UNIVERSITY OF DELHI

Revolutionizing Voting: A Smart Voting Machine with Online Voting Capability

Manu Dev (152127) | Abhishek Kumar (152105)

Under the guidance of Prof. Pankaj Tyagi

A report submitted in partial fulfillment of the requirements for the degree of B.Tech (IT and MI)

CLUSTER INNOVATION CENTRE UNIVERSITY OF DELHI

May 2, 2023

Acknowledgement

With a deep sense of gratitude, we express our dearest indebtedness to **Prof. Pankaj Tyagi** for their support throughout the duration of our project. We would like to thank them for giving us the opportunity to do this wonderful project. Their advice and constant encouragement have helped us to complete this project. It is a privilege for us to be their students. We are also thankful to our friends and family who have supported us throughout the journey.

Certificate

The work embodied in this report entitled "**Revolutionizing Voting: A Smart Voting Machine with Online Voting Capability**" has been carried out by **Manu Dev** and **Abhishek Kumar** submitted to "**Cluster Innovation Centre, University of Delhi**". We declare that the work and language included in this project report is free from any kind of plagiarism. Any illustrations that are not the work of the author of this report have been used with the explicit permission of the originator and are specifically acknowledged.

Signature of the Authors: Signature of the guide:

Abstract

India is called the world's largest democracy. In such a democratic country, voting plays a key role in electing government officials and reflects our vision of how a governing body should be formed. Surveys are conducted from time to time to address difficulties in the central voting system so that it should be more anonymous, reliable and secure while preventing any type of fraud. With the use of electronic voting, we have to deal with many problems of fraud and corruption. The design and development of a smart voting system with an online voting feature are discussed in this paper. The suggested system intends to give users with a safe and effective voting method that lowers the possibility of manipulation, and offers real-time vote counting.We provide the various works which are being proposed based on the voting system which uses biometric identification as a major concept. In the field of biometric identification, we can get better results and it is also trustworthy. We work on different techniques which are based on multimodal biometric identification such as camera and fingerprint. The proposed system also includes a database that stores the voting records and generates reports after the election. The proposed system has the potential to improve the overall efficiency and transparency of the voting process and has the potential to revolutionize the way we conduct elections in the future.

Index

S. No.	Title	Pg. No.
1	Acknowledgement	2
2	Certificate	3
3	Abstract	4
4	1. Introduction	6
5	1.1 Background	6
6	1.2 Scope and Objective	6
7	2. Methodology	7
8	2.1 Benefits over conventional EVMs	7
9	3. Flow Chart	8
10	4. Results	9
11	5. Equipments Used	12
12	6. Conclusion	12
13	7. Future Scope	12
14	References	12
15	Appendix	13

1. Introduction

In India, the online voting system is a way for people to choose their representatives and express their preferences about how they will be governed. It is very important to have confidence in the electoral process. A smart voting machine is more secure in the case of elections and the system will increase the level of security. It is designed to be easy to use and provide voters with a simple and intuitive interface to select candidates. EVMs usually consist of a display screen, a keyboard or touchpad for selecting candidates and a memory device for recording and storing votes. They may also include security features such as encryption and authentication to prevent tampering and ensure the integrity of the voting process. Despite their advantages, there have been concerns about the safety and reliability of EVMs, leading to debates in some places about their use. However, in some areas there is a possibility of Maoist attacks and fraud problems, there is a chance of losing votes, because EVM is secure, but the verification to vote is still done by humans, there may be a possibility of human error, so the public needs a safer voting system. In an online voting system using facial recognition aimed at overcoming all the shortcomings found in the existing voting system. The proposed system has many powerful attributes such as accuracy, reliability, convenience, etc. In this system, there is no need for a polling officer, ballot or any other voting system, but only a strong internet connection with electronic voting devices. and facial scanners are essential where voting can be done from anywhere. The proposed method provides a more accessible, safer and more efficient system than the existing one with many errors such as long process, time consuming, insufficient security and fake voting.

1.1 Background:

Below are some of the common problems faced during voter ID verification in India. To ensure free and fair elections, it is essential to address these issues and implement measures to prevent them from happening.

- Incorrect Information: One of the common problems during voter ID verification is the incorrect information provided by the individuals.Which leads to discrepancies in the voter ID and other identification documents.
- Duplicate Voter IDs: Another problem during voter ID verification is the existence of duplicate voter IDs. Many people have multiple voter IDs, which makes it difficult to verify the authenticity of each voter.
- Lack of Proper Information: The Voter Id card has black and white images and photos aren’t updated very frequently, which makes it hard to verify a person's identity.
- Voter Intimidation: Voter intimidation is also a problem during voter ID verification. Many voters are intimidated by political parties or candidates, which leads to incorrect information being provided during the verification process.
- Human Verification Error: There may be error by the invigilating officer during verifying one’s identity.

