AUTOMATED VOTING SYSTEM USING BIMODAL IDENTIFICATION AND VERIFICATION TECHNIQUE

Joseph Bamidele Awotunde

Department of Physical and Computer Sciences, McPherson University, Seriki-Sotayo, Ajebo, Ogun State

Corresponding author: Joseph Bamidele Awotunde, jabonnetbylinks@gmail.com

ABSTRACT: Nigeria voting system is characterized with violence and malpractices, where some people used another person voting card to vote and many have more than one voter's card in their possession, which allow them to vote more than one time. These problems does not peculiar to Nigeria alone but includes other countries that are using manual method of voting system. In order to combat the aforementioned problems the paper therefore proposed a secure voting system using bimodal identification and verification system for voting and registration of voters. The purpose is to uniquely identify voters and to eliminate the possibility of double registration at the polling booth by the voters. Also the issue of double voting will also be abolished. Further study can look into web based and mobile based automated voting system, which allow voter to catch their vote anywhere and anytime.

KEYWORD: Voting system, automated, recognition, Verification, Bimodal.

1.0 INTRODUCTION

Voting allows groups of people to make decisions, this is used to choose between tough plans of actions or to decide who is best appropriate to be conferred a prize. Therefore, voting is a process that allows group of individuals to choose between a numbers of selections.

However, each countries has certain criteria for voting regarding elect leader of their own choice during election period. Therefore, keeping the accurate record of voters is very relevant and most important.

Voter registration is usually taking manually using old file system method and paper sheets in almost all the developing countries. According to expert in politics, the manual record and counting of ballot paper for the purpose of selecting leaders into various posts in developing countries is becomes difficult for the management. Lack of adequate record keeping has indeed degenerated to a greater level especially in Nigerian political system. Election malpractices have consistently remained a bane of Nigerian political system. A common form of political malpractices is the deliberate impersonation of the voters. Part of the requirement of a credible election is that the real voter is allowed to vote for the candidate of their choice.

Technology used in the areas of politics has importantly impacted the world today. The emerged use of internet for collaborative purposes has exposed individuals to security issues, which also affect the voting system. Therefore, securing and protecting data of voters are now of great important and become great concern that cannot be overlook. System used for election must be sufficient robust enough to detect duplicitous behaviour, variety of fraudulent, sufficiently transparent and comprehensible for both candidates and voters to accept it results. In Nigeria, elections results is being manipulated in order to favour a particular candidate and always influence the outcome of such results.

An election is credible if it possess the following key elements: free and fair; devoid of partiality, duplicitous and all forms of election malpractices. Candidate impersonation as mentioned earlier is one of the prominent forms of election malpractices due to lack of adequate record of voter registration by the electoral bodies in the developing countries. The idea is that a person can vote more than one time without detect by the official in charge, in some cases under ages people can vote without disallow them from voting. The above aforementioned problems happened because of inefficiency of traditional methods of electoral process. Therefore, the paper proposed a secured and accurate biometric based model to reduce or overcome the problems.

The system of voting by which a voter make his/her choice with the aid of a computer is called electronic voting. The system allow voter to choose with the used of touch-screen display, while a voters with visual disabilities can used audio interfaces. The following four basic steps are considered in an election process, which involved in an electronic voting: the voters make their choices through ballot composition, voters submit their ballots by ballot casting; system records the submitted ballots through ballot recording; and votes are counted by the process called tabulation. The four processes are normally follow with computers even in voting systems that are not directly electronic method (i.e. ballot casting,

recording, and tabulation). Electronic voting involved two steps, ballot composition or choosing a candidate using computer system. There are two different types of electronic voting technologies namely: Internet Voting (I-voting) and Electronic Voting (e-voting).

Electronic voting is more popular among the developed world. Countries like United States, Brazil, Australia, Canada, Belgium, Germany, Romania, France, Venezuela, Philippines, The European Union, Switzerland, Italy, Norway, Romania and United Kingdom have used the system efficiently in their election process. Electronic voting system make provision for people with disabilities. There are different way by which they can make chooses by using joysticks, foot pedals, sip and puff technology and earphones, etc. The system also have touchscreens that can display the information in several languages and voting choices in audio for physically challenge voters. With the above mention attributes the physically challenged people can cast their vote, and these make voting easier, reliable and more comfortable for people with disabilities.

The major problems that characterized the use single biometric systems can be overcome by using bimodal biometric systems. A bimodal biometric system is very reliable due to the existence of multiple and independent pieces of evidence that can be used to differentiate voters. It uses more than one biometric systems to capture human features and behaviours. The integration of two or more biometric system help in meeting the rigorous performance requirements of biometrics. Bimodal helps to meet the severe performance requirements imposed by various applications ([Klu05]).

This paper aim in addresses the problems associated with the use of unimodal used in almost all the existing proposed biometric voting system and the use of manual voting by introduced bimodal identification and verification system in curbed issues of security, time consumed and unreliability of the manual voting system; it also combined the electronic voter registration process so as to minimize the cost of voter registration and to overcome the problem of multiple voters registration.

2.0 REVIEW OF EXISTING RELATED WORKS

Information technology have helped many nations of the world to replaced mechanical system of voting and archaic punch cards with electronic voting (e-voting). The system will help in increasing voter participation, productivity, speeding up election process and election results will be release on time ([Kel03]). ([Cra01]) reviewed works on electronic voting and gives general references relating to electronic voting, the study also included internet-based voting. Among developed nations that used electronic voting are Brazil and India, the system was used for both general and state elections ([Mir04]; [G+11]). The use of Electronic Voting Mechanisms (EVMs) in India has reduced and eliminated the event of invalid votes during elections from the available statistics. The number of invalid votes recorded in India was always more than the winning margin between the candidates before the introduction of EVMs. The systems also helps to ensured that the total number of votes was counted within two to three hours on like before where counting takes up to thirty to forty hours when the manual method of counting were used. In reviewing the EVMs, ([Kit04]) study the setting up the technical communication standards for electronic voting with its process. ([AE11]) evaluates various challenges associated with electronic voting, pick point their benefits and weaknesses. In May, 2007, St. Albans, UK, successfully implemented a full electronic election with no paper-based voting.

There many ways by which people can cast their vote, examples are: Internet, kiosks, Interactive Voice Recognition (IVR) via telephones or mobile phones, and by post. The counting of electronic voting can be done within six minutes, these types of voting counting and recording has been identified to be the fastest ever methods of vote count. Furthermore, there is no invalid vote that was recorded, and all efforts to sabotage the system by means of worms, viruses and Denial-of-Service proved unsuccessful ([Kel03]). The new research and improvement trends in electronic voting now encouraged developed nations to considered the use of e-voting systems over manual voting systems due to their numerous advantages it has over manual methods, the convenience and ease offer both voters and election officials ([G+5]; [AE11]). The electronic voting must still be used with caution disperse it advantages over the paper-based and other mechanical systems, researchers have the believe that such systems could still have challenges ranging from auditing pitfalls, software problems, electricity failure, insider threats, software engineering etc., which could undermining their integrity ([Rub02]; [Leb04]).

([Yee07]) proposed a voting machines system for verification purpose by combines two techniques. The system used an architecture that splits the vote confirmation code into different modules whose integrity is protected with hardware isolation techniques that create a trustworthy vote. To avoid the risk of privacy breaks and to ensure that all voters are treated equally, the system used hardware resets technique that restores the state of sections modules to a constant initial value between consecutive voters. ([Adi08]) designed the first web-based cryptographic electronic voting called Helios. The system is a single

trusted component with Helios server, which uses a public bulletin board (BB). The voters received their password by email during registration phase. The system tried to separates the ballot preparation from ballot casting. Helios authenticate only at ballot casting time, which allow anyone to generate and audit ballots. The system encrypted vote by displaying a hash of the ciphertext after the ballot has been generated. After the voter has been authenticated, the correct preparation of the ballot can either be audited, or the ballot can be cast. Voter can chooses to check the ballot, these allows for checking whether the vote was correctly transformed into the ballot, the ciphertext and the randomness used for encryption will be displayed. The voter obtains a hash of his/her encrypted vote, this will also be posted to BB next to the voter name once the ballot is cast. The ballots are shuffled and decrypted by providing proofs of correctness for both steps during tallying phase.

