I.J. Information Engineering and Electronic Business, **2021, 5, 24-37**
Published Online October 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2021.05.03

An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram

Adewale Olumide S.
Department of Computer Science, the Federal University of Technology, Akure, Nigeria
E-mail: adewale@futa.edu.ng

Boyinbode Olutayo K. and Salako E. Adekunle
Department of Information Technology, the Federal University of Technology, Akure, Nigeria
E-mail: okboyinbode@futa.edu.ng and salakoea@futa.edu.ng

Received: 09 August 2021; Revised: 28 August 2021; Accepted: 10 September 2021; Published: 08 October 2021

Abstract: An election is a formal procedure through which a group of individuals decides on an individual or multiple individual to be in a position of authority using mechanical, paper-based and electronic methods. Despite the measures to secure the voting systems from fraudulent activities among corrupt politicians and election officers, attackers have been compromising the security measures thereby, providing illegitimate opportunities for unwanted contestants to win elections. This research was on the development of an electronic voting system using fingerprint and visual semagram techniques. The proposed e-voting model had six modules for effectiveness in the e-voting system. It was implemented using Java in Android Studio and C-Sharp (C#) in Microsoft Visual Studio, and was tested in an official deanship election of five faculties in a tertiary institution. Every illegible staff was enrolled and presented with a voter identification number (VIN) card. The voter's fingerprint and VIN were the fundamental credentials required for authentication and to poll a legitimate vote to a preferred contestant at a designated polling centre. The sensitive results were firstly encrypted and secondly concealed in an image to produce "Vimago" using the visual semagram technique. The "Vimago" was subjected to steganalysis and concealed results were not detected. An Equal Error Rate of 0.0019, a sensitivity of 0.9962 and an accuracy of 99.81% were obtained from the experiment. Based on the experimental results, the proposed e-voting model is highly recommended for use by various electoral commissions for voting and security agencies for the dissemination of sensitive information through the public network, the manufacturers of electronic voting machines are hereby offered a model for use in the development and securing of a fingerprint-based platform for a voting system were made among other recommendations.

Index Terms: Security, Electronic, Voting System, Fingerprint and Visual Semagram

1. Introduction

The human is created by God with the capability to choose among many options. Countries in the world have laws that empower every citizen to decide on specific issues that have effects on their living and society, and making such decisions in elections is not exempted. An expression of interest by an individual in an election is a fundamental human right that must be protected at all times against violation. Corrupt politicians often use forces to achieve personal ambition and this dreadful situation had affected the level of development across every human endeavour. Election malpractices by corrupt politicians and election officers have been reported across the nations of the world, thereby making an unwanted contestant wins an election.

Computer technology has the potential to curb irregularities in the present election system. The use of an electronic voting system has been a welcome idea in many countries like the United State of America (USA), Estonia, Netherlands, India while other nations are still debating on the efficacy of the electronic voting system [2]. Electronic voting (e-voting) system is a platform where registered voters make choices on a preferred contestant using electronic devices based on specified rules and regulations. E-voting systems use electronic devices and computer technologies to organize an election. An election is a process of choosing a preferred contestant by popular votes from the voters. According to [10, 16] stated different types of voting systems. These voting systems include Paper-Based Voting (PBV), Web-Based Voting (WBV) and Biometric-based voting system. According to [14, 15], four different types of voting systems had

been highlighted. These voting systems included Paper-based Voting Systems (PVS), Central Count Voting Systems (CCVS), Precinct Count Voting Systems (PCVS) and Direct-Recording Electronic (DRE) voting systems.

According to [10], Internet voting can be grouped into three types. These include:

i. Poll Internet voting: This framework permits voters to cast their votes from any assigned to a controlled situation offered by the surveying webpage.
ii. Kiosk Internet voting: In this kind of voting framework, the voting gadgets are set far from customary voting areas and set up in suitable zones like schools and libraries.
iii. Remote Internet voting: In this type of electronic voting, the voters are allowed to cast their votes from anywhere in the world on the internet.

Mechanical Lever, Paper-Based and Electronic constituted major types of voting system. In [32, 34], electronic voting could further be classified into Short Message Service (SMS), Web-Based Voting (WBV) or Internet Voting System (IVS), Telephone Voting System (TVS) and Biometric-based Voting System (BVS).

2. Literature Review

The studies on different types of voting systems showed that biometric-based is a preferred system against fraudulent acts as reported in [18, 10]. Sequel to series of fraudulent acts in elections, the concept of steganography was introduced as a measure to secure sensitive data. Steganography is the concealment of a sensitive message and is classified into two: technical and linguistics. Semagram is one of the classes of linguistic techniques. The semagram has two elements namely; text and visual semagrams. Text semagrams are used to hide information through modification of letters, special characters, symbols and signs. The visual semagram hides information in images, symbols and signs which are not sensitive to the human visual system (HVS). Visual semagram does not use invisible inks, microdots and reduction techniques, unlike technical steganography [33]. According to [7], steganography techniques are advantageous to non-suspicion over cryptography and watermarking. In the steganography technique, it does not attract the attention of fraudsters, internet surveillance is difficult and the secret message is difficult to prove its existence.

A fingerprint-based electronic voting machine towards the elimination of fake voting was developed in [21]. The RFID, fingerprint and Arduino UNO R3 microcontroller were linked to the Radio-Frequency IDentification (RFID) database for authentication and to poll votes. A dedicated push button for each candidate requires a high cost of implementation for numerous contestants. Reference [13] opined that some people used another person voting card to vote. A matching technique for fusing voter's fingerprints and faces to achieve authentication was presented. The illumination variation, facial expressions and face angles to the camera were major problems to face recognition. Reference [5] implemented an online voting system using biometric verification and ESP8266 chip. Ridge extraction technique to achieve authentication was adopted and the e-voting system was simple to operate. The current and resistance ratings of the ESP8266 chip affect its effectiveness and the results on the unprotected wireless network could be intercepted and altered. In [19], a biometric authentication system based on the Aadhar card and Arduino mega 2560 microcontroller was implemented. Minutiae matching algorithm in satisfying the authentication requirement of the e-voting system was adopted and used. The Arduino Mega 2560 microcontroller has a limited memory capacity for a large population and the password of authorized officers could be detected by the imposters. The proposed e-voting model addressed the identified problems.

Reference [6] designed and developed a fingerprint enabled electronic voting machine (EVM) to achieve a greater security level. The fingerprint and GSM were used to implement the voting system. The problems of confidentiality, integrity, and secrecy were not addressed. The election results through the use of GSM could be intercepted and altered by fraudsters. The concealment of sensitive of election results using visual semagram secured the transmission through public networks as proposed.

A secured electronic voting machine using the Aadhaar on the Internet of Things (IoT) platform was developed in [20]. The materials used were PIC16F874A/877A microcontroller, fingerprint sensor, ZigBee (CC2500), Liquid Crystal Display (LCD), buzzer and power supply. The PIC16F874A/877A microcontroller has a limited memory capacity for a large population. The procurement of Aadhaar cards is economically high and not suitable for developing countries.

