iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

FACE VOTE SHIELD: A SECURE FACE RECOGNITION-BASED VOTING SYSTEM USING RASPBERRY PI

Mr. B. Kishore Kumar
Assistant Professor, Department of ECE, JBIET, Hyderabad, India
Shresta Sriramoju, P. Pooja Shanmukhi, K. Srija, T. Sri Chandana
UG Students, Department of ECE, JBIET, Hyderabad, India

ABSTRACT
The electronic voting system based on Raspberry Pi is designed with solutions to the challenges imposed by a traditional voting system. This electronic voting machine has several advantages, namely; security, transparency, efficiency, and reliability which aims to make the voting process easier for the voters and speed up the counting process. Though various electronic voting systems are available in the market, the proposed system has better features that benefit the election process. The challenges being faced in a traditional voting system are the faults that prove to be fatal in many cases. The absence of security in a traditional voting system and the miscalculations that take place while counting the votes is one of the biggest concerns in the existing systems. The security vulnerabilities lead to unauthorized personnel manipulating the voting record and hence tampering the main purpose of voting. Here, biometric authentication using fingerprint recognition is emphasized. The vote cast by only the authorized voters is considered, preventing duplicate or fraudulent voting. Hence for enabling secure and authorized voting, embedded systems and IoT is used to get proper authentication.
The real-time display of the cast vote is made possible through an screen which displays the message for confirmation. The voting data are stored in cloud data which is a Raspberry Pi based server for ensuring data integrity. By storing the data in a server, the manual errors are minimized as the data gets directly recorded into the database which reduces the risk of tampering and trust issues. The voting process gets real-time IoT-based monitoring which would allow the election authorities to track the process without the hassle of going to the polling booth.
In addition to that, this electronic voting machine also provides voter privacy to ensure the proper security of the data and accurate recording of the votes preventing any unauthorized modifications. The vote counting process happens in real-time and hence the time taken for declaring the results is reduced to a great extent. When compared to the existing electronic voting machines, this electronic voting machine based on Raspberry Pi can be modernized, scalable with reduced cost and reusable for future elections. The proposed system is easy to use and can be customized as per the election authorities. Also, the system is capable of being used for other smart governance applications.

Keywords:
Electronic Voting Machine (EVM), Raspberry Pi, Face Authentication, Internet of Things (IoT), Secure Voting, Embedded Systems.

INTRODUCTION
People vote in a democratic society to choose their leaders and representatives. In a conventional election, the most widely used voting mechanism is still the traditional paper ballots along with simple basic electronic machines. This makes the voting process tedious, as it takes a long time due to long waiting times, manual errors made during the counting of the votes, lack of transparency, and a high probability of fraudulent activities. Therefore, there is a need for a secure, efficient, and reliable voting system. Embedded systems and digital solutions can help simplify the whole voting system. In this paper, we propose an Electronic Voting Machine (EVM) using Raspberry Pi. In this project, a Raspberry Pi is used as a central controller in communicating with various subsystems such as voter authentication, vote casting, and result processing. In the voting process, the voter has to authenticate using face recognition. Only authorized voters are allowed to vote, and hence duplicate voting and unauthorized access can be eliminated. This helps to make the voting process secure. The voting machine is equipped with a screen that can display the various operations being done. It displays clear instructions and confirmation messages on successful completion of the operations. A buzzer is used in this machine to provide audio feedback for the various events triggered.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

The integration of IoT technology in the Election Process for real-time monitoring and remote access to voting data has eliminated the possibility of tampering leading the regular citizens to believe in the votes casted and promoting transparency. The Election Authorities can supervise the process of polling as it happens increasing the faith in our elections. The votes are stored at a central place which ensures the secure storage of the collected votes avoiding manipulation of the votes. The safety of the data is guaranteed which also ensures data integrity and confidentiality. The entire voting system becomes more accessible to the citizens with instant results and clear transparency as each vote is recorded and processed in real time without any manual counting leading to time efficiency. The complete elimination of the manual process however is not possible as there is a possibility of hacking externally.