Government at all levels expect fast, reliable and accurate voter registration at the polls under any conditions, the evidence is the recent used of biometric voting exercises in developing countries like Nigeria, Kenya and Ghana this has help to maintain the integrity and credibility of the electoral process and reduce mistrust and irregularities ([A+15]).

Identification of voters is required during electoral process, this can be done in two phases. Firstly, during voter registration this is done to establish the right to vote (verification) and secondly, at the voting time, which allow voter to exercise their right to vote for candidate of their choice by verifying if the person satisfies all the requirements needed for him/her to vote (authentication).

A review was conducted on the security characteristics of an electronic voting, which are as followings: availability, assurance, reliability, integrity, and confidentiality, ([Neu93]) reviewed and concluded these characteristics are very difficult to fulfill or satisfy. ([Eve04]) study the US online voting system and identified the challenges it faces, [PB04] identified security has one of the major requirements for online voting that is very important and ([ESK07]) suggested that security of electronic voting is very essential after examines the confidentiality security of an e-voting. It is believed that further studies must be carried out to improve on the security of e-voting system not minding the success stories recorded on the use of electronic voting systems, this is very necessary to improve on the security of an electronic voting.

Researchers have proposed biometrics methods of identification and verification of voters to create more secured electronic voting, which will further strengthen the security of this system whether e-voting or i-voting.

([OA14]) proposed multimodal biometrics system aimed to secure electronic voting. The biometrics used were fingerprint and facial recognition, the system used scanned passport of voter for face recognition, which make the system to be weak, since the system did not used a face recognition scanner for the voter's image.

([FS12]) web-based voting system using fingerprint was proposed. This was designed to provide a high security electronic voting system, the proposed system was implemented and evaluated using Student Union Government (SUG) election of a university.

([K+08]) a system that is proficient in handling electronic ballots was proposed. It a multifaceted online e-voting system that accommodates many types of election as the same time for examples, presidential, municipal, parliamentary, amongst others. The functional and non-functional requirements that is part of integrity of an election process was cater for by the system. A well-secured identification and authentication processes which is functional requirement was embedded in the system, this was done by the use of simple combined biometrics. Incorporation of FLAGpsilas system ensured that no votes for a given candidate are lost, which happen due to improper tallying of the voting counts. The phases of an election process are follows in other to ensure transparency throughout the process by guarantee that vote of every voter went in favor of his/her candidate of choice.

([TM16]) proposed an electronic system with multimodal biometrics (i.e. fingerprint and voice recognition), the system can be accessible through computer network with biometrics identification and verification methods. This helps the voters to cast their vote anywhere and anytime, which is the main aim of the paper. The system given a voter identification hardware used to prevent hacker from giving false votes and it also to stop fraud voting. The system also used voice recognition that can be used by physically challenged people that can talk and this is not a common biometric used in verification of a person especially in a voting system.

([Nwa15]) designed and developed a 2-modal biometrics system that is very efficient not only for authenticating persons uniquely but also for eliminating any possibility of double registration during voting registration. The proposed system constitutes what is known in the industry as an ABIS (Automatic Biometrics Identification System). The author belief that with ABIS in place, most, if not all, the errors inherent in the single modality AFIS solution, prevalent in the country will be eliminated. The system was implemented only for voter registration and not with casting of vote.

([Moh16]) proposed an electronic voting system that incorporates fingerprint biometrics. The hardware used fingerprint scanning device that match the fingerprint of the user with the pre-stored fingerprint on the database. The voters fingerprint checked for matching using fingerprints square measure, and if the voter fingerprint doesn't match, the system given an associate degree alert of victimization buzzer. An enabled show |LCD| digital display made with a resistive bit screen was used to display the various candidates and their emblem..

[S+12] proposed an Electronic Voting System (EVS) using Fingerprint Recognition, the system was developed using Matlab with Gabor filter method. Voter scan their fingerprint, which is then matched with the saved fingerprint image stored in database. After voter identification, voters are allowed to cast their vote using LCD and keypad interface. The casted vote will be updated immediately, which make the system to be very fast, efficient and fraud-free.

([AS15]) proposes electronic voting using fingerprint biometric, the system used a touch screen input system, which make it to be user friendly. Voters will be authenticated using their fingerprint for them to poll the vote. GSM system was used for sending results to the corresponding authority and a confirmation sheet was provided through printer to print sheet for the voter who polls the authenticated vote.

([R+14]) proposed web-based voting system with fingerprint biometric to verified eligible voters and aadhaar card to provide extremely security for the system. Web-based system was developed so as to make the voting easier and the voters can cast their vote at appropriate time. The system authenticated voters by scanning their fingerprint and match them with already saved fingerprint image on the database which was retrieved from aadhaar card of the government. Voters' login by their aadhaar card number and password before allow to vote for their favorite candidates.

([AU11]) a minutiae based fingerprint e-voting system was proposed, the system was analyzed using a pilot election among students in selecting their representative. Based on the pilot results the analysis predicted that the proposed voting system reduced if not totally resolves the problems that associated with current system.

([A+13]) used Iris recognition, finger vein to designed an electronic voting machine, the system authenticating voters and polling data security for e-voting, this was done to make sure that vote casting cannot be altered by unauthorized official or voter. Authentication of voters can be done online by formal registration through administrators by entering one time password. The embedded GSM allow Database Administrators in a timely manner send voted data and voters details to a nearby database administration unit with cryptography technique. Authentication can be done offline using Iris recognition, finger vein sensing that enables the electronic ballot reset for permitting voters to cast their votes.

([SPV14]) to avoid faked and repeated voting, the authors proposed an electronic voting system with biometric (i.e. fingerprint scanning) system. This was to also help the accuracy and to speed up the election process. The system uses thumb impression for voter identification, which make the system to have edge over the manual system, and the purpose of the system is to ensure that the voting right are giving to legitimate user. The thumb impression of voters were stored in the database is done as a pre-poll registration. For proper identification, the thumb impression of a voter will be entered as input, the system then compared with the images in the database. If the thumb image matches with anyone in the database access will granted to cast a vote, but in case the pattern doesn't match with the images in the database or signs of repetition, the voters will be denied access to vote or the vote gets rejected. The counting is done promptly and the result is immediate. The system reduced overhead cost of conducting elections so also it reduced the maintenance cost of the election process and systems.

([SD15]) designed electronic voting system using ARM9 microcontroller and low cost fingerprint based electronic voting machine. Controller hardware and software was used for the system, ARM9 controller was used in designing the hardware with KY-M6 fingerprint component. WINCE6 development environment as software code for interfacing the ARM processor with fingerprint part. The system help reduces the time taking in identifying voter, with the implementation of the system in the FP-EVM, have increase it flexibility, portability, and with minimum power consumption. The system is very cost-effective, easily adaptable and user-friendly, the architecture of the system is very simple, have scope for further expansion and fast response to time.

([YG13]) reviewed and studied the development and application of Biometric Electronic Voting System Software (BEVSS) in Ghana election process. Authors used Ghana a pivotal reference to speeding up their implementation. The system was developed using Microsoft Visual Basic 2010 as front end and SQL Server Database as backend. Fingerprint biometric was integrated and used to scan the fingerprint of eligible voters during the registration process and for the authentication and verification on the election day. The system was used and employed on personal computers over a Local Area Network at each polling station during Election Day.

Techniques as it is used by experts/researchers in the area of electronic voting uses unimodal biometric characteristic. Unimodal is cost efficient compare with multimodal biometric. Because of unacceptable performance and inability to operate on a large population areas, unimodal may not be always appropriate in a given domain ([HJ98]). Examples are: face recognition: ([UYA08]); fingerprint matching: ([FYJ09]); Hand Geometry: ([JR99]); Palm Prints: ([DJM02]); Dental: ([F+04]); On-line Signature: ([FKJ05]).

The combination of multiple sources of biometric traits is called multimodal. Multimodal can be done by extraction and matching different algorithms operating on the same biometric, or fusing multiple traits of an individual. These multimodal systems ([RNJ06]; [JR04]; [HJP99]), can improve the matching accuracy of a biometric, which also preventing spoof attacks and increasing population coverage in a given environment ([JR03]).

Verification (authentication) confirms or deny a person's claimed identity (Am I who I claim to be? or "Is this person whom he/she claims to be?") one-to-one comparison of biometric is called verification with the reference template on file; this is illustrated in ([HJ98]).

Identification 'Who am I? or "Who is the person?" attempts to establish a person's uniqueness, there are two ways of identified a person, firstly, from a set of already known characteristics (closed identification problem) or secondly, (open identification problem).