1.2 Scope and Objective :

Integrating biometric verification such as fingerprint and image verification with EVM to remove human verification error enabling more security for voting. Raspberry Pi and image processing based on the Electronic Voting Machine (EVM), provides a small computer capable of image processing and controls the entire voting system. Each voting machine is locked with a module of fingerprint access. When the user touches the sensor, the fingerprint is matched and then the camera is used to verify the voter's face id and if the person is legitimate and has not voted, the person will be allowed to cast his or her vote. Since Aadhar contains all these data of a person if voter id is linked with Aadhar then this verification will be secure. Online Voting System, introduces a system where people who are Indian citizens and over the age of 18 can give their vote. Even though they don’t have to go to their hometown on the allotted day. The system is based on Aadhar that, the electoral elections will allow people to vote in their current city electronically.

2. Methodology

- **Authentication:** The voter is authenticated using biometric identification (like fingerprint scanner), or other secure (such as a camera) means to ensure that only eligible voters can cast their votes.
- **Candidate selection:** The voter selects the candidates of their choice using a button, or other input devices.
- **Vote recording:** The smart voting machine records the voter's selections and stores them securely in the machine's memory.
- **Confirmation**: Once the voting is complete, the machine confirms with a beep sound after the vote and displays their voting information.

2.1 Benefits over conventional EVMs:

- **Increased security:** It has more advanced security features than conventional EVMs, such as encryption, Biometric authentication, and auditing capabilities. This makes them more resistant to tampering, hacking, or other forms of fraud.
- **Improved accessibility:** With integrated online voting capabilities, it provides a more inclusive and accessible voting process.
- **Real-time monitoring:** With real-time monitoring and analysis of voting patterns, enabling election officials to detect and respond to any irregularities or anomalies quickly.
- **Easier to use:** With visual and auditory responses it typically has more user-friendly interfaces and instructions than conventional EVMs, reducing the likelihood of errors or confusion among voters.
- **Tamper Proof:** Whenever someone tries to open or tamper with the EVM, It encrypt the file and turn off the device so no one can temper data.

