting conditions comparable to natural conditions and are subject to change based on the sensor used. The algorithm is performed on several types of images, original image, gray scaled image, and enhanced image. The results were accurate when enhanced image is used. So we applied the image enhancement algorithm proposed in [17] which can improve the clarity of ridge and furrow structures based on the local ridge orientation and ridge frequency estimated from the input images. The algorithm also recognizes the unrecognizable corrupted regions and removes them from further processing. Figure 5a, c represent the original fingerprint and Fig. 5b, d represent their enhanced images respectively. An important point to be mentioned here is that because the R3-07 is an optical-based fingerprint sensor, the pressure on the surface of the sensor is a crucial factor in ensuring that the image is stored properly and can be verified in detail. After the image enhancement part was successful, we moved on to comparing the fingerprint images without much difficulty. While it is true that each fingerprint is unique, there are similarities between any two pairs of fingerprints in the manner of the whorls or ridges that make up the fingerprint.

Figure 6 shows that the number of descriptors (descriptors describe the elementary characteristics of an image such as shape, color, and texture) matching when the same

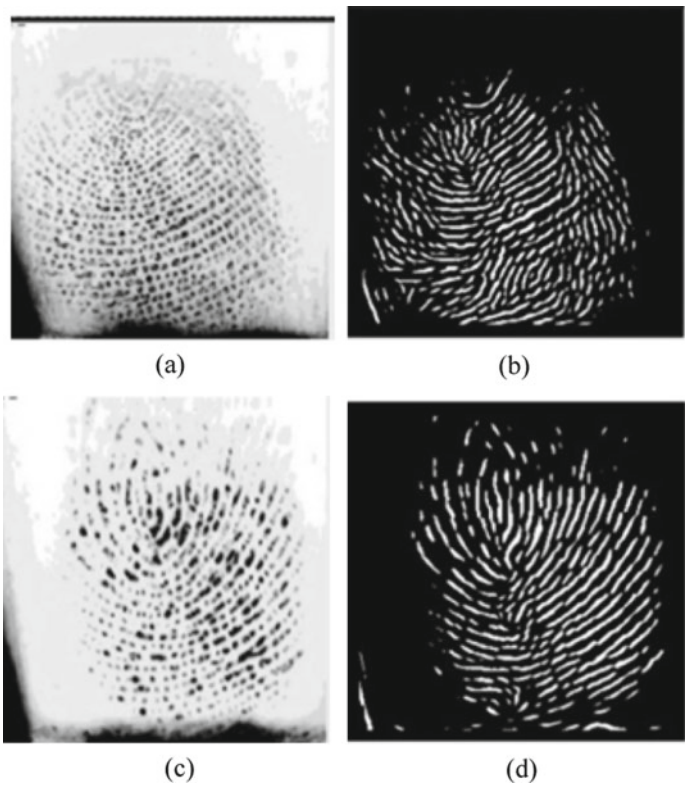

Fig. 5 Comparison of original image versus enhanced image

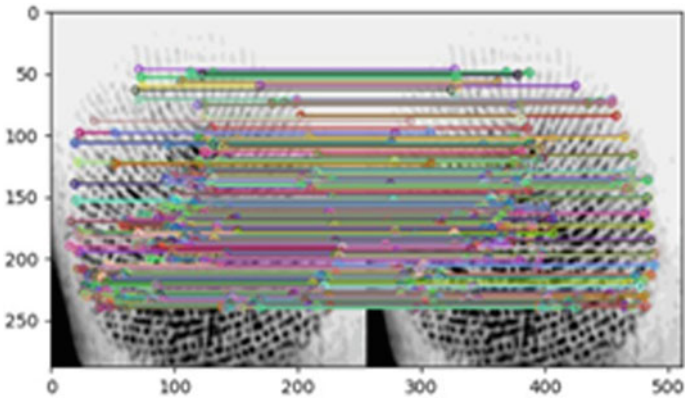

Fig. 6 Comparing the same fingerprint

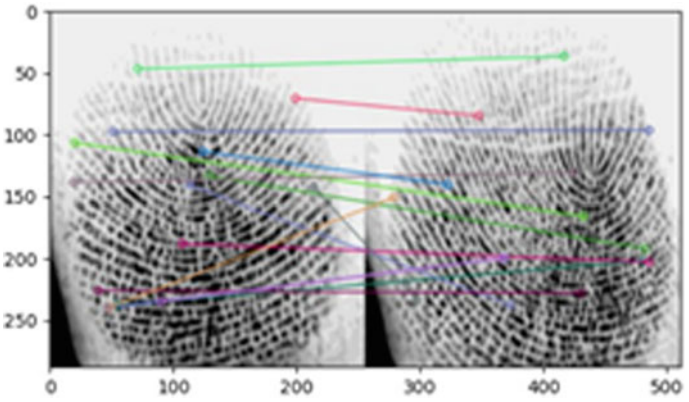

Fig. 7 Comparing different fingerprints

fingerprint is provided as input is very high. Figure 7 shows that although the number of descriptors matching for different fingerprints is very low, it is not necessarily zero. Therefore, in order to account for the small number of matching descriptors in unique fingerprints, we tried out the algorithm extensively on many images and set a threshold of '33' in the algorithm which detects whether the number of matching descriptors is enough to validate the fingerprint or not.