Many designed system especially in an electronic voting machine used unimodal. It relies on a single biometric characteristic which could be hacked by the modern burglars. There are some challenges posed against unimodal biometrics system. Among such are:

Unacceptable error rate due to deformation or aging, noise in the signals produced, intra-class variation. ([RJ03]; [J+04]). Incorrectly labeled as an impostor that resulting through noisy data, which increasing the False Reject Rate (FRR) of the system.

Tuning feature of extraction and matching modules cannot continuously increase matching performance of a unimodal biometric system. ([JBP02]).

Spoof attacks: Behavioral traits such as voice ([EW97]) and signature ([Har81]; [FOJ05]) always exposed to spoof attacks by an impostor attempting to mimic the traits corresponding to legitimately enrolled subjects. Fingerprint as an example of a physical traits can as well be spoofed by etching ridge-like structure on synthetic material like play-doh and gelatine, ([MYH02]; [PK02]).

The above highlighted problems can be overcomes by employed a bimodal biometrics systems in electronic voting system.

The credibility of elections process can be attributed to the use of unimodal biometric, though it use did not entirely make the election to be free and fair. The used of fingerprint verification and card reader that was engaged during 2015 general election in Nigeria reduced electoral fraud, rigging and casting always of ballot boxes, the total number of votes cast could not exceed the number of accredited persons, such difference in figures can easily be spotted by the card reader. The card readers make it impossible for corrupt INEC official or electoral officer to conspire bad politician to change election results. The result sheets at the wards levels must tallied will the voters' records stored in the card readers, if there is an evidence of tampering with the results submitted at the local government level both card reader and the results sheets will be used to verify. But there some problems encounters from the use of fingerprint and card reader used in Nigeria, which is common among unimodal biometric employed in designing the electronic voting system.

3.0 OVERVIEW OF THE METHOD

A review of related literature is conducted to obtain correlated works on electronic voting machine, look at its strength and weakness in order to come up with reliable and secured electronic voting; and to design a unified voting system that is based on bimodal identification and verification technique. Voter Card Holder' fingerprints and facial were captured using SecuGen fingerprint optical scanner and face recognition camera. The model will be simulated using Java Programming Language. In addition, voters' details as well as the template of voter card holder fingerprint and face recognition will be stored using MySQL database management system. Every electronic system requires reliable, potable and security than an E-commerce system, the architecture and software implementation of every electronic voting will determined the feasibility, portability, reliability and the security of such system in achieving its practicability in actual elections ([A+15]). It is therefore, very essential to have level of security by introducing bimodal system of electronic voting.

4.0 THE PROPOSED SYSTEM ARCHITECTURAL FRAMEWORK

4.1 The Framework for the Enrollment and Verification Process

The system is divided into four (4) major modules: (i) Face extractor modules, (ii) Fingerprint extractor modules, (iii) fused image recognition modules and (iv) the Matcher engine. The Face Extractor: Face

Extractor is an engine built from an algorithm developed by using the characteristic patterns of a face. The Fingerprint Extractor, the biometrics systems work with biometric templates extracted from the fingerprint image by the Fingerprint Extractor. Templates are in a data format responsive to biometrics processing by the Matcher and records in the database are stored in this format. The Fingerprint Extractor is actually an engine built from an algorithm developed by using the characteristic patterns of a fingerprint.

The Fusion Engine: The fingerprint and face templates extracted by the Fingerprint and Face extractors are fused together by the Fusion engine to form a single multimodal template that will be stored in the multimodal database. The Matcher engine: This compares the fused template with those already stored in the biometrics database with the aim to check if it belongs to the same person.

The biometric engines as shown in figure 1. The enactment of multimodal system will largely depend on them: that is, the ability of the two Extractors to generate reliable templates and the strength of the Fusion engine to wrap up everything well. The Matcher complements these functions by deciding correctly when to reject or accept a new enrollee. We adopted a biometrics algorithm that delivered excellently well on all key indices of the system.

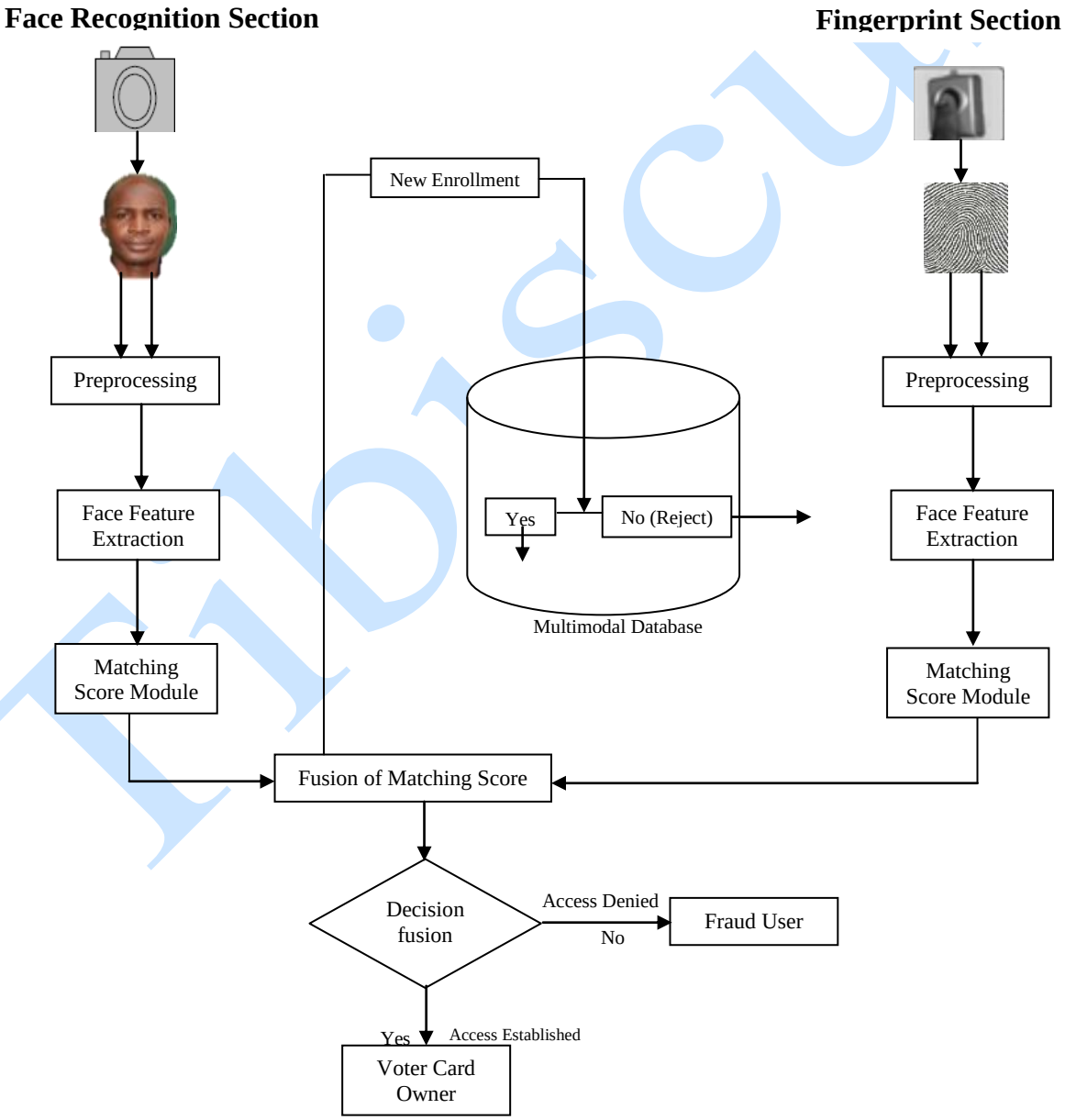

Figure 1: The Framework for the Enrollment and Verification of the Voting System

The Voting Process Flowchart

The flowchart explains the voting process, the step by step illustration of casting vote during voting process. The voter will be identify or verify by the system and determine if the person is who he/she claim to be. The system will check an individual before deny or allow such individual, after passes the authenticity conditions, the voter will logged into his/her voting account. The system will still checked to be sure that the voter has not cast any vote before, if the status is zero (0) the voter will be allow to cast his/her vote, if the status is one (1) it means voter has ready voted and the system reject such voter by not allowing he/she to vote again. Whether a voter is allow to vote or not the database status will always be updated. The update of the database mark the end of voting process of a particular voter. Voting process of the proposed system is described in the Fig. 2.

