Research Article

A Biometric based Software Solution for E-Voting using networking

Nathan David[1*], Daberechi Ubachukwu[2], Hyacinth Ijomanta[2], Chukwuebuka Gil-Ozoudeh[2]

[1]Lecturer and Project Supervisor, Department of Electronic Engineering, Faculty of Engineering, University of Nigeria, Nsukka.

[2]Final Year (2014), Undergraduate Project, Department of Electronic Engineering, Faculty of Engineering, University of Nigeria, Nsukka.

*Corresponding author
Nathan David
Email: nathan.david@unn.edu.ng

Abstract: The problem of voting in Nigeria is still critical in terms of safety and security. This paper deals with the design and implementation of a software based voting system using fingerprint authentication in order to provide a high performance with high security to the voting system. The design incorporates a database which holds the personal data of every registered voter, the Graphic User Interface (GUI) which provides a user friendly interface. The proposed EVM also allows the voters to scan their fingerprint for authentication, which is then matched with an already saved image within a database. The software is implemented completely as a .NET managed code in C# programming language with database Microsoft SQL Server support. Upon completion of the voting process, the results from the different polling centre are uploaded to a central server for verification and onward publishing using a website that is accessible by all. At the end of this work, we hope that the proposed electronic voting machine which is fast, efficient and fraud-free can be adopted for the conduction of elections.

Keywords: Electronic voting, biometric systems, minutiae, authentication, networking

INTRODUCTION

Elections allow the populace to choose their representatives and express their preferences for how they would be governed. The integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behavior and must be transparent and comprehensible, that voters and candidates can accept the results of an election. For this to happen, the system of government based on the principle of majority decision making [1], is the preferred solution since it is characterized by a credible, transparent, fair to all and ultimately, efficient electoral process.

Many people use the paper ballot to choose their representatives through the traditional voting systems. This method has been used for a long time. This method requires the physical presence of the voter to choose one of the candidates in confidence and then put the paper in the ballot box but this method has several disadvantages. For example, the voters must go to voting station and wait in a queue to cast their vote and in some cases the voters are being subjected to harassment by some officials. Also this method is easily susceptible to fraud and change of votes cast. Furthermore, it is difficult to collect the ballot boxes

and transport them to the main centre. And most importantly, the error that may occur during the counting of votes, in addition to the high cost of process and time spent.

In some countries including Nigeria, there are security problems which affect the functioning of the electoral process. For example, when the polling station is under threat, the election process will definitely be altered and that makes some voters to leave the polling station in order to secure their lives. Nigeria has been branded with negative insignias of sharp electoral practices, pre/post-election violence leading to the destruction of lives, assets and overall distrust within the electorate over falsified election results which culminates into their rejection of poll results.

In Nigeria, the inability of the Independent National Electoral Commission (INEC) to conduct credible elections has demeaned our claims of democracy. The unfortunate situation where candidates cannot trust election results has become a widespread problem. Most contestants view results released by INEC as doctored with obvious manipulations. As a result of this common view, most candidates engage in various forms of electoral and societal vices so as to manipulate the results in their favour.

Biometrics is becoming an essential component of personal identification solutions, since biometric identifiers cannot be shared or misplaced, and they represent any individual's identity. Biometric recognition refers to the use of iris, fingerprint, face palm and speech characteristics, called biometric identifiers. Fingerprint matching is a significant part of this process. It is an extremely difficult problem, due to variations in different impressions of the same finger. Fingerprints are unique to each individual and they do not change over time [2]. Fingerprint identification is based primarily on the minutiae. Minutiae matching essentially consist of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings [3]. The major minutiae features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). Biometrics holds the promise of fast, easy-to-use, accurate, reliable and less expensive authentication for a variety of applications. Electronic voting systems could improve voter identification process by utilizing biometric recognition.

In this paper, we describe a Biometric based Software Solution for E-Voting using networking.

EXISTING VOTING EQUIPMENT
In the recent years, voting equipment which was widely adopted are may divided into five types. [4]
1. **Paper-Based Voting:** The voter gets a blank ballot and uses a marker to indicate the candidate he intends to vote for. However, this process may take a long time to get a hand count under the current system. Paper ballot counting and recounting generates endless arguments about whether the 'marker' print crosses inside the square/circle.