3. Flow Chart

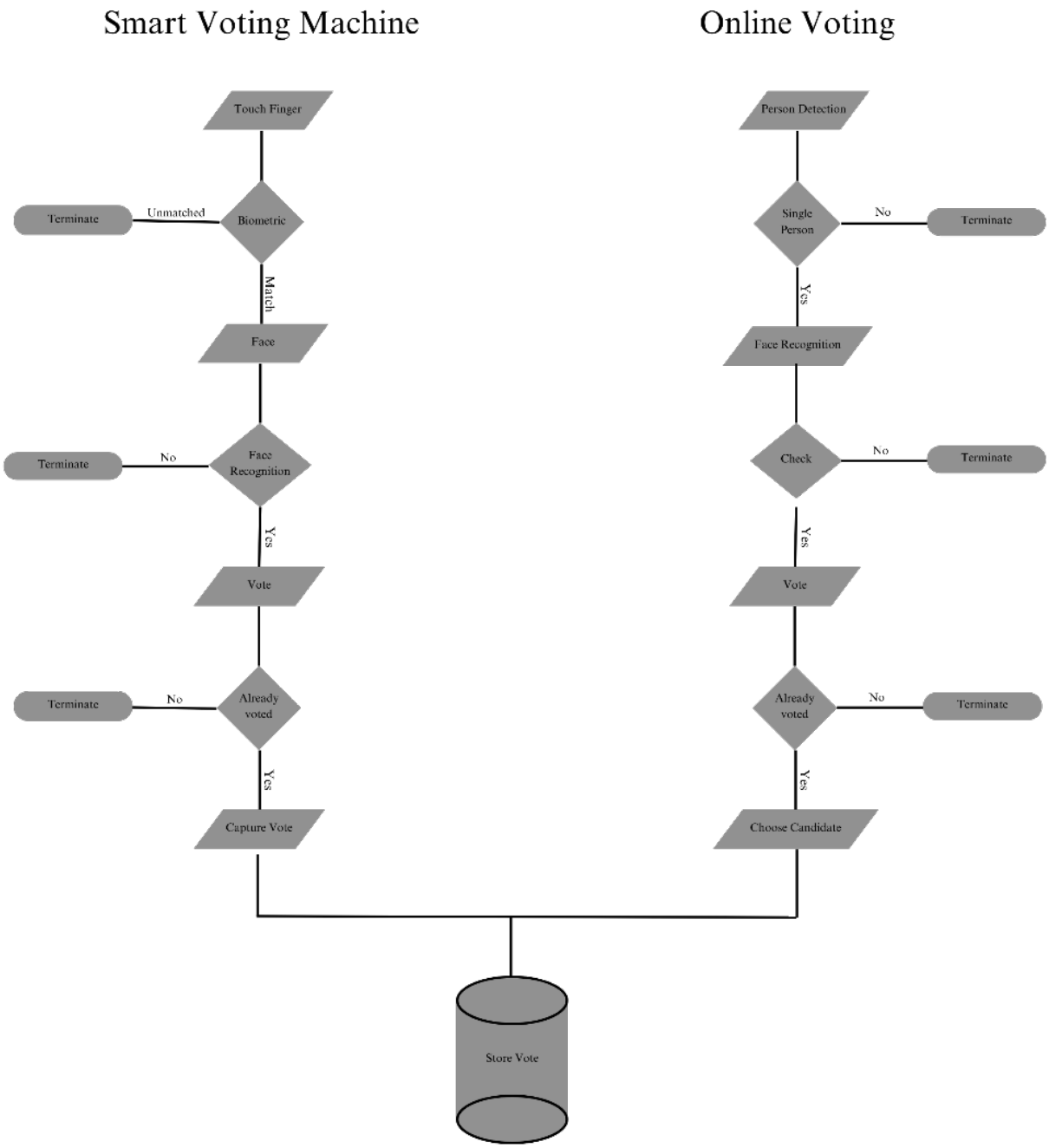

Figure 1: Flow chat

4. Results:

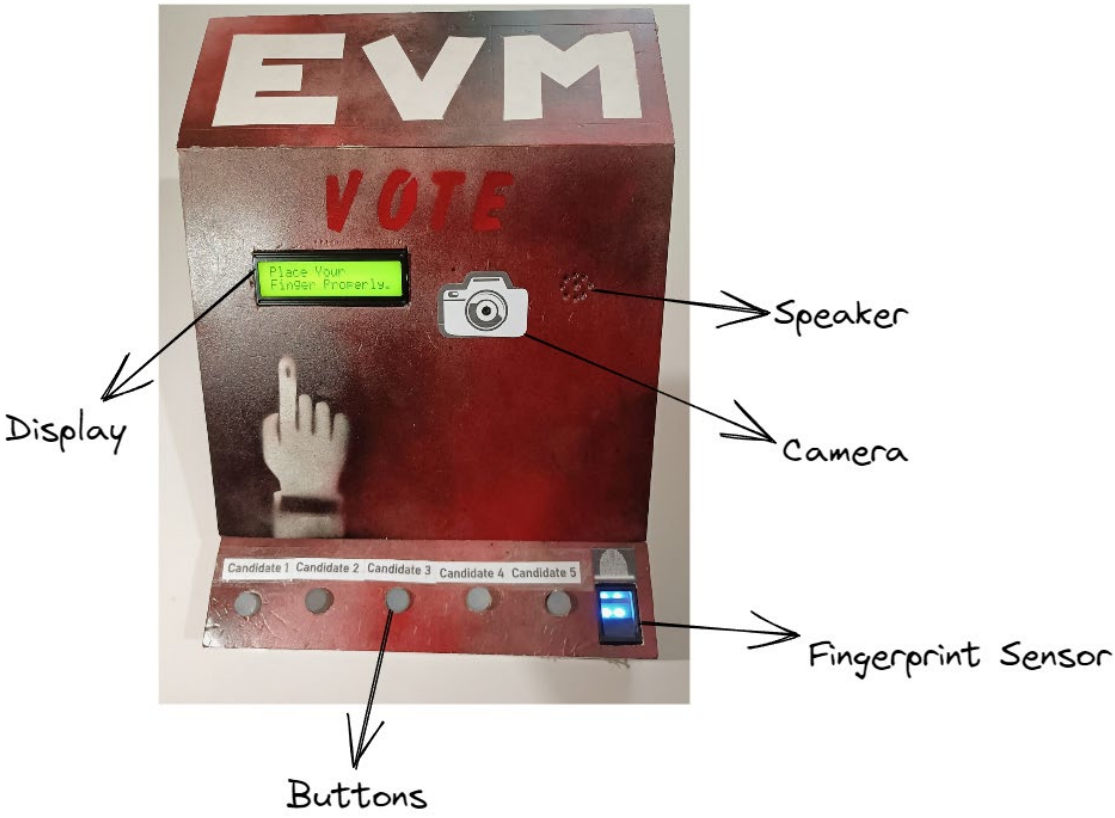

Figure 2: EVM and its parts

* If Button 4 is kept pressed and Button 2 is pressed at the same time then this secret key shows the result.