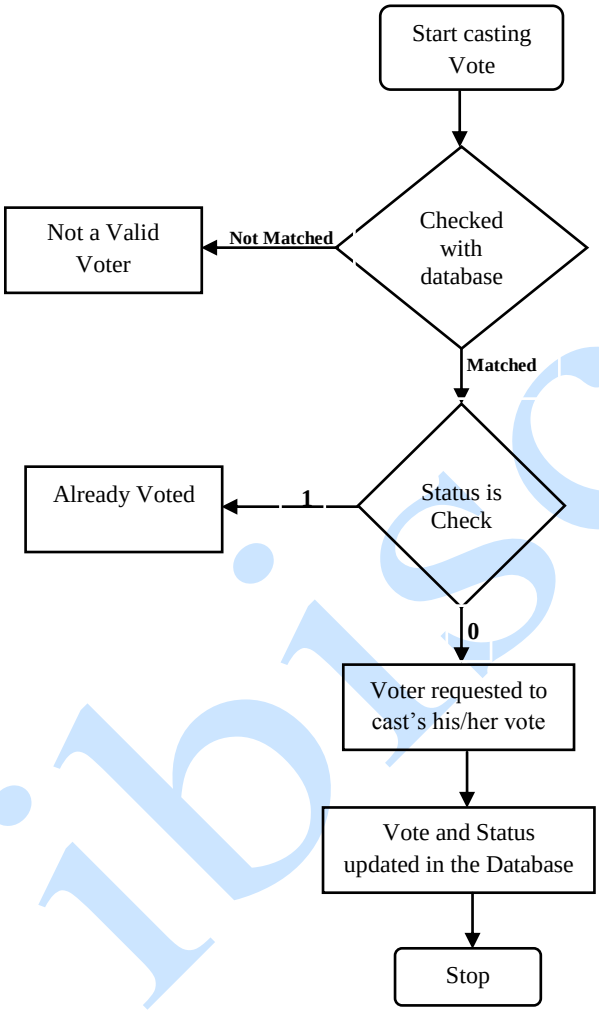

Figure 2: The Voting Process Flowchart

5.1 Fingerprint Feature Extraction

The approach used for fingerprint extraction is Crossing Number (CN) since it the most commonly used method of minutiae feature extraction ([Rol11]). The ridge endings and bifurcations was extracts from the skeleton image by using crossing number (CN). The local neighbourhood of each ridge pixel in the image using a 3 x 3 window are extracted by scanning for minutiae features. The results of CN calculated is defined as half the sum of the differences between pairs of adjacent pixels.

5.1.2 Fingerprint Template Matching

The extracted data is stored in the matrix format for efficient matching process. The stored data in the matrix are as follows. Number of rows: Number of minutiae points. Number of columns: 4

Column 1: Row index of each minutia point. (**x** Coordinate)

Column 2: Column index of each minutia point. (**y** Coordinate)

Column 3: Orientation angle of each minutia point. (the input image and template image, minutiae angle θ of the particular minutiae point to be paired).

Column 4: Type of minutia. (A value of '1' is assigned

for termination, and '3' is assigned for bifurcation). In other words $(x, y, \theta$ and the minutiae type of input template would be paired with the same of x, y, θ and the minutiae type of registered template).
Each input minutiae point is compared with template minutiae point considering the properties i.e. $(x, y, \theta$ and the type of minutiae). Input minutiae and template are selected as reference point for their respective datasets in each case. The remaining data points were convert to polar coordinates using the reference points. To convert the template minutiae from row and column indices to polar coordinates equation (1) was used.

$$\begin{bmatrix} r_k^T \\ \emptyset_k^T \\ \theta_k^T \end{bmatrix} = \begin{bmatrix} \sqrt{\left(row_k^T - row_{ref}^T\right)^2 + \left(col_k^T - col_{ref}^T\right)^2} \\ \tan^{-1}\left(\frac{row_k^T - row_{ref}^T}{col_k^T - col_{ref}^T}\right) \\ \theta_k^T - \theta_{ref}^T \end{bmatrix} \quad (1)$$

r_k^T= Radial distance of kth minutiae.
$\emptyset_k^T$ = Radial angle of Kth minutiae
θ_k^T= Orientation angle of Kth minutiae
RowTref , colref T= row index and column index of reference points currently being considered.
Similarly the input matrix data points are converted to polar coordinates using the Equation (2)

$$\begin{bmatrix} r_m^I \\ \emptyset_m^I \\ \vartheta_m^I \end{bmatrix} = \begin{bmatrix} \sqrt{\left(row_m^I - row_{ref}^I\right)^2 + \left(col_m^I - col_{ref}^I\right)^2} \\ \tan^{-1}\left(\frac{row_m^I - row_{ref}^I}{col_m^I - col_{ref}^I}\right) + rotatevalues(k, m) \\ \theta_m^I - \theta_{ref}^I \end{bmatrix} \quad (2)$$

Rotate values (k, m) denotes the variance between the orientation angles of Tk and Im. Tk and Im represent the extracted data in all the columns of row k and row m in the template and input matrices, respectively.

5.2 Face Recognition Feature Extraction

This is similar to the Fingerprint Extractor but performs functions related to extraction of face templates from face images captured using cameras.
The face image (120 x 120 pixels) is spoiled in terms of 8 x 8 corresponding blocks. Then, Discrete Cosine Transform (DCT) is applied to every block and a sequence $((X_1^F = \{x_1 \dots x_F\})$ of DCTmod2 frames is computed. DCTmod2 frames are built from DCT frames$(15$ DCT coeff. -3 first coeff. $+3\Delta_x + 3\Delta y$. Thus, $Xf \in \mathbb{R}18$.

5.2.1 Face Template Matching

For the matching process the following equation by eigenface algorithm ([IA03]; [DG04]; [TP91]) was used and it consists of the following sequence:

$$C = AA^T$$

Where:

$$C \Rightarrow MN \text{ x } MN \text{ matrix} \quad (3)$$

$$L = A^t A$$

Where:

$$L \Rightarrow K \text{ x } K \text{ matrix}$$

The (M.N) eigenvalues and corresponding (M.N) eigenvectors of length (M.N.) each is computationally intractable even for a modest size image was obtained by calculate eigenvalues and eigenvectors. To obtain K eigenvalues and corresponding K eigenvectors of length K each the eigenvectors of reduced matrix L be

$$v_{i,i=1,2,\dots,K} \quad (4)$$

The eigenvectors of large matrix C can be obtained from the eigenvectors of the reduced matrix, the:

$$U_i = \sum_{j=i}^{k} V_{i,j} \emptyset_{i,i=1,2,\dots,K} \quad (5)$$

The face images eigenvectors, Ui, are called eigenfaces. Depending on the magnitude of its eigenfaces each of the eigenvalue varying significance. Hence, it suffices to select a subset K' of the K eigenfaces corresponding to K' highest valued eigenvalues as characterizing the entire training face images. In addition to the mean face, the reduced subset eigenfaces are stored.
Projecting training face images onto the stored eigenfaces, weight vectors was calculated. A scalar weight was calculated using the contribution of a stored eigenface to a zero-mean training face image. Therefore, by projection a weight vector of length K' whose elements represent the degree of contribution of the corresponding eigenface to that zero-mean image was obtained:

$$\omega_j = U_j^T . \emptyset_j , j = 1,2, \dots, K$$
$$\therefore \Omega_i = [\omega_1, \omega_2, \dots\dots, \omega_k] \quad (6)$$
i=1,2,….,K'

The calculated $(K' \text{ x } K')$ weight matrix is store as reference templates.

5.3 Authentication

The statistical framework of both finger and face authentication are different as stated above.
Let denote the parameter set for voter C as λ_c and the parameter set describing a generic non-voter as $\neg\lambda_c$. Given a claim for voter C's identity and a set of feature vectors X supporting the claim, then find an opinion $\Delta(X)$ on the claim using:

$$\Delta(X) = \log P(X|\lambda_C) - \log P(X|\neg\lambda_C) \quad (7)$$

Where $P(X|\lambda_C)$ is the likelihood of the claim coming from the true claimant and $P(X|\neg\lambda_C)$ is the likelihood of the claim coming from an impostor. Finally, to accept or reject a claim depends on the score $\Delta(X)$ decision that could either be above (accept) or under (reject) a given threshold.

