ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Research Article

Open Access

Design and Simulation of Text-To-Speech Enabled Electronic Voting Machine

Teryima D. Kureve, G. A. Igwue, Negedu Philip* and N. S. Tarkaa

Department of Electrical Electronic Engineering, Faculty of Engineering, University of Agriculture, Makurdi

ABSTRACT

Electronic voting machine has received tremendous researches in recent times with improvement in its capabilities. However, most electronic voting machine has limitation in terms of the number of parties it can accommodate and unfriendly to visually impaired persons. This present paper incorporates test-to-speech functionality into the electronic voting as to provide user friendliness to visually impaired persons and also for election announcement. The major component used to achieve this aim are Arduino Mega 2560, SM630 fingerprint scanner, RFID scanner and keypad matrix. This present electronic voting machine met the key requirements of convenience, transparency, flexibility, accuracy, eligibility, uniqueness, auditability, confidence and privacy.

***Corresponding author**

Negedu Philip, Department of Electrical Electronic Engineering, Faculty of Engineering, University of Agriculture, Makurdi; E-mail: philipnegedu@gmail.com

Received: June 03, 2021; **Accepted:** June 09, 2021; **Published:** June 25, 2021

Keywords: Election, Electronic, Machine, Voting, Voter, Text-to-Speech

Introduction

A system which allow voters to make use of electronic tools and processes for vote casting, tallying, transmission, counting and determination of election winner is termed electronic voting machine [1]. Electronic voting is the use of electronic device (machine) in voting, where election data is recorded, stored and processed primarily as digital information [2]. Electronic voting machine has received tremendous researches in recent times with improvement in its capabilities. Though there are many types of electronic voting such as email voting, sms (text), internet voting among other, the type discussed in this paper a like a single polling unit machine which collects voters' data and use such for voter authentication and vote casting.

There are various concerns for the use of electronic voting in various literatures, one of the major concerns raised by researchers is security; the security of electronic data and that of the voters [3,4]. It is alleged that the electronic data can be hacked into and thus ridge the election. The seriousness of this security challenge was seen in last United States of America (USA) presidential, where it was alleged that the election was ridge electronically [5].

Election data and voter's data can be hacked into mainly during transmission from one voting point to the other [6]. However, with the use of imbibed system, security of voting using electronic means is guaranteed. In using embedded system, a single machine has the capability of managing voter's data, voters' authentication, vote recording, tallying and result processing. Because the system does not have shared communication with other systems outside itself for the purpose of voting, hacking into the system becomes near impossible.

In implementation of electronic voting machine, there are key requirements for the machine to be capable to function effectively. These key requirements include convenience, transparency, flexibility, accuracy, eligibility, uniqueness, auditability, confidence and privacy [7]. The voting machine should be convenient such that no required special skill(s) is needed for voter to use the machine, hence both the voters and candidates in the election should have a general knowledge and understanding of the of the voting process, thus being transparent. The system should accurately record all the data regarding the election; candidates for the election, voter's information and vote information and be flexible in its functionality. The machine should equally ensure that no record could be manipulated, detect and prevent multiple voting or unauthorized voting. The machine should ensure that all votes are accurately accounted for, vote tallying and election results, appropriately carried out. In addition,

This paper is aimed at designing and implementing a test-to-speech (TTS) enabled electronic voting machine which the following specific objectives.

i. The electronic machine should accurately receive, store and match voter data for the purpose of election.
ii. Accommodate large number of registered parties for the election.
iii. Using high system embedded technology, the machine should accurately carryout the functions as required of electronic voting machine.
iv. The voting machine should be able to provide security of the data in the machine using password and encryption for administrative purpose
v. The voting machine should be user friendly and has provision for interaction with physically disable persons like the blind using text to speech capability.
vi. The voting machine should be able to use voters' biometric

and match with the voters' card (RFID Card) for registration, authentication and verification for voting.

In this developed electronic voting machine, there are three functional operation viz; voter registration, vote casting and results population. In the registration module, the machine collects the voters' biometric data and link it with a voter's card. These information from the voters are stored in the database of the electronic voting machine. In the election module, the voter is verified for eligibility for voting using double authentication of voters' biometric and voters' card. After voting, the data of the voter is moved to the database containing voted data and the voting is added to the data of the party of choice. Hence, the voter can only vote once and can be allowed to vote if the biometric provided matches the card presented by the voters. The biometric of the voters are collected using fingerprint scanner while voters' card information is scanned using Radio-frequency identification (RFID) technology.