The voting system of [9] was designed and implemented purposefully for organisations and businesses. The voter's fingerprint and face were combined with the voter's username and password were used to implement the voting system. The fusion of fingerprint and face images requires a large memory capacity. The high accuracy of the bimodal system is not guaranteed [22]. The cost of producing Aadhaar cards is high [2] making such a system is expensive for developing nations. Reference [12] designed and implemented an electronic voting machine with facial recognition and fingerprint sensors. The Support Vector Machine and Local Binary Pattern Histogram were used for face recognition while the High Sensitive Pixel Amplifier (HSPA) was used for the fingerprint process. The Visual Basic language was used to implement the voting system. The problem of illumination affects face recognition and the error rate (FAR or FRR) of the weaker biometric could bring down the overall effectiveness of the system [1, 8, 32].

According to [17], blockchain technology was used to develop an e-voting system with the voter's information secured in the dedicated database. However, securing the sensitive results of the election was not discussed as fraudsters could launch attacks on the suspected results. The attacks could corrupt the original results thereby making unwanted contestants win elections. This research was different as a visual semagram was used to conceal the encrypted results in an image that did not raise suspicion.

Reference [3] presented a paper that focused on an Online-Voting System using Blockchain technology. The authentication of voters was achieved with the identification key and fingerprint. A one-time password (OTP) was also used to further verify the voter. Scholarly, Equal Errol Rate (EER) was not calculated to establish the accuracy of the proposed system. Moreover, the security of election results through public and unprotected networks was not considered. How reliable was the system of [3] for use by government and other institutions with the responsibilities to conduct free and fair elections when keys components were not addressed? This paper presented a highly secured and tested e-voting model for public use with core e-voting functional and requirements of enrolment, authentication, confidentiality, and integrity.

In [4], biometric voting systems that used an Aadhaar card, voter's iris and fingerprint for enrolment and authentication were developed. Diseases affect iris recognition and the performance of a multimodal system depends on data type and the fusion technique used [1]. The authentication mechanism of [4] requires high computation, large memory capacity, and high cost for implementation. This paper presented an enhanced approach to enrolment and authentication using a metadata (fusion of voter identification number (VIN) and fingerprint) technique that did not expensive and highly secured against attacks. The proposed e-voting model was developed and evaluated to address the identified problems.

3. Motivation

The existing e-voting systems have issues with functional and security requirements of electronic voting systems as corrupt politicians acquaint with breaching the rules and get indulged in corrupt practices for personal gains. In Nigeria 2019 general election, there was a problem of "votes buying and selling" between the corrupt politicians and voters. The votes were exchanged for money, thereby making undesired contestants emerged as winners from different types of elections. This was evident as there were court cases of irregularities, making different groups challenging the credibility of the election. Many countries as democratically-governed nations have undisputable bad electoral processes [16]. The genuine voters and concerned citizens have become downhearted and have practically given up hope on their votes counting in electing any credible contestant into elective positions due to the problems of results' alteration.

Many electoral processes have been characterized by lawlessness, rigging, ballot padding, candidate imposition and fighting. The problems facing the voting system in Nigeria include common practice of voters' impersonation and multiple voting by false voters, snatching of the electoral materials such as ballot boxes, ballot papers by an unauthorized group of people, massive rigging by party agents in collaboration with the polling officials and fighting and burning of valuable properties resulting from lack of truth in the electoral process. The challenges of elections also include insecurity of votes, poor funding, bad attitudes of the political class, poor structure of polling units, rigging and inability to prosecute election offenders [1, 2, 5, 32]. It is very obvious that traditional methods of voting using papers, ballot boxes and manual counting of votes have provided room for the desperate politicians to alter election results; this, in turn, makes the populace lose confidence in the integrity of the election across the globe [11].

4. Significance and Value of the Results

The core area of focus of this research was security of sensitive election data. The focus of this research was to develop a secured electronic voting system using fingerprint biometric and visual semagram techniques. The research would be a significant force in restoring confidence in the populace and enhance their participation in elections as sensitive results were highly secured against suspicion and attacks. This research would also benefit to the government and the members of various institutions and association such as the Students Union Government (SUG), schools and companies in choosing representatives into different positions. With the use of this proposed e-voting model, these institutions are guaranteed free and fair election. The proposed e-voting model could detect multiple registrations, prevent multiple votings and prevent desperate and corrupt politicians from altering the results of elections. The developed electronic voting model secured election results from manipulations and there was an improvement in authentication, confidentiality and integrity of election processes, during the pre-election, election and post-election stages. This e-voting system would be helpful to tackle the problems of buying and selling votes by the corrupt politicians and corrupt voters as there would be no link between the voter and the vote polled by the same voter. This research would also assist the researchers as literature for future reference on the subject of biometrics and electronic voting systems.

5. Research Objectives

The specific objectives of this research were to:

i. design a fingerprint and visual semagram technique for securing the e-voting system,
ii. implement the designed e-voting system in (i), and
iii. evaluate the performance of the proposed e-voting model.

6. Methodology

The proposed e-voting model consisted of six modules, namely enrolment, authentication, voting, results, semagramming, and desemagramming as illustrated in Figure 1. The modules were designed to tackle the functional and security requirements of enrolment, authentication, confidentiality, integrity, transparency and conveniences.

6.1 Modules of Proposed e-voting Model

The basic modules of the proposed e-voting model were detailed under the following sub-headings.