2. **Lever Voting Machine**: Lever machine is peculiar equipment, and each lever is assigned for a corresponding candidate. The voter pulls the lever to poll for his favourite candidate. This kind of voting machine can count up the ballots automatically. Because its interface is not user-friendly enough, giving some training to voters is necessary. However, these machines are subject to malfunctions that can invalidate hundreds of votes.

3. **Punch Card**: The voter uses metallic hole-punch to punch a hole on the blank ballot. It can count votes automatically, but if the voter's perforation is incomplete, the result is probably determined wrongfully.

4. **Optical Voting Machine**: After each voter fills a circle corresponding to their favourite candidate on the blank ballot, this machine selects the darkest mark on each ballot for the vote then computes the total result. This kind of machine counts up ballots rapidly. However, if the voter fills over the circle, it will lead to the error result of optical-scan.

5. **Direct Recording Electronic (DRE) Voting Machine**: DRE integrates with a keyboard; touch screen, or buttons for the voter press to poll. Counting the votes is done very quickly. But the DREs are costly and they fail to prove that the vote stored in the machine is really what the voter saw and confirmed on the screen.

**PROPOSED DESIGN**
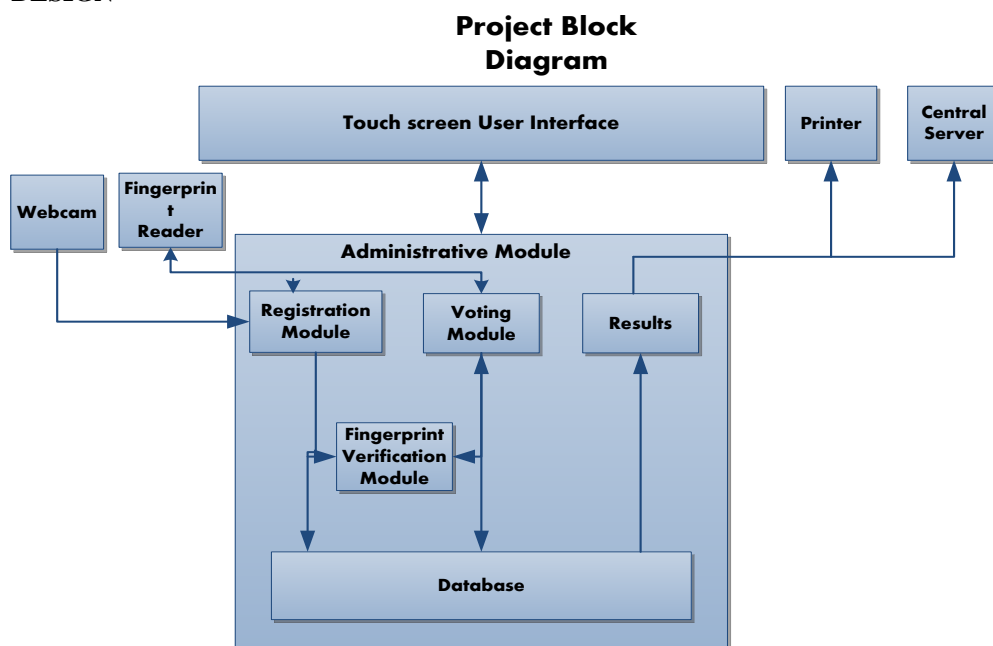
Fig-1: Project Block Diagram

HARDWARE IMPLEMENTATION: FINGERPRINT SCANNER
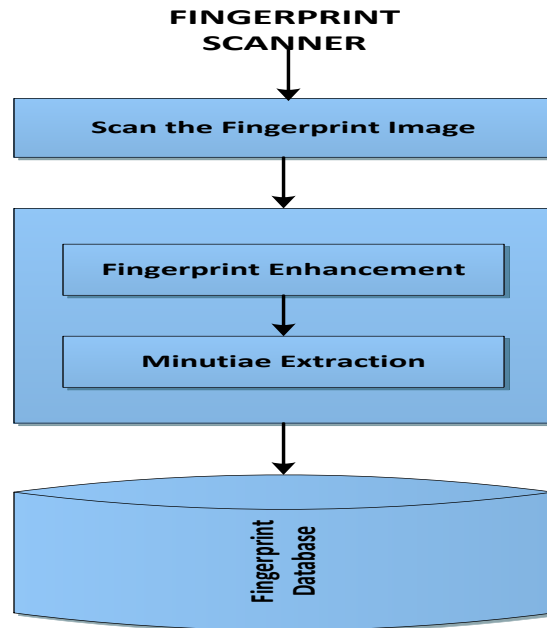
Fig-2: Flow Process for the Implementation of Fingerprint Captured