6.2 Comparison of Different Processors

Since we are not necessarily using the inbuilt library for the sensor but instead running our own algorithm, we tested the run-time of the fingerprint recognition algorithm on two different processors, namely the Broadcom BCM2711 and the Intel Core i7-9750H.

Table 1 shows that the average run-time for comparing images in Broadcom BCM2711 processor is approximately 33.45 s, while the average time taken by Intel Core i7-9750H processor is approximately 10.26 s as shown in Table 2. Clearly, the

Table 1 Run-time in broadcom BCM2711 processor

Input	Time taken for comparison (Seconds)
Matching fingerprints set 1	34.6
Matching fingerprints set 2	32.72
Matching fingerprints set 3	35.2
Unique fingerprints set 1	31.29
Unique fingerprints set 2	34
Unique fingerprints set 3	32.9

Table 2 Run-time in Intel Core i7-9750H processor

Input	Time taken for comparison (Seconds)
Matching fingerprints set 1	10
Matching fingerprints set 2	10.8
Matching fingerprints set 3	10.8
Unique fingerprints set 1	9.8
Unique fingerprints set 2	9.8
Unique fingerprints set 3	10.1

advantage with the Intel processor is superior run-time, but it is not very cost efficient. The main advantage with the Broadcom BCM2711 processor is that it comes fitted into a Raspberry Pi model which can make the voting machine far more portable and accessible but at the major cost of efficiency and much slower run-times. While it is up to the personal discretion about which processor to use, in this work we proceed with the Intel Core i7-9750H processor for the reasons discussed earlier.

Figure 8 shows a basic model of the EVM system built for testing purposes. The fingerprint sensor R3-07 is located at the far left and connected to the Broadcom BCM2711 processor. The Arduino communicates with the processor once the fingerprint is verified and takes input from one of the push buttons. The time delay in communication with the Arduino and the server running in the background by Node.js