Related Work

In order to improve on the development of electronic voting machine, there is need to review researches conducted by others and find areas that need improvement [8]. Carried out Fingerprint based Electronic Voting Machine with Inbuilt Identification and Verification System using Arduino Mega 2560 as the microcontroller for the work. Voters' biometric was collected using R305 fingerprint scanner while voting exercise was performed using a dedicated key for each party. The system features include biometric capture of the voters, voting tallying, double voting detection and prevention and result population. The voter is first enrolled and then be eligible to vote. One of the major limitations of this work is single voter verification using only biometric. Though R305 Fingerprint has high fingerprint matching accuracy, in cases that another finger matched with the one on the database, the user will be given access to vote, even if not enrolled. hence, this machine has security threat. In addition, the number of candidates for the election is not saleable, because, a dedicated button has to be made available for each candidate, limiting the number of parties that can be used in this machine due to limited pin number of the Arduino Mega 2560 used [9]. Carried out Biometric Electronic Voting Machine using two Arduino Nano microcontroller (MCU) boards and R307 fingerprint scanner One of the MCUs is used for storing the fingerprint of the voters collected during voter registration exercise while the other stores voting information during voting exercise. The system has fingerprint authentication feature, hence, can detect attempt of multiple voting and perform vote tallying, counting and result publication electronically. Apart from the fact that this system is not cost effective in terms of material, the use of dedicated button and only one means of user authentication is a limitation of the work. Another limitation is that the system uses computer during voter registration, voting and vote counting. According to, firstly database is created in the first MCU with the help of fingerprint module and a PC and after the completion of voting process, counting process can be easily performed by connecting the second MCU with PC and the result can be stored in PC in suitable file format such as excel file [10]. This makes the voting machine fairly costly and slower because it involves the use of computer and moving the MCU from the pooling unit and then connecting to the computer before counting of votes and results ascertained. Other weaknesses of the developed electronic voting machine are the use of buttons for each party, no security features for enrolment of voters and deletion of voters in the register as a single press of enrolment or deletion button can perform the action and resetting of the voting by pressing the reset button. In addition, as the results of the election are stored in human readable file format such as excel file, the results can easily be manipulated and thus may not reflect the actual voting by the voters [10]. Carried out Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections.

In the work, Arduino Mega 2560 is the microcontroller used and interfaced with ESP8266 WIFI Module, RC522 RFID reader and R307 fingerprint scanner. The system has two main modules named Election Commission (EC) and Student module. The election commission module gives administrative function to election officers such as candidate addition and removal while the student module is used for voting exercise only. The election commission module can only be accessed from a computer while the voting machine provides the user interface for voting. The system stores data on the EEPROM of the microcontroller and also send the data using the ESP8266 WIFI module to a computer for data storage and processes. Though the system has high configuration and uses double authentication of voters, it still used a dedicated button for each party, limiting the number of parties that can be handled by the electronic voting machine presented RFID Based Biometric Electronic Voting Machine. The electronic voting machine was based on Arduino Mega 2560, RFID reader and fingerprint interfaced to the microcontroller using MAX232. The electronic voting machine has the function of voter enrolment, authentication, double voter detection and prevention, voter result tallying processing and election winner determination. The system is limited due to the use of dedicated button for candidate in the election.

In all the above reviewed work, it is discovered that scalability could not be provided. Since all the authors are using a dedicated button for each party, the number of parties to be accommodated is very limited to the limitation of the pins of the microcontrollers. In addition, none of the reviewed work has text-to-speech capability, hence, cannot be used by visually impaired individuals effectively. This is because, the visually impaired persons when being assisted by another person, will not be able to know if the choice voted is the he/she choose.

Hence, this present paper presents an electronic voting machine that had its functionality and capability increased. Apart from security enhancement, the number of parties are large in comparison with what is currently obtainable as the party is not assigned any dedicated pin rather a code is generated for the party which can be stored in the memory of the electronic voting machine. In addition, the test-to-speech capability of this electronic voting machine makes it mor user friendly even for the visually impaired persons. Also the number of voters this present electronic machine are larger because it is using SM630 fingerprint scanner.