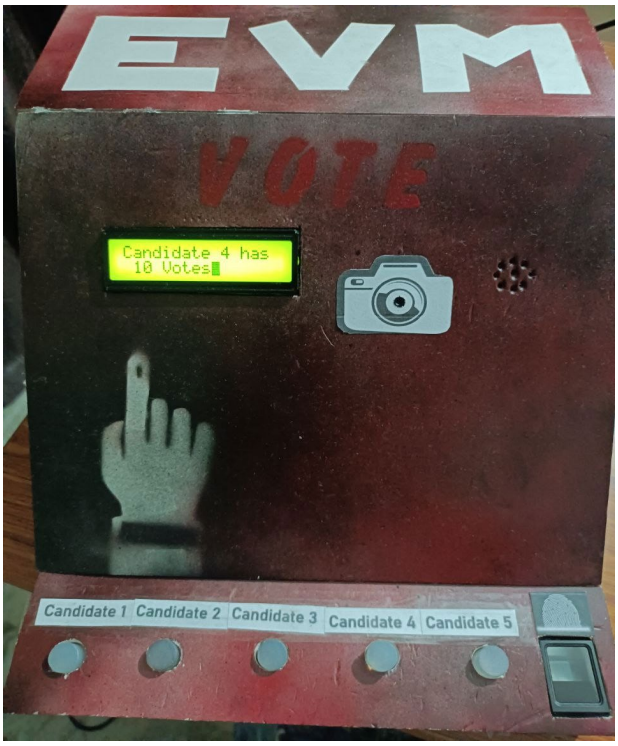

Figure 3: EVM showing results

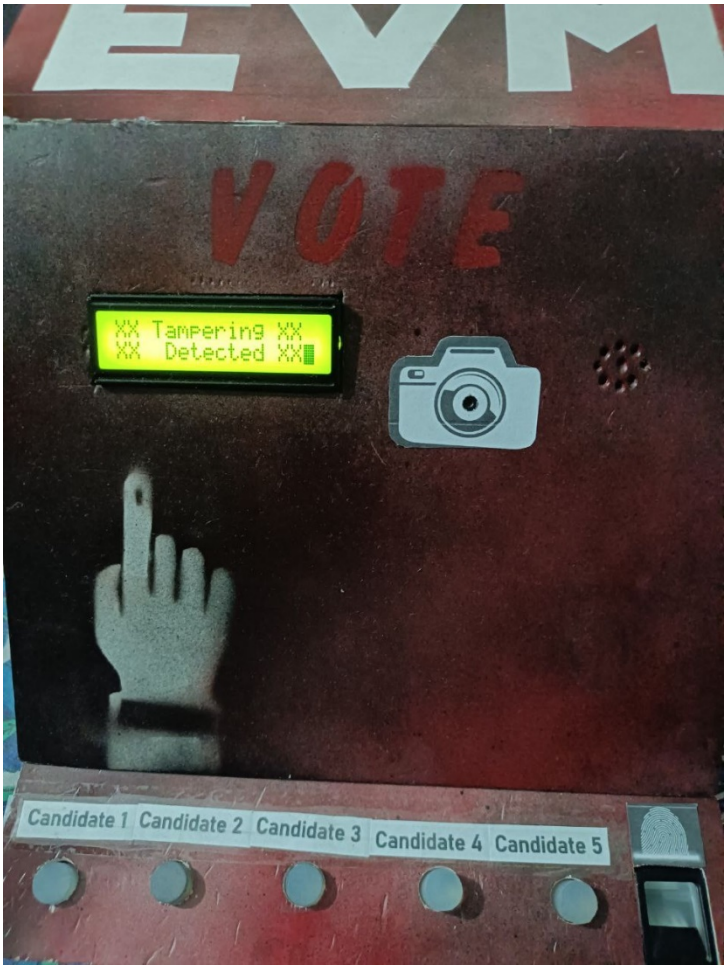

Figure 4: Tampering Detected

Online Voting Procedure

Step 1: First it will check the number of people present in front of the web camera. If there is only one person then it will allow further.