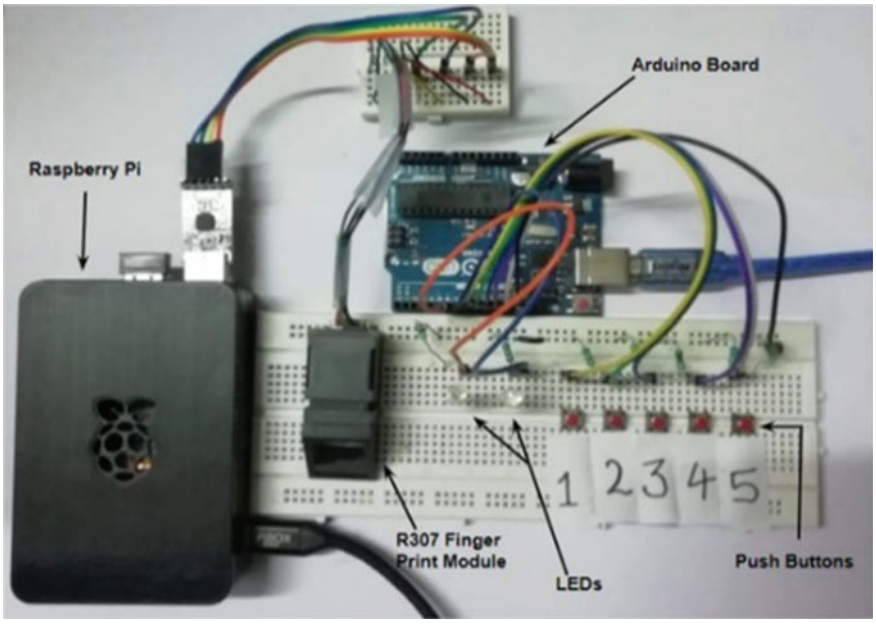

Fig. 8 Model-1 prototype of E-voting system using the broadcom BCM2711 processor

ID	Name	Gender	Status of Voting
1	voter 1	Male	Casted
2	voter 2	Male	Casted
3	voter 3	Male	Pending
4	voter 4	Male	Pending
5	voter 5	Male	Pending
6	voter 6	Male	Pending
7	voter 7	Female	Pending
8	voter 8	Female	Pending
9	voter 9	Female	Pending
10	voter 10	Female	Pending

Fig. 9 Status of votes rendered by server

is set to about 500 ms to ensure there is no data overlap. Once the Arduino detects that any of the buttons is pressed it sends a message to the server and stops communication immediately.

Salting is an apprehension that typically refers to password hashing. It is an exclusive value that can be added to the end of the password to create a different hash value. The hash value can be any random or personalized character that adds an additional layer of security to the hashing process, distinctively against brute force attack. Once the Arduino communicates with the server, the server immediately updates the database with the status of the voter and the vote cast. To prevent malpractice, the server is secured by many rounds of salting followed by hashing. The information in the database is updated in real time by the server and displayed as a list in a webpage as shown in Fig. 9 so that the election officials can keep track of who has cast their vote already in case any disputes arise.

7 Conclusion

In this work, we presented a voter ID and fingerprint-based E-voting system based on authentication in the form of voter identity card and fingerprint of the constituent. The need for such a multi-authentication system was described in the motivation section. The related works section discussed in detail about the existing research work related to secure E-voting systems and how our proposed system compares with the existing systems. We also presented the architecture of the proposed system, both hardware and the software. The process of identifying fingerprints and its results are explained in the experiments and results section along with the information in the database that is updated in real time by the server when the voter casts the vote. Based on the experiments and results, we believe that the proposed anti-fraud E-voting system can bring confidence to voters that their vote is secured.

We have some suggestions for the successful adoption of our proposed system by any agency. The website can be designed by the government through third-party developers in order to obtain a better user interface. The database can be expanded by the government in order to store data of a larger population. The fingerprint data can be obtained from the biometric data information of each resident which is stored in the government database. In the future, the system can be expanded by including the following features. The fingerprint recognition algorithm can be further optimized to reduce the run-time between acceptance and verification of the fingerprint. The prototype can be tested on better processors which can exponentially decrease the time-complexity of the entire procedure.

Acknowledgements We are gratified to express our gratitude towards the Electronics and Communication Engineering Department and HuT Labs of Amritapuri campus of Amrita Vishwa Vidyapeetham University for their ceaseless succour, without which this work would not have been progressed.