5.4 Enrolment for the Bimodal System

To train each voter model Expectation Maximization (EM) strategy was used because EM have the capacity to deal with a large amount of training data. Expectation Maximization (EM) training consists in:
1. Training a world model: $\neg\lambda_c$ from a large dataset by Maximum Likelihood,
2. Adapting a voter model λ_c from: $\neg\lambda_c$ using voter data by Expectation Maximization.
The behavioural pattern of voter is added to the system. The fingerprint and face image of a particular user are acquired, to train a user model and acclimate (retrain) the world model if necessary the following are required: pre-processed, transformed into features, and post processed. To obtain a threshold for a user, the model along with impostor presentations will be used. If needed the new model is stored along with the threshold for that user ([Des06]).

5.4.1 Enrolment Process

Before voter being identified or verified by a bimodal biometric device, the enrolment process must be completed. The aim of this enrolment process is to create a summary profile of the voter. The process consists of the following:
Bio-data: This comprises the following; Demographic Data Capture Module (to capture name, date of birth, address, Location, etc.). The Location Information is based on State, LGA, Registration Area, and Polling Unit. This is derived from the 36 states plus FCT and the 774 LGAs as defined in the Nigerian Constitution and that what the INEC is using to get the details the voters.
A Biometrics Data Capture Module that capture fingerprints and face images of an enrollee. Face and Fingerprints must be captured for each enrollee before registration can proceed beyond Biometrics Data Capture Module.
Biometrics matching is strictly enforced in the Biometrics Data Capture Module. The registration of an enrollee terminates in this module if his data is already in the database otherwise registration proceeds to the Bio-data Data Capture Module.
Algorithms: The solution implemented face and fingerprint algorithms that have "liveness" detection functionality to ensure that the system responds only if it detects that a 'live' enrollee is indeed present at the point of data acquisition.

5.4.2 The Enrollee Storage

The enrollee storage has the details of all the people that have been enrolled and its stores them with the voter's card number. When there is need to view enrollee's details or make amends, it can be done easily by using the voter's card identification number to trace individual's details. It also makes the process of verification easier and faster as it also saves time.
In this paper, both the fingerprint and face recognition (bimodal) algorithms are combined, such that the shortcomings of one biometric can make up for other. Therefore, the process of verification is done by entering the enrollee's voter card identification number and the enrollee is asked to pass through the verification process by placing his/her finger on the biometric fingerprint scanner (Secugen) and also the face of enrollee is been used to confirm the enrollee. This is captured and the administrator compares the live biometric fingerprint captured and face image captured with the one in the database, for verification purpose. Each approach (fingerprint image matching technique and face recognition matching technique) computes its matching score and the mean of the score from the two approaches are compared with the established set threshold score. If the resulting score from the matching is greater than the threshold score, the system displays **"VERIFICATION SUCCESSFUL",** and he/she will be allow to vote. But if the resulting score is less than the established threshold, the system ignores it and displays **"INVALID VOTER"** with persecution signal to alert the administrator**.**

5.5 Test the model

The probabilities in equation 7 are represented by diagonal Gaussian Mixture Models. Each finger model is a diagonal GMM (λ^p and $\neg\lambda^p$) with 200 gaussians (130`400 parameters). And each face model is a diagonal GMM ($\lambda^f$ and$\neg\lambda^f$) with 512 gaussians (180`944 parameters).

Then, the respective finger and face scores are computed using Eq. 8 and Eq. 9.

$$\Delta_{\mathrm{C}}^{\mathrm{f}}\left(\mathrm{X}_1^{\mathrm{P}}\right) = \log\mathrm{P}\left(\mathrm{X}_1^{\mathrm{P}} \middle| \succ_{\mathrm{C}}^{\mathrm{p}}\right) - \log\mathrm{P}\left(\mathrm{X}_1^{\mathrm{P}} \middle| \neg \succ_{\mathrm{C}}^{\mathrm{p}}\right) \quad (8)$$

$$\Delta_{\mathrm{C}}^{\mathrm{f}}\left(\mathrm{X}_1^{\mathrm{F}}\right) = \log\mathrm{P}\left(\mathrm{X}_1^{\mathrm{F}} \middle| \succ_{\mathrm{C}}^{\mathrm{f}}\right) - \log\mathrm{P}\left(\mathrm{X}_1^{\mathrm{F}} \middle| \neg \succ_{\mathrm{C}}^{\mathrm{f}}\right) \quad (9)$$

The system was designed, built, and tested. The fingerprints from index and thumb fingers of left and right hands of 50 voters were captured using in-built fingerprint scanner, making 200 number of fingerprint images that were captured. Also, the face images of the 50 persons were captured using the face recognition camera system. The system was tested and evaluated using the captured fingerprint and face images, the result yielded 96% finger recognition rate; and 93% of face recognition rate.

6.0 FUSION IN A BIMODAL BIOMETRIC SYSTEM

6.1 Levels of Fusion

A generic biometric system has four (4) important modules:
(a) The attribute in the form of raw biometric data called the sensor module;
(b) The process data to extract a feature set that is a compact representation of the attribute to use is called the feature extraction module;
(c) A classifier to compare the extracted feature set with the template in the database in generating matching scores is called the matching module;
(d) To determine an identity or validate a claimed identity by use matching scores is called the decision module.
In multimodal biometric system from any of the above modules, information resolution can occur (see Figure 3). (a) The data itself or the feature sets originating from multiple sensors are fused, fusion occurred at the data or feature level. (b) The scores generated by multiple classifiers relating to different modalities are combined, fusion occurred at the match score level. (c) When the final output of multiple classifiers is fused through the system, we said fusion occurred at the decision level: ([ZI96]).

6.2 Modes of Operation

A multimodal system can work with any one of three different modes namely: (i) serial mode, (ii) parallel mode, and (iii) hierarchical mode.
Serial mode: The output of one modality is normally used to slim down the number of possible identities before the next modality is used ([HJ98]). Multiple traits do not have to be acquired directly, there is no multiple sources of information that acquired straight. Therefore, decision can be made before obtaining all the traits, which can reduce the overall recognition time.
In order to perform recognition in the parallel mode of operation, the information from multiple modalities is used directly.
The individual classifiers are combined in a treelike structure in hierarchical scheme. When the number of classifiers are large this mode is very relevant. Proposed system used the hierarchical mode because the number of applicant is very large when we are talking of voters that will be register in the country. Also it very important to note that the three modes of operation listed above perform according to the number of multiple traits and number of classifiers you are use them for.

6.3 Decision Fusion

Merge of both the outputs of finger and face into a feature vector, the two biometrics was fusion together $[\Delta^1(X), \ldots., \Delta^n(X)]$ and to sort it either as a voter or an impostor, a classifier was used to achieve this. The author use a simple linear classifier from the above framework:

$$\mathrm{P}(\mathrm{X}, \mathrm{Y}|\mathrm{C}) = w.\Delta_C^p(X) + (1-w)\,.\Delta_C^f(Y) \quad (10)$$

Finally, $\Delta^*(\mathrm{X}.\mathrm{Y})$ was used for final decision that was produces by fusion as an opinion.
For recognition (i.e. authentic) classification both modes must have an output of recognition (authentic), if not the final result will not be recognised (forgery). The system simply used the decision fusion that based on the logical AND of the two matching results.

7.0 IMPLEMENTATION

The bio-modal biometrics system proposed has been will be implemented using Java Programming Language and MySql database. The fingerprint and face of voter were capture using fingerprint sensor and face camera; the voter fingerprint unit compares the finger features with the fingerprint template stored in the database, the face algorithm also extract the voter face topographies and compares them with the stored voter template stored in the database. Two possible cases can occurred: firstly, match of voter features, captured voter behavioural features are matched with stored thumb image and face templates respectively. Then the system fuses the matching score of fingerprint and face module. The fuse score will be used to determine "Who to vote: and "who not to vote" base on the rules that have been set for making such decision. Secondly, the voter will not be allowed to vote with the non-match of fingerprint and face of any user.