The flow process, shown in Figure-2, summarizes clearly the implementation of the fingerprint scanner (DigitalPersona) we employed in this project. The Process involved is very simple. First, the chosen finger for example, the thumb is captured and extracted. The fingerprint template is then enrolled and store in a database. This primary process is done during the registration of eligible voters. After that, the chosen finger can be live scan. The fingerprint template is then processed, by a special algorithm designed to function with the fingerprint, and extracted. It will subsequently match the scanned fingerprint against the stored template. Upon authentication, an eligible voter will then have the access to vote for their desired candidates. Mismatched fingerprint certainly would deny the voter from participating in the voting process. This is illustrated in Figure-9.
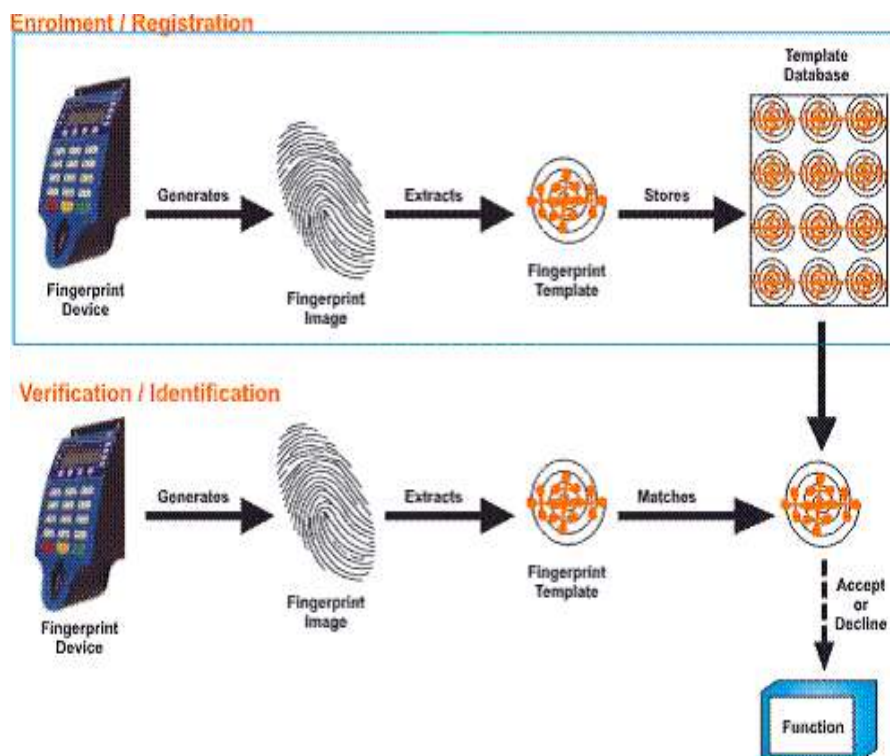
Fig-3: Enrolment and Authentication Processes

SOFTWARE DESIGN AND IMPLEMENTATION
Database Design
The database forms the backbone of the application. Nearly all the activities in the different modules interact with the database. The database is designed on the results of the requirements specification.

i.   The Admin Login table which contains all the electoral officers that have the privilege to access the system.
ii. Admin Page table which stores the administrators' login usernames and passwords.
iii. Contestant Registration Table which holds the data on the contestants vying for the different positions.
iv. Voters Registration table which stores the bio data of the eligible candidates (students) involved in the election, the scanned finger print and passport photograph of each registered voter.
v.   Departmental table which holds the departments represented in each faculty.
vi. Faculty table which holds the faculties in UNN.
vii. Voting Result Table which holds the result of each voter's votes.