Design Methodology

The methodology employed for the design of this system ensured that the objectives of the design were achieved. The system block diagram is shown in Fig. 1.

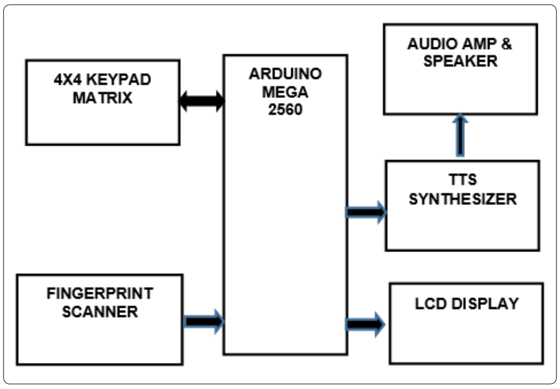


Figure 1: Block Diagram

Arduino Mega 2560

The heart of the electronic voting machine is the microcontroller, which controls the operation of the system. Arduino Mega 2560 was used for the design of the electronic voting machine due to the following reasons.

1. The EEPROM of Arduino Mega 2560 is 4KB, hence can accommodate up to 4000 bits of data on this memory. This memory can be used to store up to 400 voters' data and 1000 parties' data in the memory. This is achieved by allocating 10 bytes of EEPROM memory to each voter and 2 bytes for political parties.
2. The processing speed of Arduino Mega 2560 is 16 Mhz. This fairly lower in comparison to Arduino Mo (48MHZ), Arduino Duo (84MHz) and Arduin Tian (560MHz), however, Arduino Mega is more suitable for this application as none of these (Mo, Duo and Tian) has EEPROM. Other Arduino microcontrollers have 4KB EEPROM or less.
3. The interface (input/output) pins of Arduino Mega 2560 is 70 in total (54 digital and 16 analogue) which is the highest obtainable in the Arduino family. Hence, the device has enough pins for interfacing other peripherals required for the purpose of this research.
4. Arduino Mega 2560 has 256KB of flash memory and 8KB SRAM which is enough to accommodate program files and variables. Other Arduinos with higher flash memory and/or SRAM do not have EEPROM or they have lower EEPROM and/or pins.
5. Arduino Mega 2560 provides enough current to drive CMOS devices connected to it directly, low power consumption and wide range of power supply (6 – 20V)

Figure 2: Arduino Mega 2560

Text-to-Speech (TTS) Synthesizer

For the texts being displayed on the Liquid Crystal display (LCD) to be converted to speech which can be heard on the speaker, a text-to-speech (TTS) synthesizer was incorporated in the electronic voting machine. Though text-to-speech (TTS) synthesis is a complex process, the use of TTS integrated circuit (IC) simplifies the process as all needed operations are performed by the dedicated ICs. The TTS was designed using TTS256 and Magnevation's Speakjet.

Dictionary of words-to-allophones are contained in the TTS256 chip and are used to convert English texts into a sequence of phonemes. In addition, TTS256 comes with inbuilt 600 rules database to convert English texts to phoneme codes, hence, speech can easily be generated from ASCII text in microcontroller-based embedded applications.

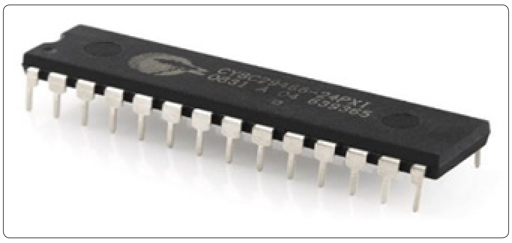


Figure 3: TTS256 IC

The phonemes generated by the TTS256 can be feed into SpeakJet which then converts the phonemes into sound. The SpeakJet chip is a low cost IC which is programmed with 72 speech elements, 43 sound effects and 12 DTMF touch tones. In addition, sound effects such as the pitch, rate, bend and volume can be controlled. The output of the speech synthesized is then feed to the amplifier for amplification and sound production at the speaker.