OBJECTIVES

An election is a formal decision-making process to choose a candidate or decide on a policy. However, in today's world, elections are subject to massive corruption in many forms. Therefore, our goal with this project is to design and implement a secure and efficient electronic voting system using Raspberry Pi as its main component and using face authentication for each vote cast. And this electronic voting system is built using embedded system technologies. Raspberry Pi is the device used to build our voting machine and also perform electronic voting using face Authentication. This project allows us to combine various embedded system technologies together in a single framework and use them to build our own embedded devices as a solution to the problem. This project overcomes the limitations of traditional voting systems and follows a specific goal outlined be:

The first goal is to create a strong mechanism for verifying the identity of voters is a voter identity verification system based on either biometric or face recognition that allows face recognition systems for the verification of authorized voters and face recognition systems based on facial features for matching with the stored voter data to authenticate the eligible voters. This verification system will prevent an unauthorized access to the voting machine and stop fraudulent voting, because only eligible voters will be authorized to cast their pertinent votes.

The second objective is to develop a suitable mechanism for secure and reliable voting is herein proposed as a system for recording and storing votes on behalf of the voting system. The user desires to input votes directly into the system through button presses (inputs) or some other user interface, while it is required they are saved securely within the system memory, providing accurate and unalterable records of the votes, providing reliability and integrity.

The third objective is to develop integrated system architecture of the election platform for authentication, vote recording and result generation in order to support secure access and vote processing to be carried out on the same platform and this will reduce errors such as duplication of vote and will improve efficiency of the platform and also improve transparency.

Additionally, the system intends to provide a user-friendly interface via the web for interaction as well as real-time analysis. Through this interface, users can register, log in, and carry out efficient fraud detection. This objective makes sure that the system becomes accessible and practical for real-world applications. Another objective is an administrator control module that allows secure monitoring and management of user activities. The admin interface provides restricted access to sensitive data so that only authorized personnel can view user information; hence enhancing security as well as integrity within the system. Moreover, the system should be able to conduct real-time detection of fraudulent activities which means that it should immediately flag any suspicious click thereby reducing potential financial losses with improved response time.

METHODOLOGY

Electronic voting is an important part of democracy. In this paper, we've proposed an EVM-based electronic voting machine. Our EVM provides a secure, efficient, and automated voting system using hardware and software components. We will also discuss the entire system design including user authentication, vote casting, data storage, and result generation.

1) The first stage is adding a buzzer, and push buttons or a touch interface can be added. Also, a camera/biometric module can be interfaced to this hardware-software integration. And to jumpstart it, Python can be used with some libraries and drivers. Use Raspberry Pi GPIO pins to connect the components for communication between the hardware and software.

2) In next step, the system is powered up by a Raspberry Pi computer. It runs a system check where it verifies that all system components are properly connected, such as the external buttons and the camera. It then gives a screen message on the display welcoming the user and informing him or her that it is ready for operation.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