GRAPHIC USER INTERFACE (GUI) DESIGN: FRONT-END DESIGN
The front end design comprises the Graphic User Interface (GUI) design and its effects. The GUI provides a graphical representation of the software. Its design gives an emotional feel of the system from the user's perspective. It is object-oriented, consisting of various modules interacting with a central database.

The Login Page.
This page gives access into the voting software and can only be accessed by pre-defined administrators, either as a Polling Admin or Main Admin, as shown in Fig-4. The Polling Admin has limited administrative functions such as coordinating the registration and voting processes for the polling station, and sending the result to the central database. The Main Admin on the other hand, can perform all these functions, and in addition, is responsible for creating new Polling Administrators. It is the Main Admin who is responsible for collating and publishing the results from the different polling centres to the internet for public viewing.


Fig-4: Administrator Page

The Admin Page.
This page is the home of the administrator and provides navigation options, using buttons for interaction with the other modules and sub modules. It is peculiar to the logged in administrator.

The Registration Page/module
This comprises the registration pages for both the contestants and voters. The contestant registration page captures the necessary data for the contestants vying for the different positions such as their basic data (name, registration number, department and passport). The voter registration page, shown in Figure-5, captures the voter's information (basic data, passport photograph and fingerprint) and enroll them into the database. These pages also check against invalid entries/incomplete registration.
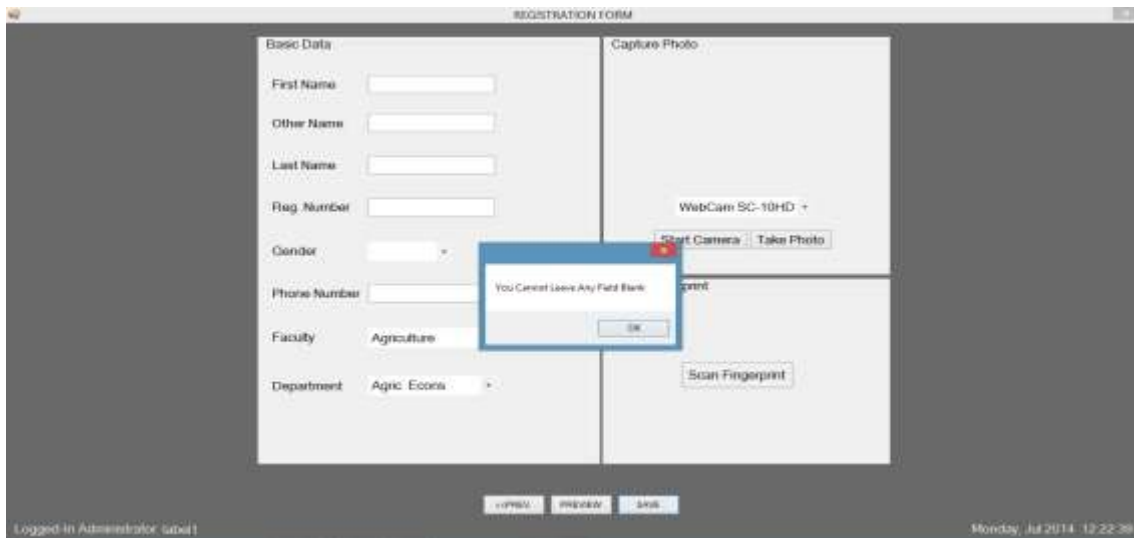
Fig-5: Voter Registration Page

The Preview Page

This page shows a summary of the registered student's information and helps to readily check for errors in the student's input data. It is accessed from the Registration Page which protects against Preview of incomplete registration.

The Voting Module

This is the most fundamental module of the EVM. It provides the platform for voting and is the seal of the electoral process. It comprises the Authentication Page, the Voting Page and the Voting Result Summary page. The Authentication page takes the voter's registration number and fingerprint and compares it to the registered data in the database. This page provides access to the Voting Page. The Voting Page, shown in Figure-6, displays all the contestants from each department in the Faculty for each office/position. As each voter votes, the next office and contestants are displayed till the last office is voted for. The Voting Result Summary page, shown in Figure-7, shows the voter the summary of their votes and prints out the result slip for the voter at the end of the session. It also allows the voter to make adjustments should they change their mind about their choice candidate for any office.