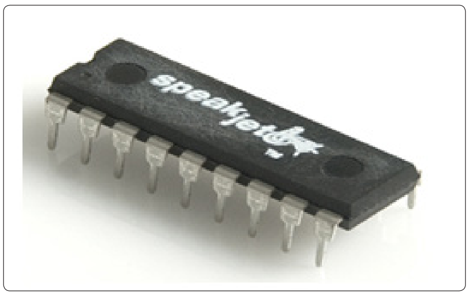


Figure 4: Magnevation's Speakjet IC

Audio Amplifier and Speaker

The audio amplifier receives input from the TTS synthesizer and outputs sound on the speaker. The main purpose of this unit is to enable more friendly user interaction with the device especially for visually impaired persons.

The audio amplifier was designed using LM386. The LM386 is a power amplifier designed for use in low voltage consumer applications. The rational for choosing the amplifier for the application are few components are needed for biasing, low power consumption and high amplification gain (up to 200). 8Ω speaker was selected for this work as the amplifier has the capacity of driving the speaker to produce appropriate speech. LM386 is an eight-pin dual-in-line package (DIP) IC with pin configuration as shown in Fig. 5.

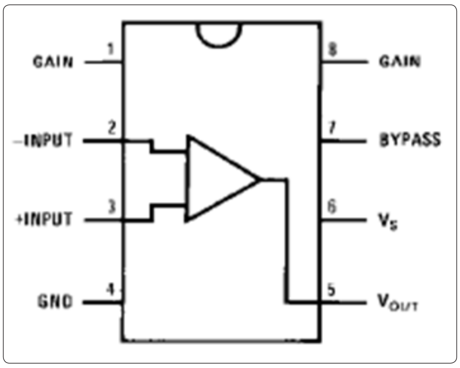


Figure 5: Pinout of LM386 Audio Amplifier IC

Fingerprint Scanner

Fingerprint technology has been used over the years for identification purpose as fingerprint is unique to every individual, even identical twins have different fingerprints. The incorporation of fingerprint technology into the system ensures higher security of the system, enhances its reliability and increases faster response of the machine.

The fingerprint module used for this system is SM630. SM630 integrated fingerprint module consists of optical fingerprint sensor, high performance DSP processor and Flash. It boasts of functions such as fingerprint enrollment, fingerprint deletion, fingerprint verification, fingerprint upload, fingerprint download among others.

Figure 5: SM630 Fingerprint Module

The fingerprint module was chosen due to its higher fingerprint template memory (768 templates), low power consumption, high performance and TTL communication interface.

4x4 Keypad Matrix

For user to interact with the electronic voting machine, 4x4 Alphanumeric keypad was employed. The keypad enables users to impute data into the system which are typically password for administrative purpose, operation selection, voter identification number (VIN), phone number, political party ID and operation cancelation or confirmation.

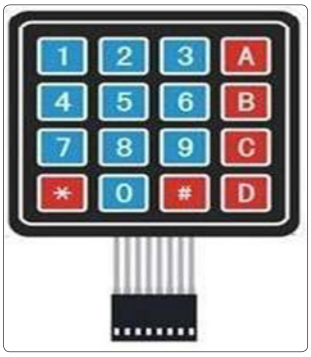


Figure 6: 4x4 Keypad

LCD Display

The display unit for the electronic voting machine is 20x4 liquid crystal display (LCD). LCD is an electronic display module which uses liquid crystal to produce a visible image. The LCD used displays 20 characters in a column over 4 rows as shown in Fig. 7.

Figure 7: 20x4 Liquid Crystal Display (LCD)

The display was selected as it can easily be interfaced with the microcontroller, cost effective and can display up to 40 characters a time. Therefore, it enhances user friendly characteristics of the electronic voting machine as users can clearly read and communicate with the machine effectively.

Power Supply

The power supply is critical part of the system, as without power, the machine cannot work. The machine operates on 5V DC power supply, hence, 3.7V lithium battery was used. The battery voltage was boasted to give 5V output to power the machine using boost converter technique. The boost converter was designed using MT3608 current mode step-up converter IC, which is intended for small and low power applications. MT3608 was selected due to its high efficiency (up to 93%), stable output and few peripheral components for voltage setting.