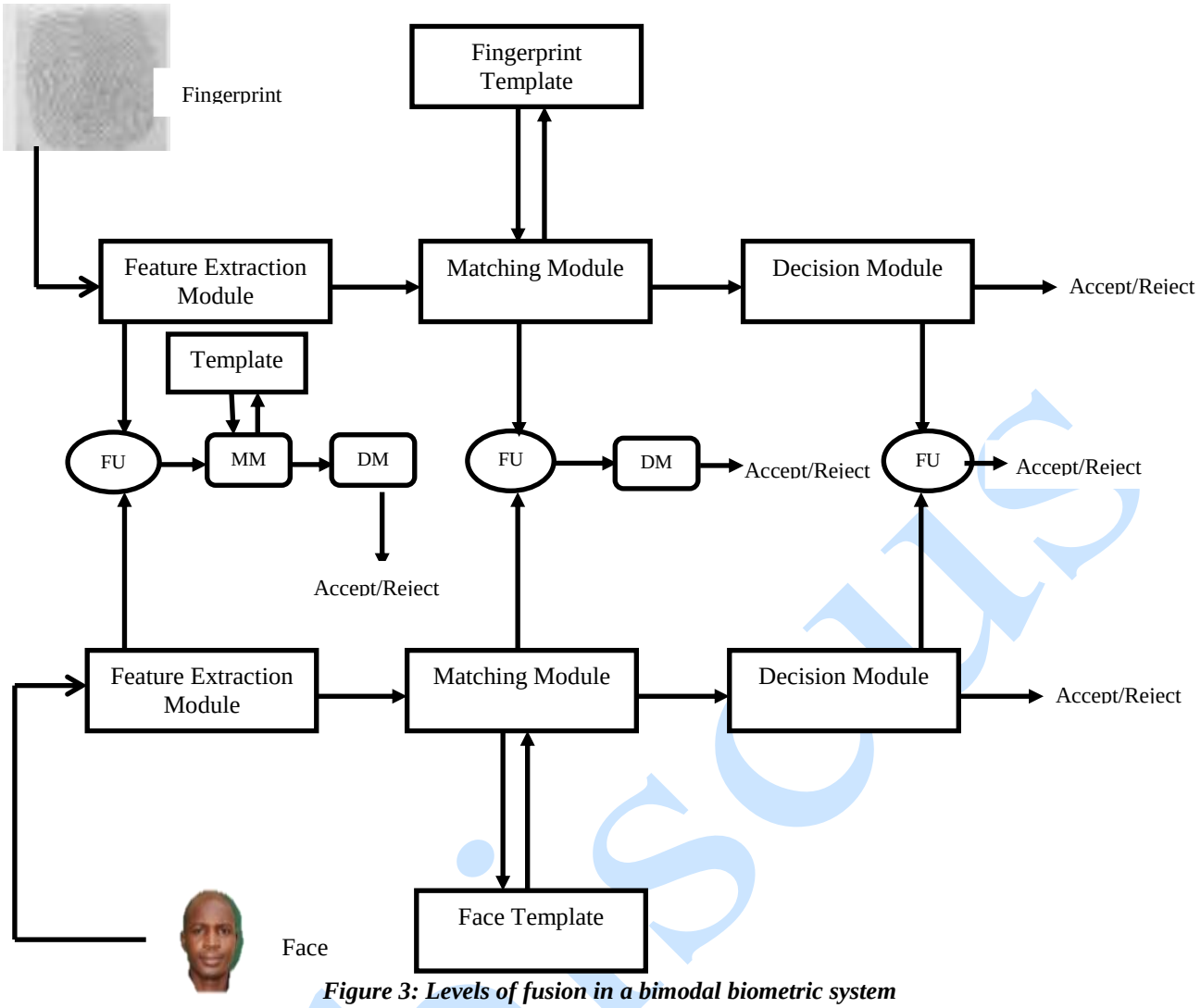

Figure 3: Levels of fusion in a bimodal biometric system

To make a final decision on whether an individual should be accept (allow to vote) or rejected (not allow to vote), the fusion will generate the fused score that will be used. This was generated by combing the matching scores obtained from fingerprint and that of face modalities through the use of weighted sum rule fusion technique that have been established.

7.1 Verification Phase

This is the phase where the voters is to be verified to make sure voters are who they truly claim they are before voters are allowed to vote for the candidate of their choice, the voters are prompted to supply their fingerprint and face it is then placed on the biometric fingerprint scanner and face recognition camera, once this is done, the fingerprint and face are then compared with the templates stored in the database with the aide of fingerprint and face recognition algorithms and the system compute the mean score of the result from the two algorithms and then compare it with the thresh hold that has been set if it is greater than the thresh hold the system then displays **VERIFICATION SUCCESSFUL** otherwise it displays **"INVALID VOTER"** with an alarm to alert the administrator**.**

8.0 EVALUATION OF ELECTRONIC VOTING SYSTEM SOFTWARE APPLICATION STANDARD

In the proposed model, two hundred and fifty people from five communities (c1, c2, c3, c4, and c5) and five metrics (parameters) were used (p1, p2, p3, p4, and p5). Statistical Package for Social Sciences (SPSS) 20 Version to obtain the mean scores. This was used with a view to arriving at a reasonable method for evaluating the standardization of system developed for use in Nigeria voting system.

Table 1:

Evaluation metrics	**Representation**
Security compliance	P1
User friendliness	P2
Dependability	P3
Platform compatibility	P4
Robustness	P5

Table 2 shows the evaluation metrics and their corresponding relative importance. The numerical value is the membership grade assigned to each metric and the cut off mark is 2.5. Any metrics that has weighted mean score that is below 2.5 is not meets the specification of the proposed system.

Table 2: Standards set for the metrics

Symbols	Standards set for the metrics	Relative Importance
US	Unacceptable standard	2.0
MS	Minimum standard	2.5
NS	Normal standard	2.7
BS	Best standard	3.0

The standards set for the metrics symbolized with two letters in table 2.

Table 3: E-voting software standard rating across the selected Departments

	C1	C2	C3	C4	C5
P1	BS	NS	NS	NS	NS
P2	MS	MS	MS	NS	BS
P3	MS	NS	NS	NS	BS
P4	NS	NS	BS	BS	MS
P5	NS	BS	BS	BS	BS

The opinions of people regarding the system were randomly sampled, opinion that has highest frequency in respect of each metric (which reflect the general opinion of people) are recorded as shown in table 3. The summaries of data from the respondents were extracted to table 3.

Table 4: E-voting software standard rating across the selected communities

	C1	C2	C2	C4	C5
P1	3.0	2.7	2.7	2.7	2.7
P2	2.5	2.5	2.5	2.7	3.0
P3	2.5	2.7	2.7	2.7	3.0
P4	2.7	2.7	3.0	3.0	2.6
P5	2.7	3.0	3.0	3.0	3.0

In table 4, the numerical value replaces the standards set symbols in table 3. The table gives the relative importance of metrics 1 to 5 across the five communities where the opinions were sampled.

Collection of data

The form was used for data collection, this was used to capture the thoughts of people across the selected communities.

Table 5: Data collection

COMMUNITIES	P1(Security compliance)	P2 (User friendliness)	P3 (Dependability)	P4 (Platform compatibility	P5 (Robustness)
Ayetoro-Ile **C1**					
Marafa-Oja **C2**					
Elesin-Meta **C3**					
Budo-oba **C4**					
Pepele **C5**					

Table 5 is the form used in the collection of data to capture the opinions of people across the five selected communities.

Table 6: Overall rating score across the selected communities

Electronic Voting Software Standard	Overall Score
Ayetoro-Ile **C1**	2.68
Marafa-Oja **C2**	2.75
Elesin-Meta **C3**	2.78
Budo-oba **C4**	2.82
Pepele **C5**	2.86

Part of testing the security requirements of electronic voting system, an election was conducted for some selected communities in Marafa/Pepele wards, Iponrin district of Ilorin East Local Government Area. The system was used to identify and authenticate the voters before allow to vote, the results of the election was embedded and stored into the database before extracted after the election. Questionnaire was adopted to gather relevant information about the developed electronic voting system from the respondents. The results was weighed using SPSS version 20 to obtain the mean scores.

Table 7 shows mean evaluation metrics on authentication of the developed system. The findings from the evaluation of the developed system indicated that the evaluated means were greater than the expected minimum mean of 2.00. This implies that the developed electronic voting system satisfied the security requirement of identification and authentication. The respondents' rating of the developed system on System Degree of Voter's Identification and Authentication Index (SDVAI) indicated 2.40 out maximum obtainable value of 3.00.