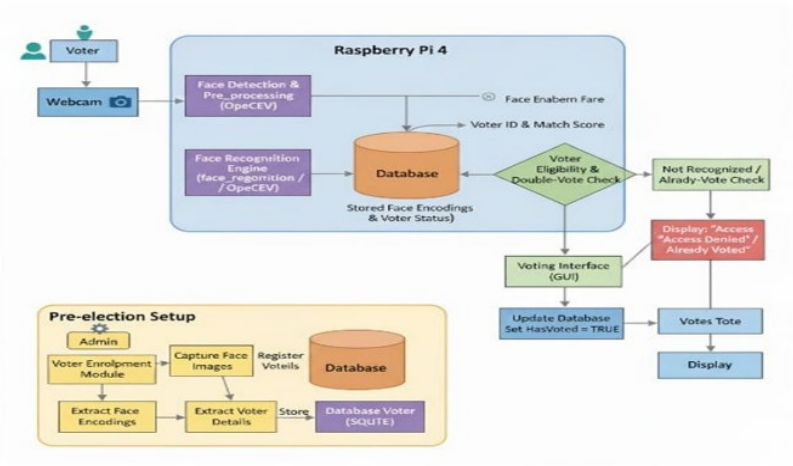

Figure 1: EVM using Raspberry Pi

3) The third stage is voting system, voter authentication is done using Face recognition. This eliminates the need for proving citizenship by displaying a valid identification card. Face recognition is a biometric verification process that captures a facial features and then compares it with a stored database. If there is a match, authentication is confirmed; if not, authentication is denied. Biometric face recognition is done for authorized users only, thus preventing unauthorized access.

4) In fourth stage, the system displays the authentication voting candidates on screen. After successful authentication, a candidate list is displayed on screen in a clear and organized manner. The voter options on the system are very clear and organized as well as attractive to the user. The user can interact smoothly with the system.

5) The fifth stage a separate review. A person can register their vote simultaneously with the push of buttons or selecting candidates on the touch interface. The voter will also be able to see the details of selected candidates. In this process, the Raspberry Pi reads voter input, processes it and records the vote. The components selected are very accurate which provides a smooth user experience. It also improved the speed resulting in registering votes with quick response time. No delays occur to record the vote.

6) In sixth stage the electronic Voting System records a vote and confirms successful voting. The voter status is updated and duplicate voting is blocked. The voting system will successfully utilize regular data recording of voting. Any siege in data that might corrupt data is handled by using data protection techniques and Reservoir land as the data for code is protected. The LCD will display the output if the voter votes successfully. The buzzer will also sound at the successful voting of a vote. After successful vote casting, the user status is updated and duplicate voting is prevented. As a result, each voter can vote only once.

7) The last stage deals with the proposed system uses IoT technology as an interface for real-time monitoring of voting sessions held at each polling booth. The data is transmitted to the container if required. The Raspberry Pi in the system ensures that the votes get counted automatically after the voting process is complete. The results will be available instantly to the administrator without any manual counting and less possibility of errors. Thus, we can provide a fast and reliable system to declare the results.

Parameter	Description	Type	Role
Raspberry Pi	Main controller of the system.	Processing Unit	Manages authentication, vote recording, and result generation
IoT Module	Provides internet connectivity.	Communication .	Enables real-time monitoring and data transmission.
Secure Storage	Memory used to store voting data securely.	Storage Device	Maintains vote data safely and prevents

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

			data loss or modification.
Camera / Biometric	Device used to capture face or fingerprint data for authentication.	Input Device	Verifies voter identity and prevents unauthorized access.
Push Buttons / Keypad	Input interface used by voters to select candidates.	Input Device	Allows users to cast their votes.
Buzzer	Audio output device that produces sound signals	Output Device	Indicates successful vote casting or system alerts.
Power Supply	Provides electrical power to the system.	Support Unit	Ensures proper functioning of all components.

Table1: Functional Description of EVM System Components

The table above presents a summary of the key components used in the Electronic Voting Machine system. The proposed Electronic Voting Machine system consists of various components. It consists of input components and output devices. Push Buttons or camera modules are the input components of the system. To capture the voter id and selection, push buttons are provided. To display the message for user interaction and confirmation, output devices are used like display and buzzer. At the center, Raspberry pi is used as main processing unit. IoT module is used for the real-time monitoring and data transmission. Thus a secure, efficient and reliable voting process is achieved.

RESULTS AND DISCUSSION

The Electronic Voting Machine system using Raspberry Pi was implemented. A camera-based face recognition module is being tested for our electronic voting system. The photo of authorized voters is taken at the time of voting and is saved in a database. The recognition of the voter's face is done based on this photo and voting is permitted for authenticated person only. This will be helpful to prevent unauthorized voting and to prevent duplicate voting. The module will function in real-time \u2013 it will identify the authorized voter and will send a signal to the further action. The module require testing under controlled conditions at the moment to fine-tune the applied algorithms and improve its reliability.