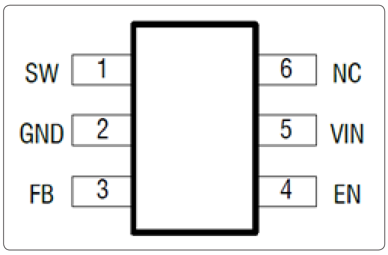


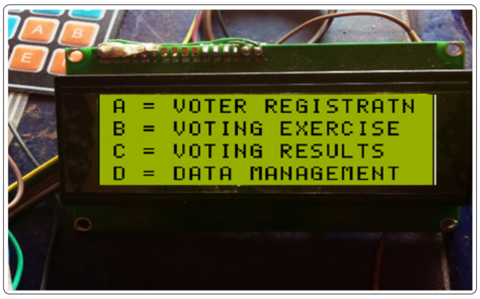
Figure 9: Pin configuration of MT3608 IC

Figure 10: 3.7V Lithium Ion Battery

In order to charge the battery, a 5V 2A DC supply adaptor is employed.

Machine Description

The electronic voting machine designed and developed has four major menus, which are voter registration, voting exercise, election results and data management as shown in Fig. 11.



```
A = VOTER REGISTRATN
B = VOTING EXERCISE
C = VOTING RESULTS
D = DATA MANAGEMENT
```

Figure 11: Main Menu of the E-Voting Machine

Voter Registration

For voter to be registered and data captured into the database of the machine, this option is selected. There are security features embedded in this section to ensure that only valid voters' data are acquired by the machine and that an authorized registration officer is present during registration. Though registration officers can be many, for the purpose of demonstration, five officers were added with the password and name shown in Table 1.

Table 1: Registration Officers' Details

S/No	Name	Password
1.	Mr. Tivde	287
2.	Mrs. Eunice Afolabi	895
3.	Mal. Yunusa Ismaila	392
4.	Mrs. Ngozika Asogwa	647
5.	Mr. Ocheja Agbonika	573

Once the registration option is selected from the main menu, the registration officer in charge enters the password and proceed to registration. However, if the password is incorrect, registration access will be denied and after five attempts, registration access will be locked for five minutes. In case the machine is powered ON and then OFF when the attempts are up to five, the timer is reset to 0 and start counting up until five minutes before it unlocks the registration access. This was achieved by allocating a particular EEPROM address to monitor the access of registration.

During registration, voters are required to place their thumb for biometric capture and it is linked with the voters' card using the RFID technology. The system has features to detect cases of double registration.

Voting Exercise

This menu enables eligible voters who had been registered to exercise their franchise. The voter is requested to place the voters' card on to be scanned and also the finger on the fingerprint scanner to capture the biometric. If a match of the fingerprint is found in the database with the voter card is found, the voter will be granted access to vote, otherwise, voting access is denied.

When the voting access is granted, the voter is requested to enter the code of the party intended to vote for. If the code is correct, the name of the party is displayed so the voter can check if he intended party is what is shown and then can proceed to vote, cancel voting or reenter party code. The list of registered political parties and their voting codes are shown in Table 2.

Table 2: Political Parties Registered and Their Voting Codes

S/No	Political Party	Voting Code
1.	ABC	001
2.	CMC	002
3.	AGM	003
4.	MMF	004
5.	ITF	005
6.	ILC	006
7.	GMB	007
8.	AAL	008
9.	SSL	009
10.	EEE	010
11.	MPS	011
12.	GND	012
13	GDP	013
14.	APA	014
15.	ALN	015
16.	APO	016
17.	NNP	017
18.	PPS	018
19.	GSS	019
20.	MSC	020

The electronic voting machine has security architecture to detect attempt of multiple voting as voter data that had already voted is marked and thus, will not be allowed to vote again in the election.

Election Results

The results of section of the electronic voting machine is categorized into two. These are general election results and declaration of winner for the election. This menu is strictly for administrators only, hence, both options are password protected. The general election sequentially announces the total number of votes scored by each political party, shows the total number of registered voters and the total number voted in the election. The election winner declaration option announces the winner of the election with the total number of votes the party got in the election.