Fig-6: Voting Page

Fig-7: Voting Result Summary Page

The Results Page

This page, accessible only by authorised personnel, shows the total result of the elections at each polling point. The results are now saved and uploaded to the central server from here. Figure-8 shows the result from 5 voters for the different positions available in the sample NUESA elections.
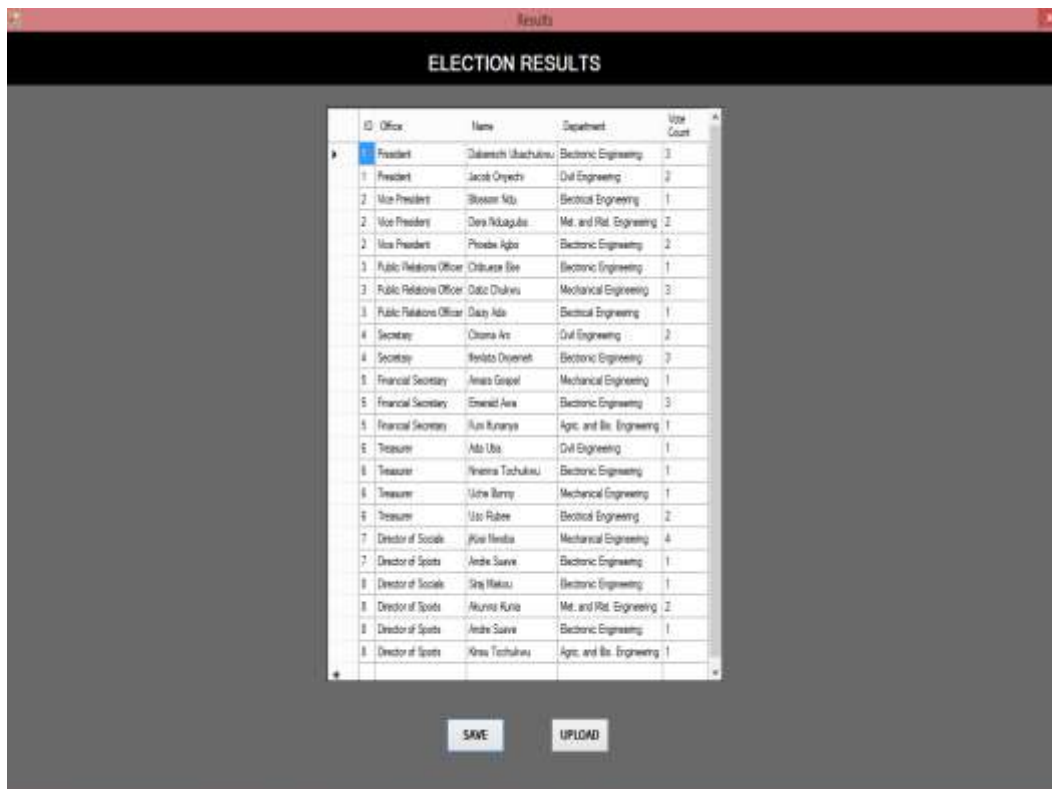

Fig-8: Election Result

BACK-END DESIGN

This basically refers to the functionalities/ codes used in our design processes. For the software analysis and graphic display, we are using the C# programming language with SQL database support and fingerprint security. In the design of this software

section, we took great care to ensure a level of security. Firstly, in order to launch the program, a password login page appears. This ensures that only the registered administrators are allowed to launch the program. Secondly, to access the voting module, the voter is