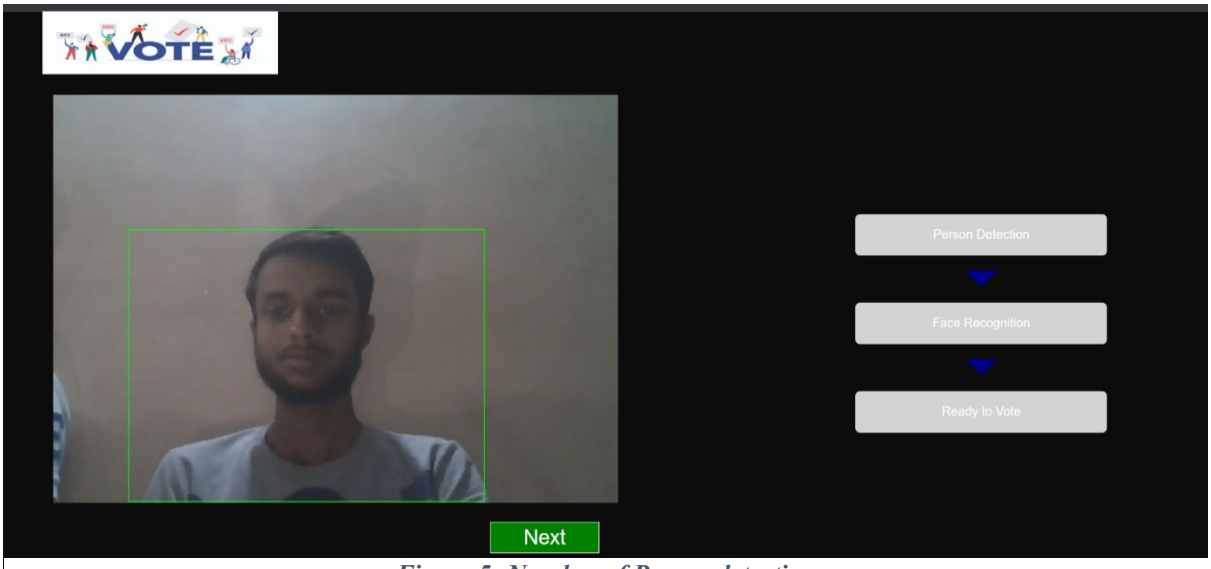

Figure 5: Number of Person detection

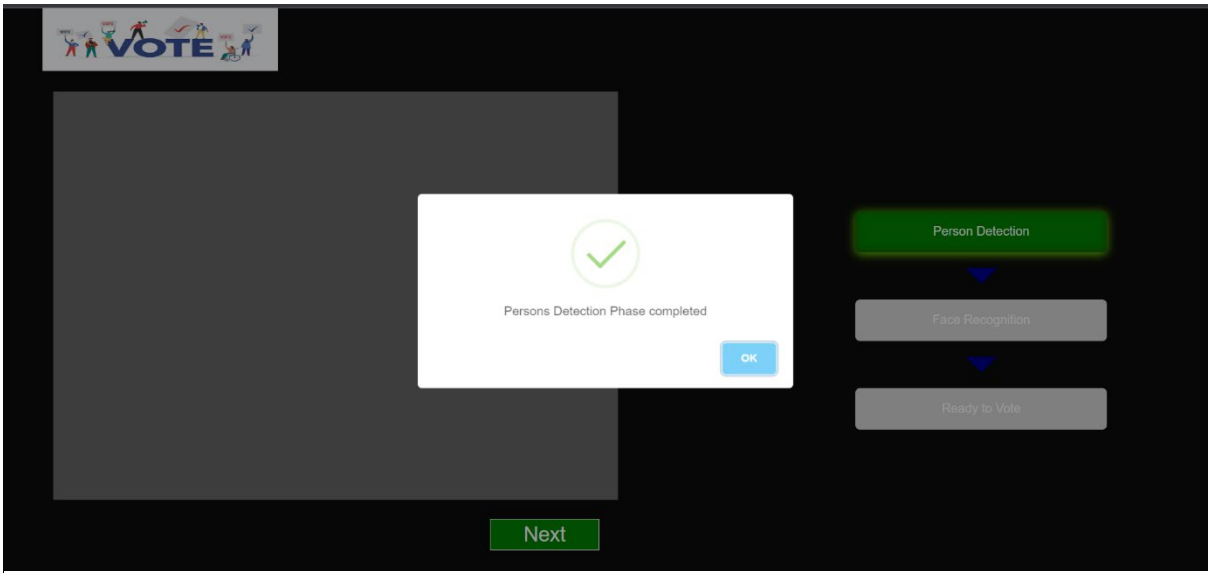

Figure 6: Success when single person detection

Step 2: After completing the person detection, it will now run face recognition and match the person with stored information which is present in the database. After a successful match, a person will be allowed to vote.