Data Management

The data management option is for administrators only and was added to make the electronic voting machine flexible. During design and programming of the voting machine, registered political parties where added. However, in event of new party being registered, the data management option provides a means of including the newly registered party in the party database of the machine. Voters' data and voting count cannot be altered, however, there is room to delete all the data in the machine (voters' data and election data) or election data only to make the machine useable in different elections and/or voting centres.

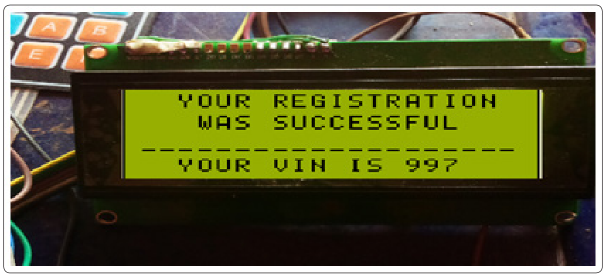
Experimentation and Results

At the completion of the development of the electronic voting machine, the performance of the machine was experimented using ten (10) registered voters. The evaluation of the machine covered all the four menus of the electronic voting machine.

Voter Registration

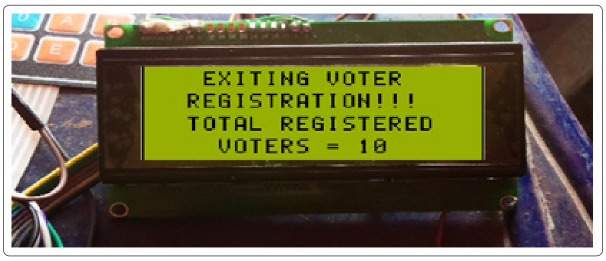
The machine was experimented to know its capability of voter registration and the results obtained showed that machine functioned as designed and intended for voter registration.

At the completion of registration, successful registration and VIN is shown on the LCD as shown in Fig. 12 and Fig. 13 shows the total number of registered voters when exiting the voters' registration exercise.



```
YOUR REGISTRATION
WAS SUCCESSFUL
--------------------
YOUR VIN IS 997
```

Figure 11: Successful Registration of Voter



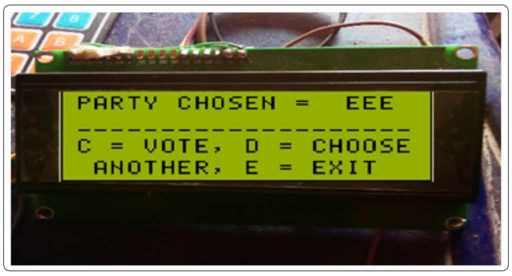
```
EXITING VOTER
REGISTRATION!!!
TOTAL REGISTERED
VOTERS = 10
```

Figure 12: Total Number of Registered Voter

Voting Exercise

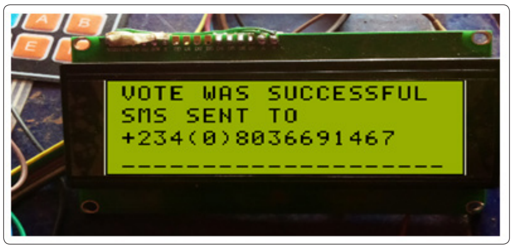
During voting exercise, the machine constantly scans the fingerprint module to detect if fingerprint is placed on the scanner. Once fingerprint image is detected, the machine automatically searches for a match in the database, if found and not marked for voted, the voter is given access to cast vote and when the voting was successful, a text massage will be sent to the voter and the vote added to the appropriate political parties.

Fig. 13 shows the political party chosen by a voter and massage for the successful voting is depicted in Fig. 14.



```
PARTY CHOSEN =  EEE
--------------------
C = VOTE, D = CHOOSE
ANOTHER, E = EXIT
```

Figure 13: Voter's Choice of Party



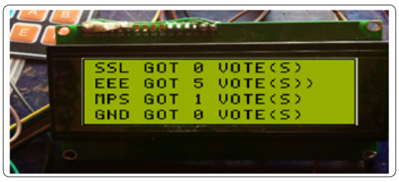
```
VOTE WAS SUCCESSFUL
SMS SENT TO
+234(0)8036691467
--------------------
```

Figure 14: Successful Voting Exercise

Election Results

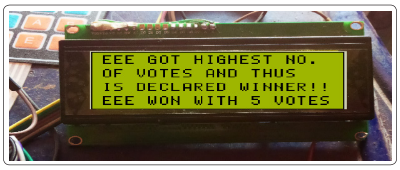
The experimental results showed that the machine successfully tallies the votes. When the general election option in the Election result menu is selected and correct password is entered, the machine sequentially declared the number of votes scored by each political party. The winner of the election was declared with the number of votes got when the election winner option was selected and the password entered correctly.