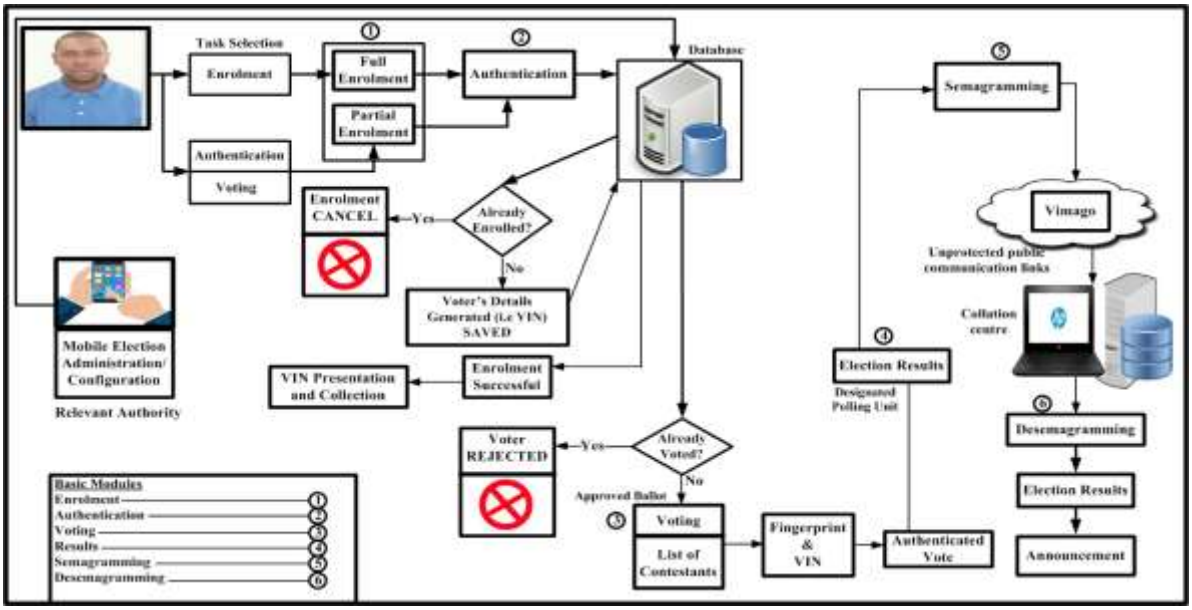

Fig.1. Functional diagram of a proposed e-voting model

(a) Voter's Fingerprint Enrolment and Authentication Modules

The data of voters were acquired, processed and stored in a database for future reference. The fingerprint processes involved image pre-processing, minutiae extraction and matching. The minutiae considered for this research were ridge-end and bifurcation. Equation (1) was used for the identification of minutiae points. The "CN" was the crossing number, P_i was the pixel value (0 or 1) in the neighbourhood of P, P was the pixel value (0 or 1) at the centre of a 3x3 window of the fingerprint reader, and "i" was the position value of a pixel.

$$CN = \frac{1}{2}\sum_{i=1}^{8}|P_i - P_{i+1}| \quad : P_9 = P_1 \tag{1}$$

The voter's minutiae were stored as a template, V_f during enrolment using Equation (2).

$$V_f(V_R, V_B, \omega) = \left((|V_R - V_B|) + \omega\right) \tag{2}$$

V_R was the sum of distances and angles of ridges, V_B was the sum of distances and angles of bifurcations in respect to the centre of fingerprint reader and Omega, ω was a numerical variable that denoted the current time in seconds at the instance of creating the template, V_f. Also, a new voter's identification number (V_{in}) was generated using Equation (3). In Equation (3), V_k was the previous V_{in} of a voter that has been successfully enrolled, $f(V_k)$ was a formulated function, "$f'(V_k)$" and "$f''(V_k)$" were first and second derivatives of $f(V_k)$ respectively and "t" was the current time and

date in seconds, "k" were citizens and "q" was the last citizen for enrolment. To get the first V_{in} for the first voter, "V_0" was a default value and "k" was zero (0). When a citizen has successfully enrolled with proof of generated V_{in}, then such a citizen becomes a registered voter.

$$V_{in\,(k+1)} = (V_k) + \left(\frac{f(V_k)}{f/(V_k)}\right) + f//(V_k) \;+\; t \quad : k = 1, 2, 3, \ldots, q \tag{3}$$

Equation (4) fused the scores of V_f and V_{in} in the enrolment to produce voter's ticket (V_t) for authentication in a secure e-voting system. The Beta (β) was a numerical constant that denotes voter' sensitivity to detect the difference in the scores between a genuine voter and an imposter.

$$V_t(V_f, V_{in}, \beta) = \left(\frac{1}{\beta}\right) * \left(\frac{V_f}{V_f + V_{in}}\right) \tag{4}$$

Furthermore, the threshold scores (V_{h1}, V_{h2}) of "V_t" were computed and stored for moderate acceptance and rejection rates to be achieved during authentication; where "V_{h1}" was the minimum threshold score, "V_{h2}" was the maximum threshold score.

In the authentication module, a new voter's ticket (V_T) was recomputed for comparison with V_t, V_{h1} and V_{h2}. A voter was accepted to vote when Equations (5), (6), (7) and (8) were satisfied, otherwise rejected;

$$V_T = V_t \tag{5}$$

$$V_T = V_{h1} \tag{6}$$

$$V_T = V_{h2} \tag{7}$$

$$V_{h1} \leq V_T \leq V_{h2} \tag{8}$$

(b) Voting Module

After successful authentication, a pop-up menu of contestants was displayed for a voter to elect a preferred contestant. Equation (9) was generally be used to compute votes scored by each contestant, C_X at a specific collation centre for an election type, E_t. The winner with maximum score, $W(E_t)$ was declared; where "x" and "y" were first and last contestant; "e" and "f" were first and last authenticated voter; "a" and "b" were first and last collation centre, "AVe" and "PBa" were authenticated voters and collation centres respectively.

$$W(E_t) = \max \sum_{X=1}^{y} \cdot \left(\sum_{e=1}^{f} C_X AV_e + \sum_{a=1}^{b} C_X PB_a \;+\; .\;\; .\;\; .\right) \tag{9}$$

(c) Results and Semagramming Modules

Firstly, the results (M) to be transmitted to the collation centre on the network was encrypted using Equations (10) and (11). The "K" was the signature and verification key, "Mc" was a character coded number of "M", "p" was the current date and time in seconds, "H" was an encrypted message, "σ" was ASCII character insertion. Secondly, a visual semagram which is one of the classes of steganography that uses sign, symbol and image to conceal sensitive data against attacks was used to conceal the encrypted results and form a carrier ("Vimago", V) using Equation (12). The "φ" was a character binary converter for image pixels. Figure 2 shows the encrypted results ready for the creation of "Vimago".

Fig. 2. Encrypted results in Vimago

$$K = (12M_C + 1 + p) \quad (10)$$

$$H = \sigma((K) \bmod 107)) + \sigma(M_C+6, 123) \quad (11)$$

$$V = \varphi(H) \quad (12)$$

(d) Desemagramming Module

At the collation centre, the receiver uncovered, decrypted and verified the received results using Equation (13).

$$M = (((9(\varphi^{-1})V) - 9 - 9p) \bmod 107) - \sigma(M_C-6, 123) \quad (13)$$

6.2 Implementation

The proposed electronic voting model/system was implemented using Java in Android Studio to develop the frontend interface for relevant authorities to carry out administrative activities such as the creation of election's officers, polling booths, wards, local government areas, states, registration of political parties, and contestants, and Internet Information Server (IIS) for the backend to provide services for mobile clients, enhance fast election configuration, and hosts the application that communicated to the database. Furthermore, a C-Sharp (C#) programming language was used to develop a desktop version that was deployed on a personal computer for voters' fingerprint biometric enrolment, authentication, voting, transmission and reception of sensitive results. Additionally, Microsoft Structured Query Language (SQL) was used to create the database as a backend for data organization, storage and retrieval of relevant information. Figure 3 shows the enrolment page of the proposed e-voting model.

The proposed e-voting model was tested at FCT College of Education, Zuba, Abuja during the Deanship election conducted in October 2021. The staff of five faculties participated in an official election to elect a Dean of a respective faculty.