Table 7: Mean evaluation metrics on authentication of the developed e-voting system

S/N	ITEMS	OBSERVED	SDVA I
1	The developed system provides interface that can be used easily for enrolment and verification.	2.35	
2	The system verifies every individual correctly.	2.41	
3	The developed system prevents false identity.	2.33	
4	The electronic voting features prevent all unauthorized attempts to cast votes.	2.39	2.40
5	The developed system provides extremely accurate and secured access to voting procedures.	2.56	
6	The developed system makes the votes casted remain secret	2.41	
7	The developed system has the potential of restoring confidence for free and fair election	2.38	

N=250 $\bar{X}$ **= 3.00**

CONCLUSION

Voting has recently become a very popular and hot research topic in the field of computer science and other related fields. Electronic methods of counting ballots papers has been around for a while, the focus have been shifted to how to cast electronic ballots. The system can speed up the casting of vote and counting of ballots, which can also provide improved accessibility for disabled voters through different methods available for voters in electronic voting. Voters can vote through direct recording machines or the Internet that could decrease the use of ballots paper and the manual work of preparation during any general elections, there wouldn't be need for printing ballots papers in different languages, which have been the practise in some countries. Right application of these systems is also very critical, since the purpose of using it is to minima errors so there wouldn't be room for errors in the electronic recording or counting of ballots.

The associated risks of electronic voting are very substantial, the system can also facilitate electoral fraud. There is urgent needs for enhanced systems for integrity, security, authentication, secrecy, confidentiality and anonymity in the areas of election process since the aforementioned characteristics are very crucial to a successful voting system. There is urgent need to provide security against threats and identification of voters in any election process. The introduction of biometrics scanning can eliminate the problems associated to card fraud in voting system. Credit has been given to biometrics by faultfinders, because of its ability to erode anonymity. Multimodal will secure the electronic voting system.

The paper reviewed works on technologies used for electronic voting, since the methods is an area of growing interest. This research include a description of modern solutions and techniques, new voting systems evolving, and also requirements and security issues of these modern systems geared this research.

This paper has proposed an approach bimodal system by combining fingerprint and face recognition to curbing the activities of double or multiple registrations and the use of invalid voter card, and using some deceitful acts to escape being caught by the machine (fingerprint scanner) that has been set up. This is achieved by providing a reliable extraction and matching process via a combination of the fingerprint and face recognition techniques. The basic idea behind this is that one technique makes up for the deficiency of the other thereby bringing about a reliable and efficient result.

A model for evaluating the standard of e-voting system using SPSS v20 method was used to evaluate the proposed system. The result shows that the software developed for e-voting meets the minimum acceptable standard and capable of giving the decision maker a clear and flexible method of evaluating the software standard where the available data to be used for evaluation is based on the metrics and parameters to evaluate the system.

However, the evaluation have shown that the system is very useful in election system and also it shed light on the need to make some improvements so as to make the system to meet the standard of software adopted for electronic voting for the purpose of quality enhancement. It provides a more secured environment where voters will not be able to beat the system with their fraudulent tactics if the bimodal system is been used in our polling unit across all the nations of the world.

REFERENCES

[Adi08] Adida B. - *Helios: Web-based open-audit voting*, in USENIX Security Symposium, pp. 335–348, 2008.

[Ala09] **Alabi M. O.** - *Electoral reforms and democratic consolidation in Nigeria: The Electoral Act 2006*. CEU Political, Science Journal 4(2), 278-304, 2009.

[Ale11] **Alemika E. E. O.** - *Post electoral violence in Nigeria: Emerging trend and lessons*. CLEEN Foundation, 2011.

[AE11] **Awad M. L., Ernst L.** - *Internet voting in the USA: Analysis and commentary*. Transforming Government: People, Process Policy, 5(1): 45-55, 2011.

[AS15] **Anandaraj S., Sakthivel V.** - *Secured Electronic Voting Machine using Biometric*, International Journal of Advanced Engineering and Global Technology I Vol-03, Issue-11, Pp. 1371-1375, 2015.

[AU11] **Ashok Kumar D., Ummal Sariba Begum T.** - *A Novel design of Electronic Voting System Using Fingerprint*, International Journal of Innovative Technology & Creative Engineering Vol.1 NO.1, Pp. 12-19, 2011.

[AGJ13] **Alaguvel R., Gnanavel G., Jagadhambal K.** - *Biometrics using Electronic Voting System with Embedded Security*, International Journal of Advanced Research in Computer Engineering & Technology Volume 2, Issue 3, Pp. 1065-1072, 2013.

[A+15] **Awotunde J. B., Abdulkadir I. S., Adeyemi A., Idepefo O. F.** - *Automated Voting System: Bio-Modal Identification and Verification Approach*. Proceedings of 9th International Conference on ICT Applications (AICTTRA 2015), 112 – 122, Published by University of Ife (OAU), 2015.

[B+97] **Bigun E., Bigun J., Duc B., Fischer S.** - *Expert conciliation for multimodal person authentication systems using Bayesian Statistics*, in First International Conference on AVBPA, (Crans-Montana, Switzerland), pp. 291–300, 1997.

[Cra01] **Cranor L. F.** - *Electronic Voting*, Encyclopedia of Computers and Computer History, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.

[DG04] **Dhawan A., Ganesan A. R.** - *Handwritten Signature Verification*, ECE533 Project Report, pp. 1-15, 2004.

[DJM02] **Duta N., Jain A. K., Mardia Kanti V.** - *Matching of Palmprint*, Pattern Recognition Letters, vol. 23, Number 4, pp. 477-485, 2002.

[D+06] **Dessimoz D., Richiardi J., Champod C., Drygajlo A.** - *Multimodal Biometrics for Identity Documents*, State-of-the-Art, Research Report PFS, UNIL Univesite de Lausanne (EPFL), 341-08.05, 2006.

[Eve04] **Evers J.** - *Experts Challenge US Online Voting System*. Retrieved from: http://www.infoworld. com/article/04/01 /21/HNonlinevoting_1.html, 2004.

[EW97] **Eriksson A., Wretling P.** - *How Flexible is the Human Voice? A Case Study of Mimicry*. In Proceedings of the European Conference on Speech Technology, pages 1043–1046, 1997.

[ESK07] **Evangelia K., Stefanos S., Kalloniatis C.** - *Protecting privacy in system design: The electronic voting case*. Transforming Government: People, Process Policy, 1(4): 307-332, 2007.

[FS12] **Firas H., Seifedine K.** - *New System of E-Voting Using Fingerprint*, International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, Pp. 356-363, 2012.

[FYJ09] **Feng J., Yoon S., Jain A. K.** - *Latent Fingerprint Matching: Fusion of Rolled and Plain Fingerprints*, Proc. International Conference on Biometrics (ICB), June, 2009.

[F+04] **Fahmy G., Nassar D., Haj-Said E., Chen H., Nomir O., Zhou J., Howell R., Ammar H. H., Abdel-Mottaleb M., Jain A. K.** - *Towards an Automated Dental Identification System (ADIS)*, Proc. of the International Conference on Biometric Authentication (ICBA), Hong Kong, July, 2004.

[F+05] **Fierrez-Aguilar J., Krawczyk S., Ortega-Garcia J., Jain A. K.** - *Fusion of local and regional approaches for on-line signature verification*, Proc. International Workshop on Biometric Recognition Systems (IWBRS), pp. 188-196, 2005.

[GC13] **Gelb A., Clark J.** - *Identification for development: The biometrics revolution*. Working Paper 315. Centre for Global Development, Washington, D.C., 2013.

[GD12] **Gelb A., Decker C.** - *Cash at your fingertips: Biometric technology for transfers in developing countries*. Review of Policy Research, 29(1), 91–117, 2012.

[GKH02] **Gadekar R. R., Kiran T., Hwa A. P.** - *Websites for E-Electioneering in Maharashtra and Gujarat*, India. Int. Res., 21(4), 2011.

[GKO14] **Golden M., Kramon E., Ofosu G.** - *Electoral fraud and biometric identification machine failure in a competitive democracy*. Retrieved from: http://golden.polisci.ucla.edu/workinprogress/golden-kramon-ofosu.pdf, 2014.

[G+05] **Gefen D., Rose G. M., Warkentin M., Pavlou P. A.** - *Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa*. J. Global Inf. Manage., 13(1): 54-78, 2005.