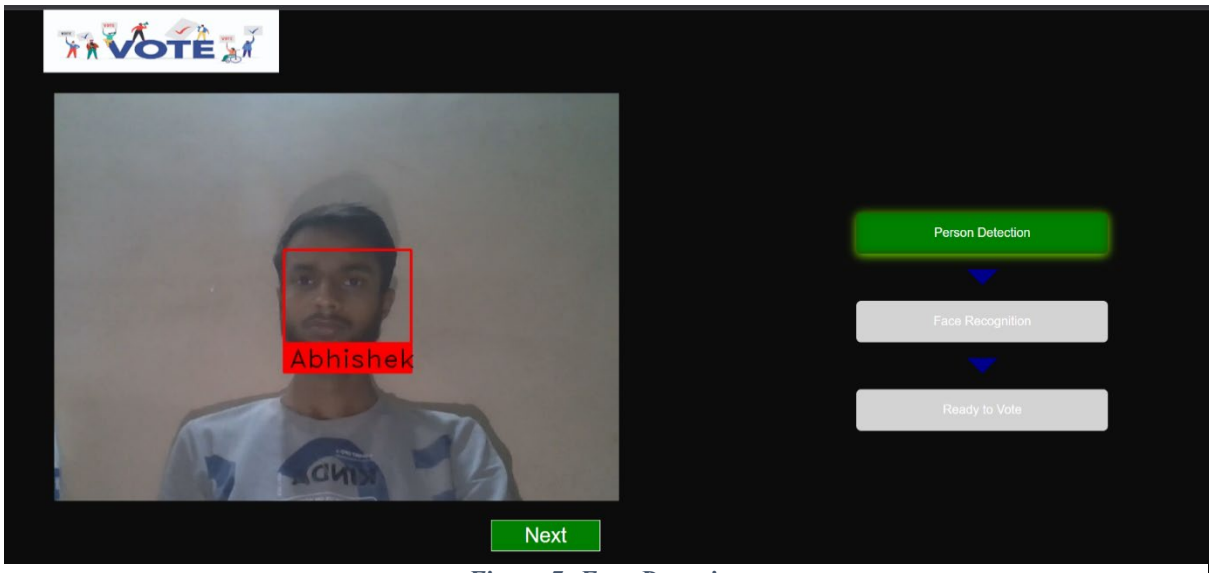

Figure 7: Face Detection

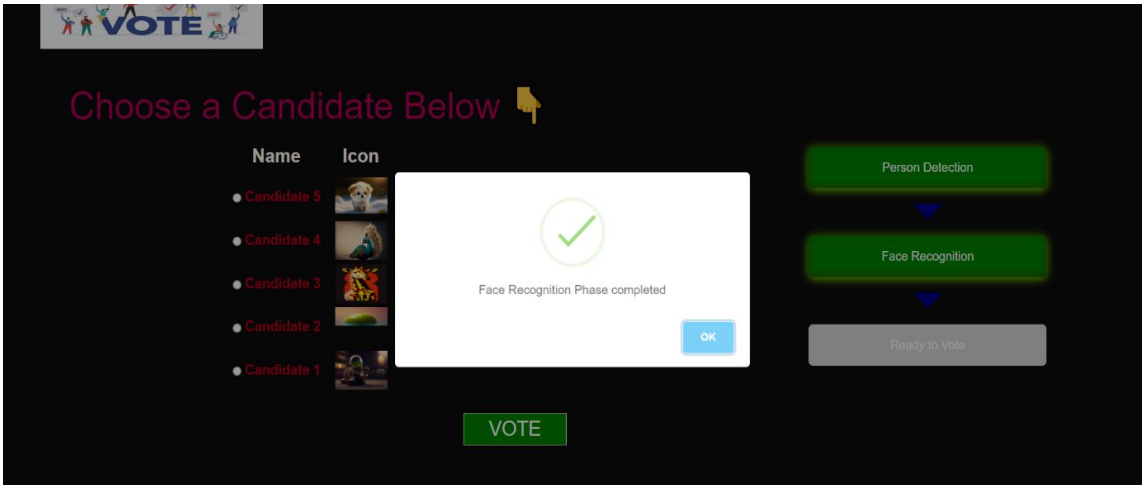

Figure 8: Successful Face detection

If person has already voted then it will not allow to vote again

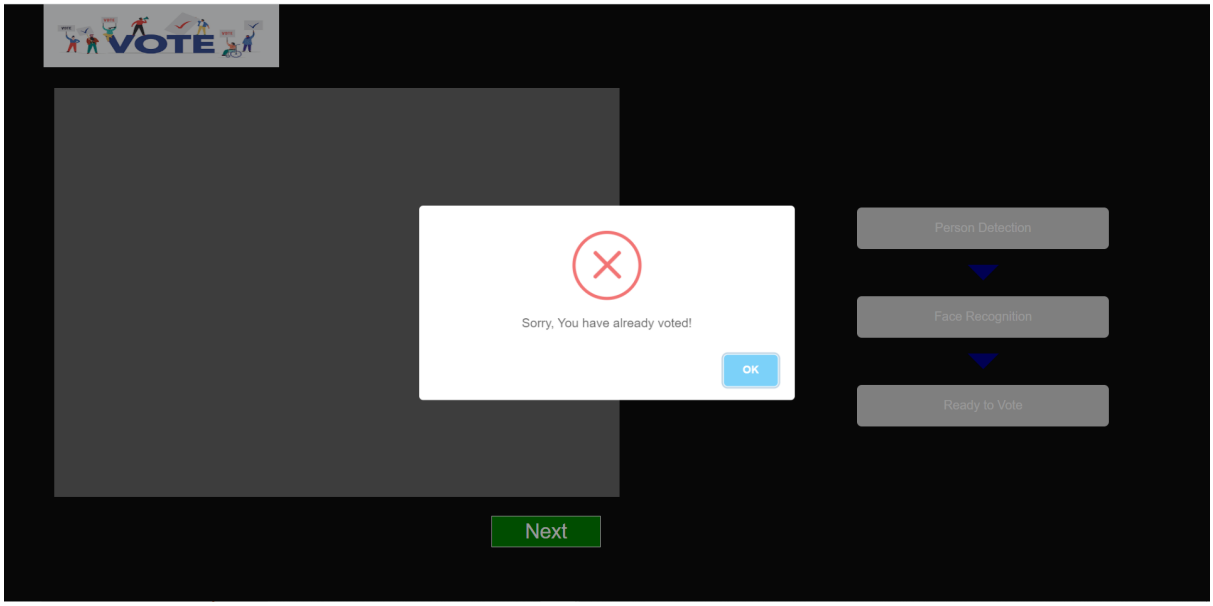

Figure 9: Prevention of Re-voting

Step 3: After completing face recognition , now candidate will able to give vote

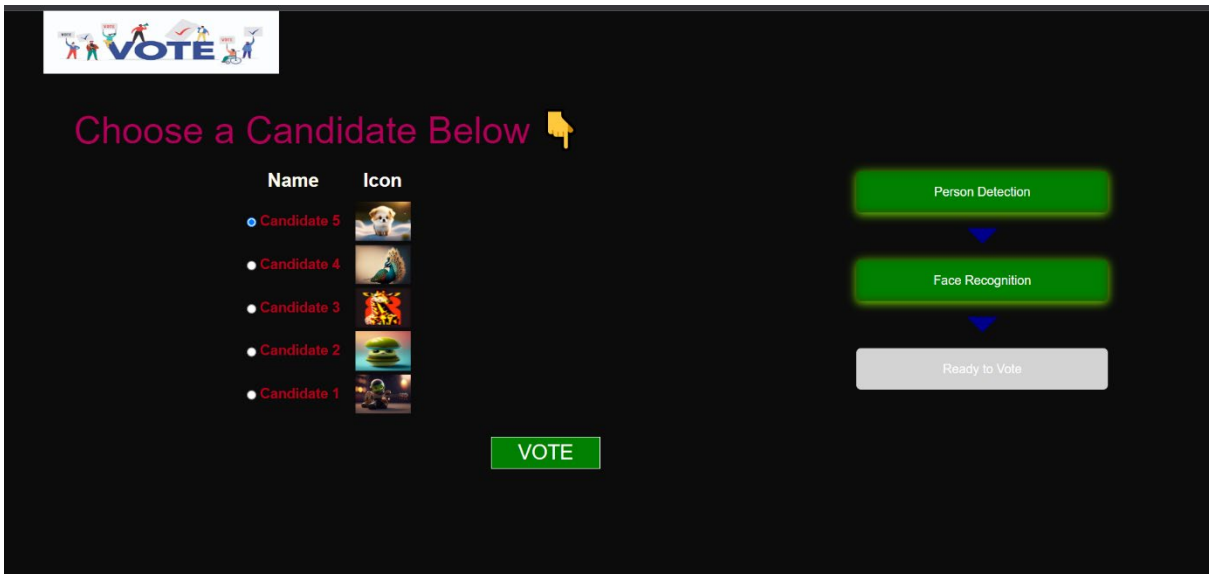

Figure 10: Choose candidate

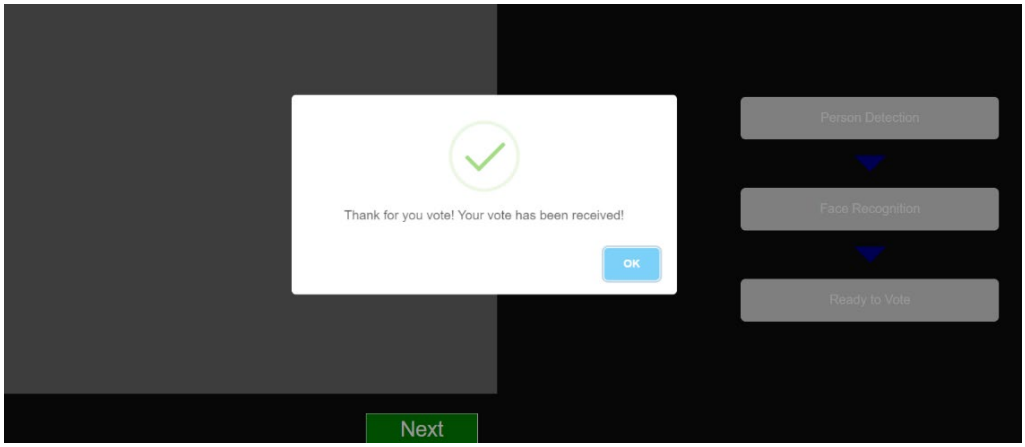

Figure 11: Voted Successfully

5. Equipments Used:

- Raspberry Pi 4
- Raspberry Pi Camera Module
- R307 Fingerprint scanner
- Display L1602
- Speaker
- Push Buttons
- Jumper Wires
- Bread Board

6. Conclusion

The voting process can be greatly enhanced by integrating electronic voting machines and internet voting platforms. In addition to being simple to use, smart voting machines offer strong security and monitoring functions. The advantage over conventional EVMs is inscrasing security and accuracy, better accessibility for voters with disabilities to detect and respond to any irregularities quickly. In contrast, online voting systems provide convenient remote voting that could increase voter turnout. Both systems have their own unique strengths and weaknesses, and the decision to use one over the other ultimately depends on the specific needs and constraints of the election. It is possible that a hybrid approach, incorporating aspects of both systems, may be the best solution for future elections. Regardless of the approach chosen, priority is to ensure the security and integrity of the voting process so that the results accurately reflect the will of the people. Both smart voting machines and online voting systems have the potential to achieve this goal, and continued research and development will be necessary to further improve and refine these technologies.