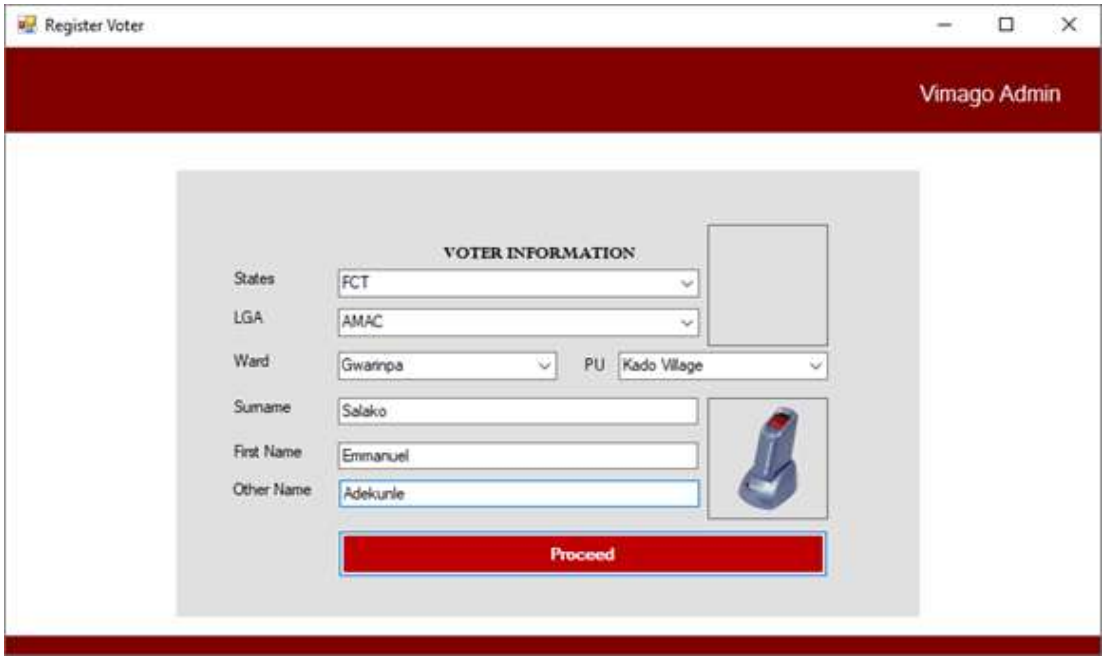

Fig.3. Enrolment page

7. Results

The performance evaluation of the proposed e-voting model was carried out using standard metrics. The data collected were analysed to establish the accuracy of the proposed model. Table 1 shows a confusion matrix of acceptance and rejection of genuine voters and imposters attempts.

Table 1. Confusion matrix of voters' and imposters' acceptance and rejection

Individual	Accept	Reject	Total
Genuine (Real voter)	RA (521)	FR (2)	TTA (523)
Imposter (Fake voter)	FA (0)	RR (281)	TFA (281)
Total	TA (521)	TR (283)	GT (804)

Total True of Attempts (TTA) by the genuine voters was the sum of "RA" and "FR":

$$\text{TTA} = \text{RA} + \text{FR} = 521 + 2 = 523$$

Total False of Attempts (TFA) by imposters was the sum of "FA" and "RR":

$$\text{TFA} = \text{FA} + \text{RR} = 0 + 281 = 281$$

1. Sensitivity or True Acceptance Rate (TAR) = $\frac{\text{Total True Accept}}{\text{Total True Attempts}} = \frac{\text{RA}}{\text{TTA}} = \frac{521}{523} = 0.9962.$
   This computational value implied that the proposed e-voting model had a 99.62% possibility to correctly accepted genuine voters and matched a template in the database.

2. Specificity or True Rejection Rate (TRR) = $\frac{\text{Total True Reject}}{\text{Total False Attempts}} = \frac{\text{RR}}{\text{TFA}} = \frac{281}{281} = 1.0000.$
   This computational value implied that the proposed e-voting model had a 100% possibility to correctly rejected imposters and found no match of a template in the database.

3. False Acceptance Rate (FAR) = $\frac{\text{Total False Accept}}{\text{Total False Attempts}} = \frac{\text{FA}}{\text{TFA}} = \frac{0}{281} = 0.0000.$
   This computational value implied that the proposed e-voting model had a 0.00% possibility to incorrectly accepted imposters and matched a template in the database.

4. False Rejection Rate (FRR) = $\frac{\text{Total False Reject}}{\text{Total True Attempts}} = \frac{\text{FR}}{\text{TTA}} = \frac{2}{523} = 0.0038$
   This computational value implied that the proposed e-voting model had a 0.38% possibility to incorrectly rejected genuine voters and found no match of a templated in the database.

5. Equal Error Rate (EER) = $\frac{\text{FAR} + \text{FRR}}{2} = \frac{0.0000 + 0.0038}{2} = \frac{0.0038}{2} = 0.0019$
   This implied that the mean error rate of the proposed e-voting model was 0.0019 as illustrated in Figure 4.

6. Failure to Enrol Rate (FTE) = $\frac{\text{Enrolment Not Successful}}{\text{Total Enrolment Attempts}} = \frac{\text{ENS}}{\text{TEA}} = \frac{0}{810} = 0.0000$
   This computational value indicated that the proposed e-voting model had no failure in the enrolment of the respondents.

7. Mean Time-to-Enrol (MTTE) = $\frac{\sum_{i}^{f} T_i}{f} = \frac{1{,}241.5226}{627} = 1.98\text{seconds}$

8. Mean Time to Detect (MTTD) = $\frac{\sum_{x}^{y} TD_x}{y} = \frac{1{,}989.1200}{518} = 3.84\text{seconds}$

9. Accuracy = 1 – EER = 1 – 0.0019 = 0.9981
   Percentage of System Accuracy (PSA) = $(\text{Accuracy}) \times 100 = 0.9981 \times 100\% = 99.81\%$

Table 2 shows the summary of computational values of standard metrics used for the performance evaluation of the proposed e-voting model.

Table 2. Computational values of standard metrics

S/n	Metric	Value
1	TAR	0.9962.
2	TRR	1.0000
3	FAR	0.0000.
4	FRR	0.0038
5	EER	0.0019
6	FTE	0.0000
7	MTTE	1.98seconds
8	MTTD	3.84seconds
9	Accuracy	99.81%

This computational value indicated that the proposed e-voting model had 99.81% of correctness to correctly perform all specified functions.

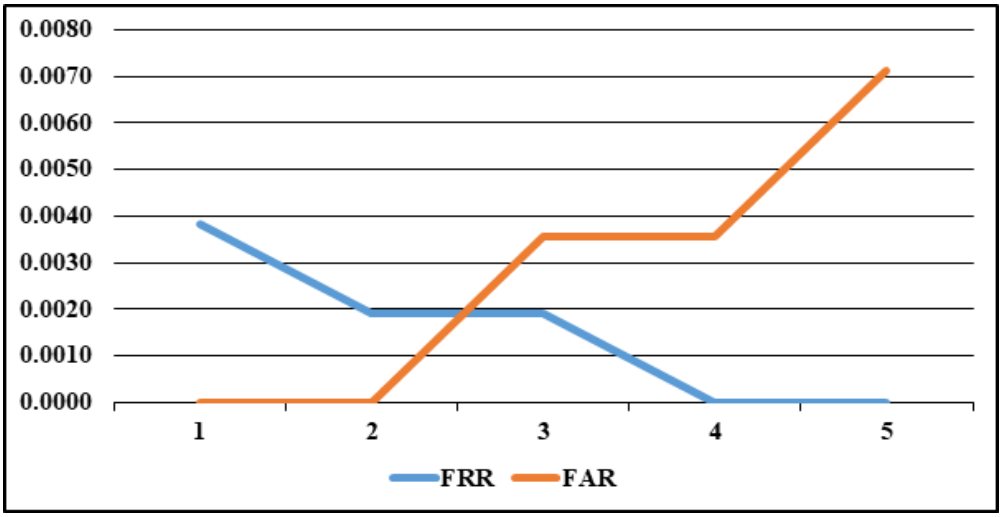

Fig. 4. Proposed system trade-off curve

Table 3 shows the comparison of EER values of the proposed e-voting model and the existing systems. The EER of the proposed system had the lowest value of 0.0019 as shown in Figure 4 and the highest accuracy of 99.81%.