To conduct the enrollment, connect to the Raspberry Pi from a separate PC system using the free software of RealVNC Viewer. After opening the application window, navigate through the project files until you reach the folder containing the dataset. Double click on the dataset folder to view the contents of the folder. There you can see various images of people who are already enrolled in the system. To conduct the enrollment, double click on the "enroll new person" module. To start the enrollment process, make sure you have the camera running properly so that the facial data of the candidate will be captured and stored in the dataset for further processing and registration for the voter's system.

Figure 1: Home page

Once the user is successfully enrolled, an encoding module encodes the captured facial data into a structured format for further use in recognition. This allows for efficient comparison of the real-time input with what is already stored in the facial recognition system. Once the post-enrollment processing stage of our facial recognition system is done, the data collected will be converted into a format that is easy to carry out the comparison workflow

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

with. Furthermore, all facial data collected will be stored in a structured recognition database. For this phase of our perfect facial recognition, we focus mainly with the efficiency with which the comparison of the real time video runs against it's structured database. This phase will subsequently run through out while the facial recognition system is running and will be continuously running back and forth and it's output will be what is fed into the automated matching process of the facial recognition system.

Figure 2: Enrollment page

The final voting system allows the camera access request to capture the face of the user. It captures the face from the image and compares it with the face stored in the dataset. If the user is a registered voter, access is granted; otherwise, access is denied. In this system, only authorized voters are allowed to proceed.
After authenticating, the voter casts the vote through the provided interface. The system records the vote and updates the database instantly. In addition, it will block the repeated voting attempts by the same user. The vote is cast successfully. The user tried to enter the same credentials again. It is a duplicate entry. The system detects the duplicate entry and thus prevents the multiple voting. Hence, here a successful authentication is done but when the same person is trying it again for the voting then the duplicate entry is detected and thus the repeated action is blocked. The last action is recorded and the database is updated. Hence the vote which is cast is stored.
The system displays clear indication of whether access was granted or denied, as well as confirmation of recorded votes. This helps to ensure users have a smooth experience with the confident knowledge their choice has been recorded. All information is secure and displayed clearly for users and administrators alike
.

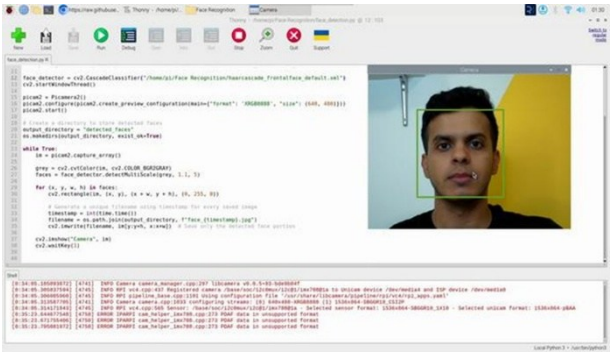

Figure 3: Final Voting System

Proposed experimental voting system based on face recognition with hardware based embedded processing to ensure both the quality of the secure voting mechanism and the reliability of the authentication, vote recording, and fraud prevention. The results of the experimental tests show that the intended implementation of the proposed experimental voting system retains a strong performance to allow utilization in real-world applications and situations such as secure transactions, secure elections, and automated ballot handling under the test conditions of this study. This reduces the risk of impersonation and allows efficient data capture over the overall prototype workflow.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