References

1. S. Patil, A. Bansal, U. Raina, V. Pujari, R. Kumar, E-mart voting system with secure data identification using cryptography, in *International Conference for Convergence of Technology (I2CT)* (2018). https://doi.org/10.1109/I2CT.2018.8529497
2. S. Vidhya, J. Rajiv Krishnan, B.A. Sabarish, P. Sachin, E-vaccination fingerprint based vaccination monitoring system. Int. J. Pure Appl. Math. **118**, 623–628 (2018)
3. S. Nisha, A. Neela Madheswari, Prevention of phishing attacks in voting system using visual cryptography, in *International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)* (2016). https://doi.org/10.1109/ICETETS.2016.7603013
4. M.A. Khasawneh, M. Malkawi, O. Al-Jarrah, A biometric-secure e-voting system for election processes, in *International Symposium on Mechatronics and Its Applications ISMA08* (2008). https://doi.org/10.1109/ISMA.2008.4648818
5. M. Venkata Rao, V.R. Ravula, P. Pala, Development of anti rigging voting system using biometrics based on aadhar card numbering. Int. J. Sci. Eng. Adv. Technol. IJSEAT **3**(2) (2015)
6. R.K. Megalingam, G. Sriteja, A. Kashyap, K.G.S. Apuroop, V.V. Gedala, S. Badhyopadhyay, Performance evaluation of SIFT and FLANN and HAAR cascade image processing algorithms for object identification in robotic applications. Int. J. Pure Appl. Math. **118**(18), 2605–2612 (2018)
7. R.K. Megalingam, K.S. Sarathkumar, V. Mahesh Kumar, A secured healthcare platform for remote health monitoring services, in *Conference: NGCT 2105, IEEE International Conference on Next Generation Computing Technologies* (2015)
8. R.K. Megalingam, K. Jyothsna, T.S. Aparna, T. Anjali, M. Meera, S.D. Amruth, IoT-based women security system, in *2019 Inventive Communication and Computational Technologies, Proceedings of ICICCT* (2019)
9. M. Faheem Rana, A. Altaf, S.Z. Naseem, Enhanced real time system of E-voting using fingerprint, in *2013 International Conference on Electronics, Computer and Computation (ICECCO)* (2013), pp. 297–300. https://doi.org/10.1109/ICECCO.2013.6718287
10. T. Singh, Design of a dual biometric authentication system, in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (2016). https://doi.org/10.1109/ICEEOT.2016.7754806

11. T. Bagyammal, L. Parameswaran, Context based image retrieval using image features. Int. J. Adv. Inf. Eng. Technol. (IJAIET) **9**(9), 27–37 (2015)
12. J. Deepika, S. Kalaiselvi, S. Mahalakshmi, S. Agnes Shifani, Smart electronic voting system based on biometric identification-survey, in *2017 Third International Conference on Science Technology Engineering and Management (ICONSTEM)* (2017), pp. 939–942. https://doi.org/10.1109/ICONSTEM.2017.8261341
13. R. Balaji, M.P. Muhammed Afnas, B. Praveen Kumar, V. Varun, C. Tamizhvanan, Embedded based E-voting system through fingerprint and aadhaar card verification (2019)
14. B. Madan Mohan Reddy, D. Srihari, RFID based biometric voting machine linked to aadhaar for safe and secure voting. Int. J. Sci. Eng. Technol. Res. (IJSETR) **4**(4) (2015)
15. M.M.H. Ali, V.H. Mahale, P. Yannawar, A.T. Gaikwad, Overview of fingerprint recognition system (2016), pp. 1344–1350. https://doi.org/10.1109/ICEEOT.2016.7754902
16. L. Hong, Y. Wan, A.K. Jain, Fingerprint image enhancement: algorithm and performance evaluation. IEEE Trans. Pattern Anal. Mach. Intell. **20**(8), 777–789 (1998). https://doi.org/10.1109/34.709565
17. J. Samuel Manoharan, A novel user layer cloud security model based on chaotic Arnold transformation using fingerprint biometric traits. J. Innov. Image Process. (JIIP) 36–51 (2021). https://doi.org/10.36548/jiip.2021.1.004
18. M. McGaley, J. McCarthy, Transparency and e-voting democratic versus commercial interests, in *Electronic Voting in Europe—Technology, Law, Politics and Society, Workshop of the ESF TED Programme Together with GI and OCG, July, 7th–9th* (2004), pp. 53–163