Table 3. Comparison of EER and accuracy

S/n	Author(s)	Existing EER
1	[23]	0.0060
2	[24]	0.0560
3	[25]	0.0200
4	[26]	0.0081
5	[27]	0.0400
6	[28]	0.0376
7	[29]	0.0763
8	[30]	0.0040
9	[31]	0.0128
10	Proposed model	0.0019*

Figure 5 shows a graphical representation of the comparison of EER of the proposed e-voting model and the existing systems.

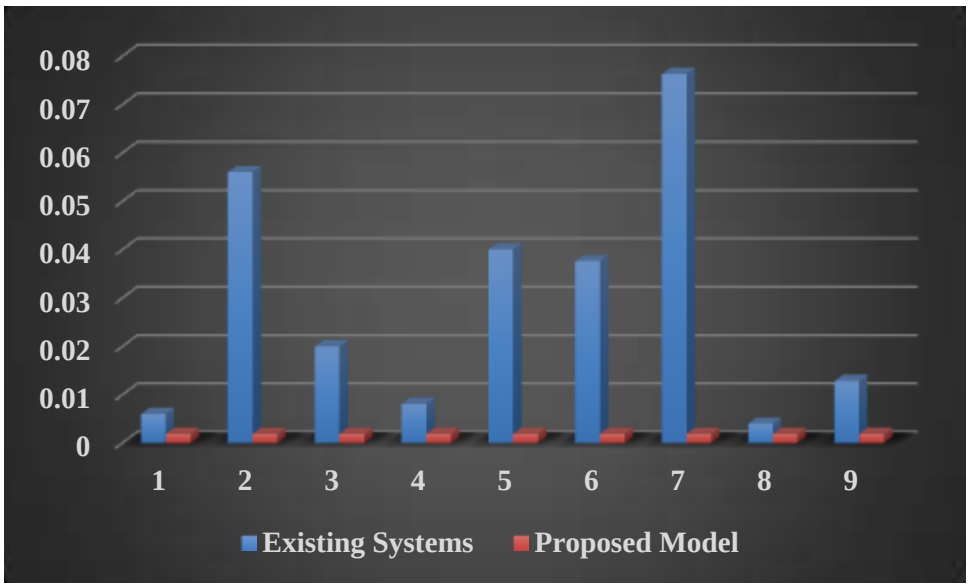

Fig. 5. EER representation of proposed e-voting model and existing systems

Figure 6 shows the result of Mcafee online steganalysis on the “Vimago”. The results indicated that not sensitive results were concealed in the image.

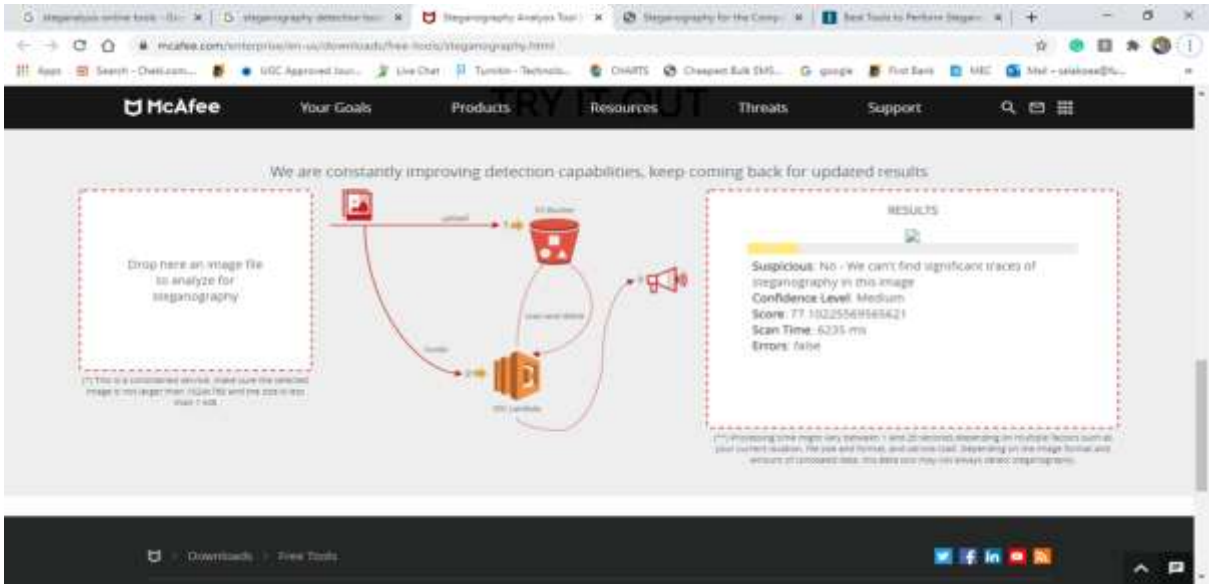

Fig. 6. The output of Mcafee online steganalysis

8. Conclusion and Recommendations

The paper-based voting system has been characterized by irregularities such as voter's impersonation, votes' alteration by corrupt election officers and multiple voting by a voter leading to an unwanted candidate emerge as the winner of an election. This research was on a secured electronic voting system based on fingerprint and visual semagram techniques. A highly secured e-voting model was designed, implemented, tested and evaluated. The results indicated an accuracy of 99.81% making the proposed system reliable in tackling the identified problems, restoring confidence and improve citizens' participation in the electoral process.

Based on the experimental results, the following recommendations were made:

1. the proposed e-voting model is highly recommended for use by the Students Union Government (SUG) and other local/international electoral commissions for voting an individual into the position of authority.
2. the proposed model is also recommended to various security agencies such as the State Security Service (SSS), the Defence Intelligence Agency (DIA), the Nigerian Armed Forces, the Federal Bureau of Investigation (FBI) and others across the world for dissemination of sensitive information through the public network.
3. the manufacturers of electronic voting machines are hereby offered a model for use in the development and securing of a fingerprint-based platform for a voting system.
4. reduction of error rate through a new fusion of ear biometric trait and randomly generated number should be the focus of future e-voting systems for extremely secure authentication.
5. finally, scholarly investigations on other functional and security requirements are recommended to strengthen the use of e-voting systems.