[Har81] **Harrison W. R.** - *Suspect Documents, their Scientific Examination*. Nelson-Hall Publishers, 1981.

[HJ98] **Hong L., Jain A.** - *Integrating faces and fingerprints for personal identification*, In Proceedings 3"d Asian Conference on Computer Vision, pp. 16-23 Hong Kong, China, 1998.

[HJP99] **Hong L., Jain A. K., Pankanti S.** - *Can Multibiometrics Improve Performance?*. In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pages 59–64, New Jersey, USA, 1999.

[IA03] **Ibiyemi T. S., Aliu S. A.** - *Automatic Face Recognition by Computer*, Abacus: Mathematics Series, vol 30, no. 2B, September, pp180-188, 2003.

[JR03] **Jain A. K., Ross A.** - *Information Fusion in Biometrics*, Pattern Recognition letters, Vol. 24, pp. 2115-2125, 2003.

[JR04] **Jain A. K., Ross A.** - *Multi-biometric Systems*. Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1):34–40, 2004.

[JR99] **Jain A. K., Ross A.** - *A Prototype Hand Geometry-based Verification System*, M.S. Project Report, 1999, biometrics.cse.msu.edu/RossHand_MS99.pdf, 1999.

[JBP02] **Jain A., Bolle R., Pankanti S.** - *Introduction To Biometrics In Biometrics Personal Identification In Networked Society*, The Kluwer International Series In Engineering And Computer Science, Kluwer Academic Publishers, New York, 2002.

[J+ 04] **Jain A. K., Ross A., Prabhakar S.** - *An introduction to biometric recognition*. IEEE Trans. Circ. Systems Video Technol. 14 (1), 4–21, 2004.

[Kel03] **Kelly A. D.** - *Secure Oracle 91AS Gets Their E-Vote*. Oracle Magazine, January-February, 45-50, 2003.

[Kit04] **Kitcat J.** - *Government and ICT standards: An electronic voting case study*. J. Inf. Commun. Ethics Soc., 2(3): 143-158, 2004.

[Klu05] **Klugler D.** - *Advance security mechanisms for machine readable travel documents, Technical report*, Federal Office for Information Security (BSI), Germany, 2005.

[K+08] **Khasawneh M., Malkawi M., Al-Jarrah O., Barakat L., Hayajneh T. S., Ebaid M. S.** - *A biometric-secure e-voting system for election processes*, Mechatronics and Its Applications, 2008. ISMA 2008. 5th International Symposium on, Amman, pp. 1-8, 2008.

[LU02] **LeVan C., Ukata P.** - *Countries at the crossroads 2012: Nigeria*. Retrieved From http://www.freedomhouse.org/sites/default/files/Nigeria%20-%20FINAL.pdf, 2012.

[L+04] **Lebre R., Joaquim R., Zúquete A., Ferreira P.** - *Internet voting: Improving resistance to malicious servers*. Paper

presented at the IADIS International Conference Applied Computing, Lisboan, 2004.

[Mir04] **Mira L. M.** - For Brazil Voters, Machines Rule. Wired News, 2004.

[Mor02] **Morse R.** - *Electronic voting: progress over setbacks*. Law Technol., 35(4): 1-6, 2002.

[M+02] **Matsumoto T., Matsumoto H., Yamada K., Hoshino S.** - *Impact of Artificial Gummy Fingers on Fingerprint Systems*. In Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE, volume 4677, pages 275–289, 2002.

[M+16] **Mohamed S. S., Anto Bennet M., Arawind A. A., Rajvel S. K., Janakiraman G.** - *A Design of E-Voting Using Fingerprint Recognition System for Secured Voting*, Middle-East Journal of Scientific Research Techniques and Algorithms in Emerging Technologies, Pp. 385-390, 2016.

[Neu93] **Neumann P. G.** - *Security Criteria for Electronic Voting*. 16th National Computer Security Conference of the ACM, Baltimore, Maryland, 45(12): 39-43, 1993.

[Nwa15a] **Nwangwu C.** - *Biometric Voting Technology and the 2015 General Elections in Nigeria*, Paper Presented at Two-Day National Conference on "The 2015 General Elections in Nigeria: The Real Issues" organized by The Electoral Institute between 27th and 28th July 2015, Pp. 1-28, 2015.

[Nwa15b] **Nwannenna C. C.** - *Design and Development of a Multi-Modal Biometric System with De-Duplication Functionality*. 12th International Conference Proceeding (IT4InDev 2015) by Nigeria Computer Society (Akure, Nigeria) Vol. 23 pp 186-192, 2015.

[Ogb11] **Ogbaudu F.** - *2011 General election review: Experience sharing, lessons learnt and the way forward - The Nigeria police perspective*. Paper presented at the review of elections security during the 2011 general elections in Nigeria justice sector reform monograph series, 2011.

[OA14] **Olowookere A., Awode T.** - *Design of a Secured Electronic Voting System Using Multimodal Biometrics*, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, Pp. 1701-1706, 2014.

[PB04] **Pescatore J., Baum C. H.** - *Online Voting can't be Trusted on Standard PCs*. From: http://news.zdnet.co.uk/security/0,10000 00189,391 48110,00.htm, 2004.

[PK02] **Putte T., Keuning J.** - *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned*. In Proceedings of IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pages 289–303, 2002.

[Rub02] **Rubin A. D.** - *Security Considerations for Remote Electronic Voting*, Communications of the ACM, Vol. 45, No. 12, 2002.

[RJ03] **Ross A., Jain K.** – *A Learning user-specific parameters in a multibiometric system*. In: Proc. Internat. Conf. on Image Processing, Rochester, New York, 2003.

[RNJ06] **Ross A., Nandakumar K., Jain A. K.** - *Handbook of Multibiometrics*. Springer, New York, USA, 1st edition, 2006.

[RPP11] **Roli B., Priti S., Punam B.** - *Minutia Extraction from Fingerprint Image: A review*, International Journal of Computer Science Issues Vol. 8, Issue 5, No3, 001, 2011.

[R+14] **Rakesh S. R., Raghavendra A., Madhushree K. R., Bhargavi D.** - *An Online Voting System Using Biometric Fingerprint and Aadhaar Card*, International Journal of Computing and Technology, Volume 1, Issue 4, Pp. 87-92, 2014.

[SD15] **Sudhakar M., Divya Soundarya Sa B.** - *Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller*, Journal of Electronics

and Communication Engineering (IOSR-JECE) Volume 10, Issue 1, Ver. II, Pp. 57-65, 2015.

[SAR15] **Sabo A., Siti A. J. B., Rozita B. A.** - *Issues and Challenges of Transition to e-Voting Technology in Nigeria*, Public Policy and Administration Research, Vol.5, No.4, 95-102, 2015.

[SPV14] **Shanu A., Pradeep M., Vipin Y.** - *Fingerprint Recognition Based Electronic Voting Machine*, National Conference on Synergetic Trends in engineering and Technology (STET-2014) International Journal of Engineering and Technical Research, Pp. 255-259, 2014.

[TM16] **Trupti U. P., More S. V.** - *A Survey on Secured E-Voting System Using Biometric*. International Journal of Advanced Research in Science, Engineering and Technology, Vol. 3, Issue 3, Pp. 1700-1704, 2016.

[TP91] **Turk M., Pentland A.** - *Eigenfaces for Recognition, Journal of Cognitive Neuroscience*, vol. 3, no.1, Pp 71-86, 1991.

[TR13] **Tejasvee P., Reshamwala A.** - *E-Voting System using Multimode Bio-Metric Analysis for Authentication*, International Journal of Computer Applications Volume 83 – No 14, Pp. 11-17, 2013.

[UYA08] **Unsang P., Yiying T., Anil K. J.** - *Face Recognition with Temporal Invariance: A 3D Aging Model*, 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition, Amsterdam, Netherlands, September, 2008.

[Yee07] **Yee K.-P.** - *Extending Prerendered-Interface Voting Software to Support Accessibility and Other Ballot Features*, in EVT, 2007.

[YG13] **Yinyeh M. O., Gbolagade K. A.** - *Overview of Biometric Electronic Voting System in Ghana*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, Pp. 24-27, 2013.

[ZI96] **Zuev Y., Ivanon S.** - *The voting as a way to increase the decision reliability*, in Foundations of Information/Decision Fusion with Applications to Engineering Problems, (Washington D.C., USA), pp. 206–210, 1996.