required to input their registration number and then run their fingerprint on the fingerprint reader to authenticate their identity. Hence only registered and eligible voters are allowed access to the voting form. The Process Flowchart of Figure-9 clearly illustrates this.
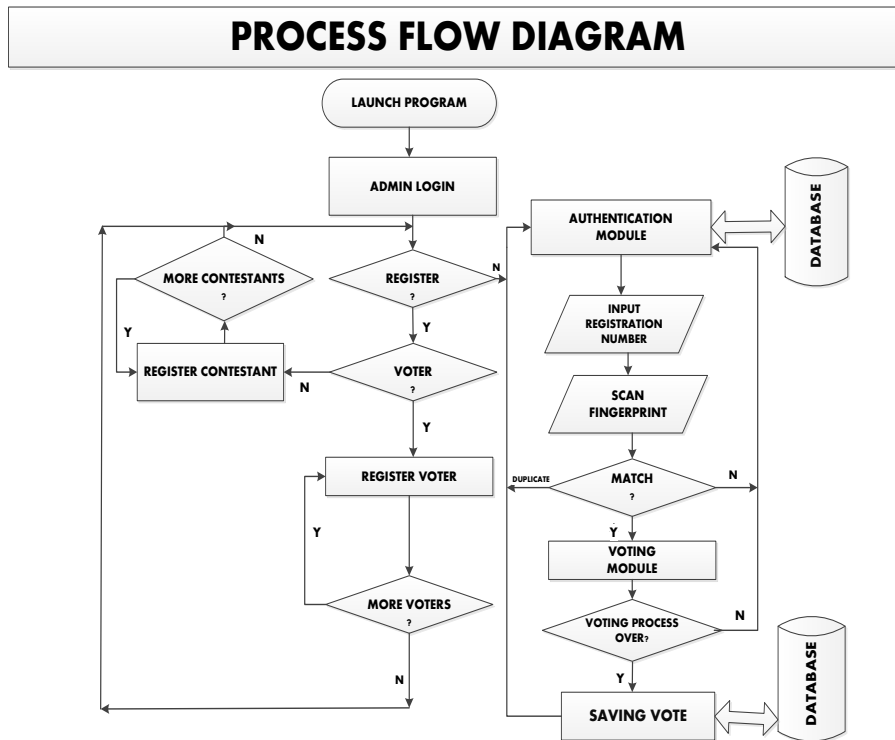
PROCESS FLOW DIAGRAM

Fig-9: Process Flowchart

NETWORKING

At the end of the elections, the voting results from the various polling units (departments, in our case) are uploaded to the central server (web server) via the internet for onward publishing of results by the central administrator, as shown in Fig-10.

The central administrator can be a polling unit administrator or a different administrator, otherwise known as the main or super administrator with a unique login identity. The super administrator is the only authorized personnel to publish the final election results for public viewing via the internet.
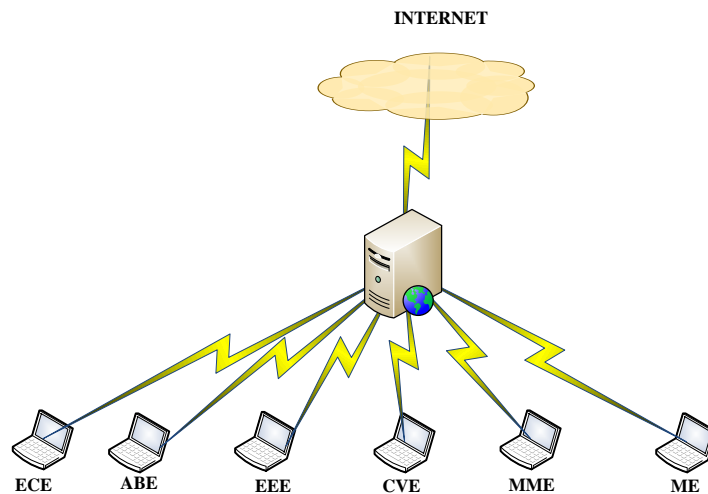
Fig-10: Network Design

REFERENCES

1. Democracy. Washington DC: Microsoft Encarta, 2008-2009.
2. Sobia B, Ummer I, Ayesha K, Usman I, Hassan MJ; Electronic Voting System Using Fingerprint Matching with Gabor Filter. Proceedings of International Bhurban Conference on Applied Sciences & Technology Islamabad, Pakistan, 2011; 130-135.
3. Hazzaa F, Kadry S; New System of E-Voting Using Fingerprint. International Journal of Emerging Technology and Advanced Engineering, 2012; 2: 355-363.
4. Mercuri RT; Physical Verifiability of computer systems. Proceedings of 5th International Computer Virus and Security Conference, March, 1992.