Appendix Flowcharts of proposed e-voting model

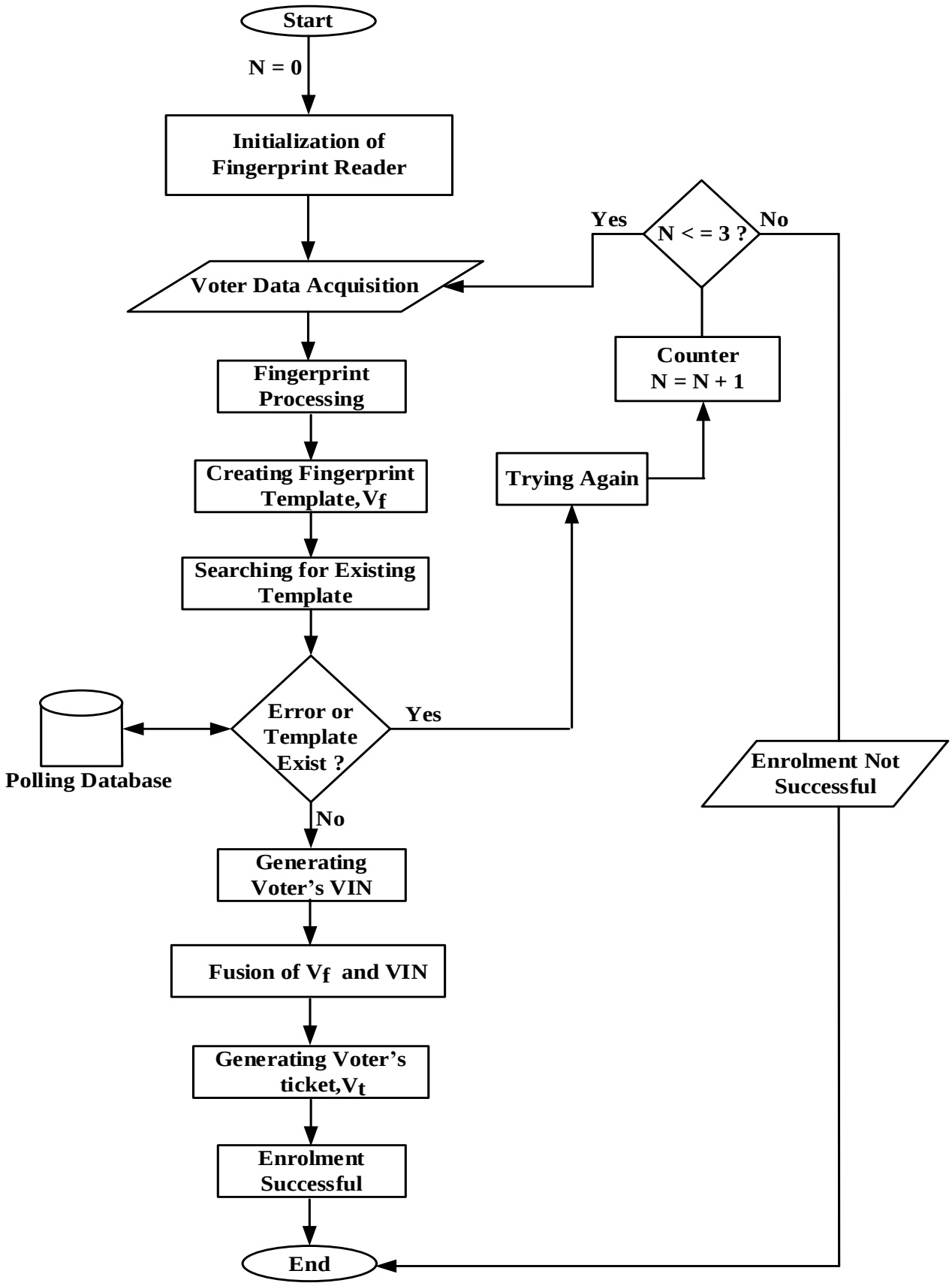

Fig.7. Enrolment module

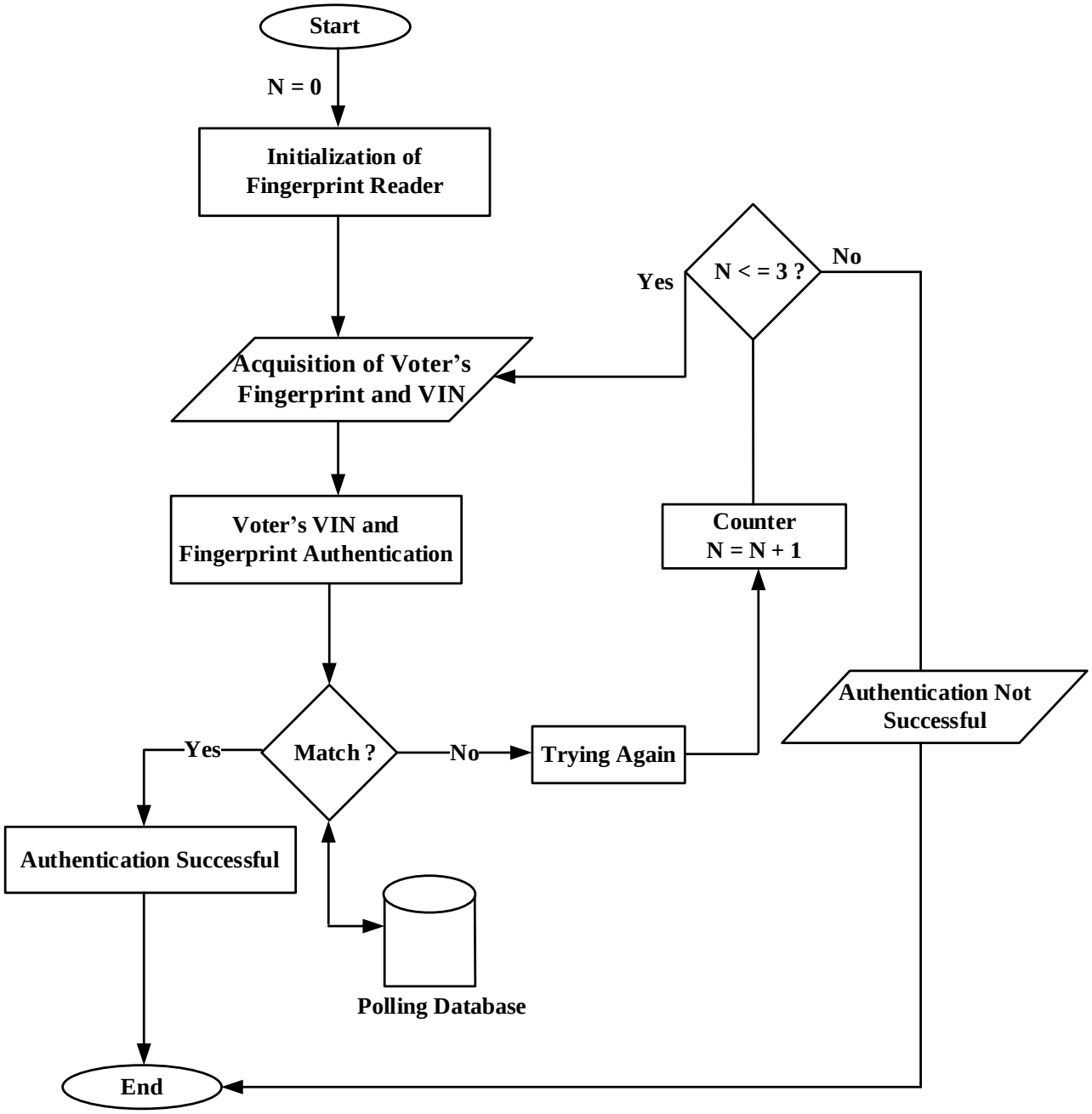

Fig.8. Authentication module

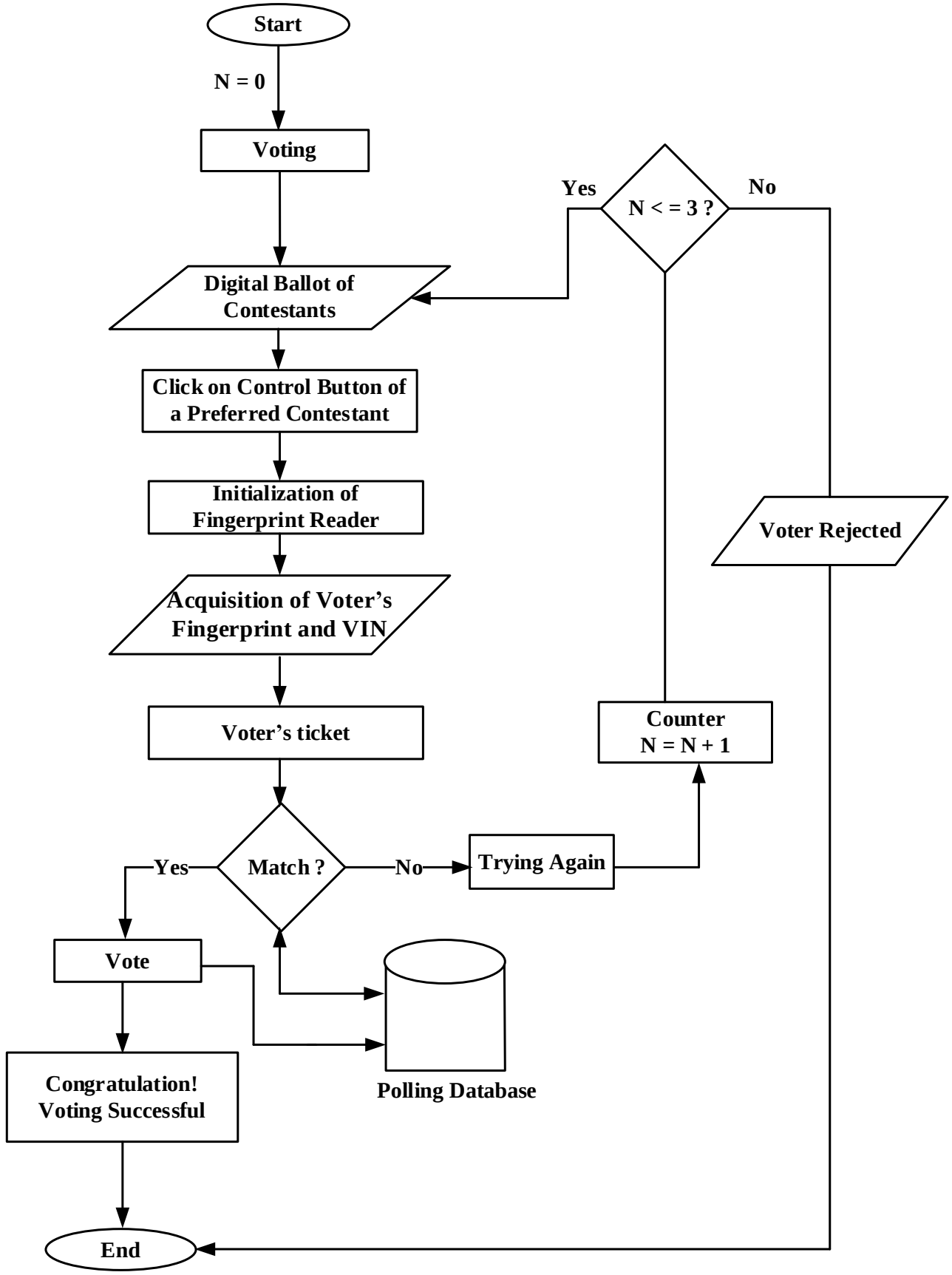

Fig.9. Voting module

References

[1] Adewale, O. S., Boyinbode, O. K., & Salako, E. A. (2020b). An enhanced computational fusion technique for the security of authentication of electronic voting systems. *International Journal of Smart Security Technologies*, Vol. 7, No. 2, pp. 22–37.

[2] Adewale, O. S., Boyinbode, O. K., & Salako, E. A. (2020c). A review of electronic voting systems: a strategy for a novel. *International Journal of Information Engineering and Electronic Business (IJIEEB),* Vol. 12, No.1, pp. 19–29.

[3] Akhil, S., Nishita, S., Shruti, S., Soumi, B., & Madhuri, C. (2020). Blockchain enabled online-voting system. A paper of ITM Web of Conferences 32, 03018 (2020), International Conference and Expo on Advanced Ceramics and Composites. https://doi.org/10.1051/itmconf/20203203018

[4] Aman, J., Yojna, A., Jitendra, P., Sachin, Y., & Konark, S. (2020). Design and development of biometric enabled advanced voting system. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST),* Vol. 8, No. 3, pp. 50-53.

[5] Annadate, M. N., Shreyans, S. G., Nivita, R. K., & Pushkar, S. N. (2017). Online voting system using biometric verification. *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 6, No.4, pp. 276 –281.