7. Future Scope

- **Use of AI (Artificial Intelligence):** It could enable real-time monitoring and analysis of voting patterns, potentially improving the detection and prevention of irregularities or anomalies by predicting election outcomes with greater accuracy.
- **Integrating Blockchain-based Voting:** It provides a more secure and transparent method of recording and counting votes, potentially reducing the risk of fraud over the internet.
- **Accessibility features:** Using accessibility features such as voice and visual assistance for voters will help disabilities. This will encourage them to vote.
- **Improve security:** By using Iris recognition and other Biometrics Identification cheating can be prevented enhancing the resistance of smart voting machines to tampering, hacking, or other forms of fraud.

References

OpenCV: OpenCV modules
Raspberry Pi Documentation
Django documentation | Django documentation | Django (djangoproject.com)
Raspberry Pi Fingerprint Sensor Interfacing Project with Code and Circuit diagram (circuitdigest.com)

Appendix

Code:

```
import RPi.GPIO as GPIO
import time
import Adafruit_CharLCD as LCD
import serial
import adafruit_fingerprint
from gpiozero import Button, Buzzer
import Face_Recog as f
import json

uart = serial.Serial("/dev/ttyS0", baudrate=57600, timeout=1)
finger = adafruit_fingerprint.Adafruit_Fingerprint(uart)

touch_sensor = Button(22)
voter =["1","2","3","4","5"]
voter[4] = Button(23)
voter[3] = Button(24)
voter[2] = Button(16)
voter[1] = Button(20)
voter[0] = Button(21)
buzzer = Buzzer(27)

# Define GPIO pins
lcd_rs = 26
lcd_en = 19
lcd_d4 = 13
lcd_d5 = 6
lcd_d6 = 5
lcd_d7 = 11

# Define LCD size
lcd_columns = 16
lcd_rows = 2

# Initialize LCD
lcd = LCD.Adafruit_CharLCD(
    lcd_rs,
    lcd_en,
    lcd_d4,
    lcd_d5,
    lcd_d6,
    lcd_d7,
    lcd_columns,
    lcd_rows
)

def get_fingerprint():
    """Get a finger print image, template it, and see if it matches!"""
    print("Waiting for image...")
    lcd.clear()
    lcd.message("Place Your \nFinger Properly...")

    while finger.get_image() != adafruit_fingerprint.OK:
        pass
```

```
    print("Templating...")
    if finger.image_2_tz(1) != adafruit_fingerprint.OK:
        return False
    print("Searching...")
    if finger.finger_search() != adafruit_fingerprint.OK:
        return False
    return True

def finger_verify():
    if get_fingerprint():
            print("Detected #", finger.finger_id, "with confidence", finger.confidence)
            lcd.clear()
            lcd.message(f'Hello! {name[finger.finger_id]}\nLook at camera')
            buzz(0.2,2)
            if f.detect_face(name[finger.finger_id]):
                lcd.clear()
                lcd.message(f'Now you can \nvote.....')
                time.sleep(0.5)
                vote()
            else:
                lcd.clear()
                lcd.message(f'Error in Face\nDetecting .....')
    else:
        print("Finger not found")
        lcd.clear()
        lcd.message('Finger not found !')
        buzz(0.5,1)

def vote():
    lcd.clear()
    lcd.message('Press The Button\nTo Vote .... !')
    flag = True
    while flag:
        for i in range(5):
            if voter[i].is_pressed:
                lcd.clear()
                lcd.message(f'{name[finger.finger_id]} Voted to\nCandidate {i+1}')
                update_vote(i+1)
                buzz(1,1)
                time.sleep(2)
                flag = False
                break


def update_vote(index):
    with open("votes.json", "r") as f:
        data = json.load(f)

    data[str(index)] += 1

    with open("votes.json", "w") as f:
        json.dump(data, f, indent=4)


def buzz(t, no):
    for i in range(no):
        buzzer.on()
        time.sleep(t)
        buzzer.off()
        time.sleep(t)
```

```
def display_results():
    if voter[3].is_pressed:
        lcd.clear()
        lcd.message(f" 2 presed")

        with open("votes.json", "r") as f:
            data = json.load(f)

        for i in range(5):
            lcd.clear()
            lcd.message(f"Candidate {i+1} has\n {data[str(i+1)]} Votes")
            time.sleep(1)
            voter[4].wait_for_press()



while True:

    lcd.clear()
    lcd.message('Touch the --\nSensor !')


    if touch_sensor.is_pressed:
        lcd.clear()

        # Display another message
        lcd.message('Validating...!')
        buzz(0.2,1)
        time.sleep(0.2)

        finger_verify()
        time.sleep(2)

        # Clear LCD
        lcd.clear()

    if voter[1].is_pressed:
        display_results()

    time.sleep(0.5)
```