Fig. 15, Fig. 16 and Fig. 17 show the experimental results for the election result menu of the electronic voting machine.



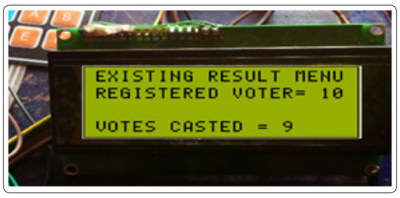
```
SSL GOT 0 VOTE(S)
EEE GOT 5 VOTE(S))
MPS GOT 1 VOTE(S)
GND GOT 0 VOTE(S)
```

Figure 15: Declaration of Results of Four Parties



```
EEE GOT HIGHEST NO.
OF VOTES AND THUS
IS DECLARED WINNER!!
EEE WON WITH 5 VOTES
```

Figure 16: Declaration of Winner in the Election



```
EXISTING RESULT MENU
REGISTERED VOTER= 10

VOTES CASTED = 9
```

Figure 17: Declaration of Number of Votes Casted

Conclusion

From the experimentation results on text-to-speech enabled electronic voting machine indicated that the electronic voting machine performed creditable as required of any functional electronic voting machine with an added capability of text-to-speech.

Acknowledgement

We thank the Almighty God for making the completion of this work a success. The contributions of the Engr. Dr. Abuh Abdullahi, Engr. Dr. N. S. Parkaa, Engr. P. S. Awuhe P G. and Engr. Dr. J. A Enokela among others towards the success of this work are well acknowledged.

References

1. Kumar DA, Begum TUS (2011) A Novel design of Electronic Voting System Using Fingerprint. International Journal of Innovative Technology and Creative Engineering 1: 12-19.
2. Umar BU, Olaniyi OM, Ajao LA, Maliki D, Okeke IC (2019) Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines. KINETIK 4: 115-126.
3. Kohno T, Stubblefield A, Rubin A, Wallach DS (2004) Analysis of an Electronic Voting System. In Proceedings of IEEE Symposium on Security and Privacy 1-23.
4. Olaniyi OM, Aruloun T, Omidiora EO (2013) Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions. International Journal of Computer and Information Technology 02: 1122-1130.
5. Holmes S (2020) Republicans are right: democracy is rigged.

But they are the beneficiaries. A Publication of the Guardian of Thursday. Retrieved from https://www.theguardian.com/commentisfree/2020/nov/26/democracy-rigged-trump-biden.

6. Bannet J, Price DW, Rudys A, Singer J, Wallach DS (2004) Hack-a-Vote: Security Issues with Electronic Voting Systems. Security & Privacy IEEE 2: 32-37.
7. Haque SR, Asaduzzaman MM, Bhattacharjee P, Ashik AU, Kormokar R (2015) Finger Print Enabled Electronic Voting Machine with Enhanced Security. International Journal of Engineering and Technology (IJET) 5: 268-273.
8. Kalash Srivastava, Chawla MPS (2018) Fingerprint based Electronic Voting Machine with Inbuilt Identification and Verification System. Journal of Advances in Electrical Devices 3: 6-13.
9. Thakurendra Singh, Chirag Sharma, Rahul Sharma, Avadh Pratap Sharma, Yogesh Kumar Upadhayay (2020) "Biometric Electronic Voting Machine" Published in International Journal of Trend in Scientific Research and Development (IJTSRD) 4: 617-620.
10. Vinayachandra S, Poornima KG, Rajeshwari M, Prasad KK (2020) Arduino Based Authenticated Voting Machine (AVM) using RFID and Fingerprint for the Student Elections Journal of Physics: Conference Series 1712.