[6] Atul, M., Divyansh, Y., Ankit, C., Deepak, P., & Shubham, G. (2018). A secured electronic voting machine using biometric. *International Journal of Electronics, Electrical and Computational System*, Vol. 7, No. 4, pp. 105–108.

[7] Bhavneet, K., Pooja, N., & Harish, K. (2013). Steganography techniques: Concepts and overview. *International Journal of Computer Science and Communication Engineering*, Vol. 2, No. 4, pp. 33–38.

[8] Catalin, L. (2010). Car access using multimodal biometrics. The annals of the "Ştefancel Mare" University of Suceava. *Fascicle of the Faculty of Economics and Public Administration*, Vol. 10, pp. 368–377.

[9] Divyank, M., Aaditya, S., & Saurabh, G. (2018). Android voting system using facial recognition. *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, No. 3, pp. 288–291.

[10] Firas, I. H., Seifedine, K., & Oussama, K. Z. (2017). Web-based voting system using fingerprint: design and implementation. *International Journal of Computer Applications in Engineering Sciences*, Vol. 2, No. 4, pp. 404-409.

[11] Lichun, C. (2018). Trust and security in the e-voting system. *Electronic Government: An International Journal*, Vol. 6, No. 4, pp. 343-351.

[12] Jaison, I. P., Kishoritha, K. R., Ganesh, B., Gokulprashanth, P., & Udhayakumar, G. (2018). Electronic voting machine with facial recognition and fingerprint sensors. *International Journal of Advance Research and Development*, Vol. 3, No.3, pp. 165–170.