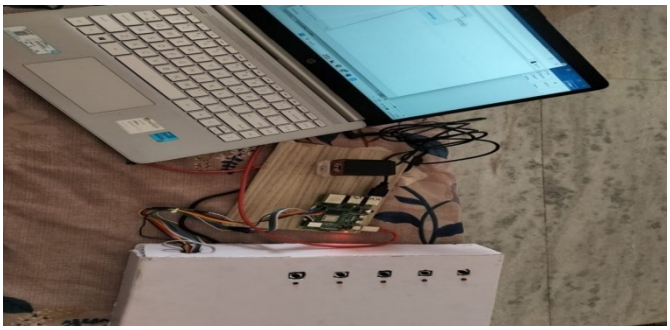

Figure 4: EVM kit

ACKNOWLEDGEMENT

We are thankful to the management and faculty of J.B. Institute of Engineering and Technology, Hyderabad, for providing the necessary environment and facilities to complete this work in time. Their continuous support and encouragement were instrumental in the completion of this project. We express our gratitude to our project guide and faculty members for their valuable guidance, suggestions, and constructive criticism during the course of development of this work which helped us greatly in improving its quality as well as direction. We acknowledge with thanks the help received from peers and classmates in discussions, suggestions, and motivation at different stages of the project that contributed toward improving implementation and overcoming challenges effectively. We also take this opportunity to thank all developers who have contributed toward open-source technologies/tools used in developing a real-time project that made it possible to implement successfully an application as proposed here. Last but not least, we would like to extend our thanks to family members for their constant encouragement, patience, and moral support which kept us motivated as well as focused while completing this work.

CONCLUSION

This project focuses on proposing a face shield detection system for safety compliance in hospitals, laboratories, and industrial workplaces, using the Raspberry Pi 4 Model B, a single-board computer, to automatically detect face shields and trigger real-time alerts. The revolutionary Raspberry Pi 4 Model B enables the deployment of robust, compact and affordable systems for real-time computer vision applications.

The proposed system recognizes the importance of face shields. The purpose of a face shield is to protect the user's face and eyes from potential hazardous substances and/or agents, including chemical splashes, blood splatter, and arc flashes. The proposed face shield detection system assists in the automatic detection of face shields and timely triggering of alerts to ensure the safety of the user. To achieve this, a state of the art image processing algorithm, is applied to identify facial features and subsequently face shields when they are worn.

The hardware components in the implementation of this proposal include a Raspberry Pi, a camera module as well as an alert mechanism including a buzzer or LED. The overall system is powered by the low volume Raspberry Pi OS which is also equipped with capabilities to connect to a wireless system to send alerts through messages. The system is programmed using Python and the image processing library OpenCV which is capable of performing live video frame processing.

The face shield detection system employs an image processing algorithm that includes several modules: image acquisition and pre-processing, face detection, face shield detection, decision-making, and alert modules. The first module obtains and pre-processes a live video feed from the onboard camera. The second module detects whether there is a face present in the video frame, while the third module identifies whether a face shield is being worn by the person (if a face is detected). The results of the detection are passed onto the next module which makes a decision based on those results to implement the function of an alert module in either case.

In conclusion, a highly automated, reliable, and cost-effective face shield detection system to monitor safety compliance. The proposed solution utilizes computer vision technologies in embedded systems. It can be further developed and expanded into an advanced and scalable system that allows for real-world deployment.

REFERENCES

1) OpenCV Documentation, *Open Source Computer Vision Library*, Available at: https://opencv.org/
2) Raspberry Pi 4 Model B Official Documentation, *Raspberry Pi Foundation*, Available at: https://www.raspberrypi.org/documentation/

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

3) Raspberry Pi OS User Guide, *Raspberry Pi Foundation*, Available at: https://www.raspberrypi.com/software/
4) Python Documentation, *Python Software Foundation*, Available at: https://docs.python.org/3/
5) TensorFlow Documentation, *Google Developers*, Available at: https://www.tensorflow.org/
6) Research Paper: "Face Detection using Haar Cascade Classifier," *International Journal of Computer Applications*
7) Research Paper: "Real-Time Face Mask Detection using Deep Learning," *IEEE Xplore Digital Library*
8) Book: "Learning OpenCV: Computer Vision with the OpenCV Library" by Gary Bradski and Adrian Kaehler
9) Research Paper: "Deep Learning for Image-Based Face Detection and Recognition," *Springer Publications*
10) Online Resource: Raspberry Pi Camera Module Documentation, *Raspberry Pi Foundation*