[13] Joseph, B. A. (2017). Automated voting system using bimodal identification and verification technique. *Annals Computer Science Series*, pp. 117–133.

[14] Olaniyan, O. M., Mapayi, T., & Adejumo, S. A. (2011). A multiple scan biometric-based system for electronic voting. *African Journal of Computing & ICT*, Vol. 4, No. 2, pp. 9-16.

[15] Olowookere, A., & Awode, T. (2014). Design of a secured electronic voting system using multimodal biometrics. *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, No. 12, pp. 7101 – 7106.

[16] Rajnikannan, M., & Ashok, K. D. (2016). Estimating the impact of fingerprint image enhancement algorithms for better minutia detection. *International Journal of Computer Application*, Vol. 1, No. 7, pp. 126 – 137.

[17] Razu, A., Javed, M. S., Asraf, A., Rajib, M., & Arifa, K. (2020). The future of electronic voting system using blockchain. *International Journal of Scientific & Technology Research*, Vol. 9, No. 2, pp. 4131-4134.

[18] Sanjay, K., & Manpret, S. (2017). Design a secure electronic voting system using fingerprint technique. *International Journal of Computer Science Issues (IJCSI*), Vol. 10, No. 4, pp. 201-218.

[19] Sathya, G., Jeevanantham, C., Sangeetha, K., Venmathi, V., & Ramya, P. (2017). Biometric authentication system based on aadhar card. *International Journal of Pure and Applied Mathematics*, Vol. 117, No. 9, pp. 7–10.

[20] Snega, S., Saundarya, S., & Balraj, R. (2018). Highly secured electronic voting machine using aadhaar in IOT platform. *International Journal of Electrical and Electronics Research*, Vol. 6, No. 2, pp. 41–47.

[21] Tamilarasu, P., Aadhithyan, S., Gowthaman, K., & Hariprakash, V. (2018). Fingerprint based electronic voting machine. International Journal of Current Engineering and Scientific Research (IJCESR), Vol. 5, No. 2, pp. 67–70.

[22] Varsha, N. G., Sangamesh, J., Shravya, R., & Shivaraja (2018). Aadhar based biometric voting system. *International Journal of Advance Research, Ideas and Innovations in Technology*, Vol. 4, No. 3, pp. 424–427.

[23] Ameh, I. A., Olayemi, M. O., & Olumide, S. A. (2016). Securing cardless automated teller machine transactions using bimodal authentication system. *Journal of Applied Security Research*, Vol. 11, No. 4, pp. 469-488.

[24] Kaur, N. S., & Patterh, M. S. (2017). A biometric fusion based on face and fingerprint Recognition using ANN. *International Journal Recent Innovation Trends Computer Communication*, Vol. 5, pp. 88–92.

[25] Milind, R. E., & Deshpande, P. P. (2018). Multimodal biometric recognition system using feature level fusion. In Proceedings of the 2018 IEEE Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India,16–18 August 2018, pp. 1–5.

[26] Arjona, R., Prada-Delgado, M.A., Baturone, I., & Ross, A. (2018). Securing minutia cylinder codes for fingerprints through physically unclonable functions: an exploratory study. In Proceedings of the 2018 International Conference on Biometrics (ICB), Gold Coast, Australia, 20–23.

[27] Huadi, Z., Wenqiang, J., Mingyan, X., Srinivasan, M., & Ming, L. (2020). Blinkey: A two-factor user authentication method for virtual reality devices. Proceeding ACM Interact. Mob. *Wearable Ubiquitous Technol,* Vol. 4, No. 164, pp. 29 https://doi.org/10.1145/3432217

[28] Rohit, S. (2020). A Score Level Fusion approach for multimodal biometric fusion. *International Journal of Scientific & Technology Research*, Vol. 9, No. 1, pp. 4241-4245.

[29] Yaseen, M., Anton, D. K., Gugulethu, M. H., Cynthia, S. N., Norman, N., & Portia, K. (2021). Biometric recognition of infants using fingerprint, iris, and ear biometrics. *Institute of Electrical and Electronics Engineers (IEEE) Access*, Vol. 9, pp. 38269-38286.

[30] Tajinder, K., Shashi, B., & Surender, J. (2021). An improved biometric fusion system of fingerprint and face using whale optimization. International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 12, No. 1, pp. 664-671.
[31] Leghari, M., Memon, S., Dhomeja, L. D., Jalbani, A. H., & Chandio, A. A. (2021). Deep feature fusion of fingerprint and online signature for multimodal biometrics. *Computers*, 10, 21. https://doi.org/10.3390/computers10020021
[32] Salako, E. A. (2021). Design and Implementation of a Fingerprint-Based Platform for Securing Electronic Voting System. A Thesis in the Department of Computer Science, School of Computing, Submitted to the School of Postgraduate Studies in Partial Fulfilment of the Requirements for the Award of Doctor of Philosophy (Phd) in Computer Science of the Federal University of Technology, Akure, Nigeria.
[33] Adewale, O. S., Boyinbode, O. K., & Salako, E. A. (2020). Visual semagram: An enhanced technique for confidentiality requirement of electronic voting system. *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.12, No.4, pp.51-59, 2020. DOI: 10.5815/ijcnis.2020.04.05
[34] Olayemi, M. O., Taliha, A. F., Aliyu, A., and Olugbenga, J. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto- watermarking approach. *International Journal of Information Engineering and Electronic Business (IJIEEB)*, Vol. 8, No. 5, pp. 9–17, DOI: 10.5815/ijieeb.2016.05.02.

Authors' Profiles

Adewale Olumide Sunday is a Professor of Computer Science, Department of Computer Science, School of Computing, Federal University of Technology (FUTA), Akure, Nigeria. He has Ph.D. in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria in 2002; M.Tech in Computer Science, Federal University of Technology, Akure, Ondo State, Nigeria–1998; BSc Computer Science with Mathematics Ogun State University (Now OOU), Ago Iwoye, Nigeria, in 1991. His Research/Areas of Interest are Cyber Security, Software Engineering, E-Learning and Digital Library. He is a member of many professional bodies. He is a member of the Institute of Electrical and Electronic Engineers and Association of Computer Machineries (135763); Member, Infonomics Society, United Kingdom; Member, Computer Professional & Registration Council of Nigeria (CPN). At present, Prof. Adewale is the Dean, School of Computing, Federal University of Technology, Akure (FUTA), Nigeria.

Olutayo Boyinbode (PhD) is an Associate Professor and Head of the Department of Information Technology, Federal University of Technology, Akure, Nigeria. Her research interests are Mobile and Ubiquitous Learning, Mobile Networks, Machine Learning and the Internet of Things for Development ((IoT4D). She has several publications in reputable peer-reviewed journals and has also served as a reviewer to several peer-reviewed journals. She is a professional member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE).

Salako E. Adekunle is a Ph.D holder in Computer Science, received a Master of Technology (M.Tech) in Computer Science and a degree (B.Eng) in Electrical and Computer Engineering. He is a member of the Nigeria Computer Society and Teachers Registration Council of Nigeria (TRCN). His research interests include Biometric Security, Educational Technology and Control Technology. He has published papers in reputable local and international journals and his published textbooks included Introduction to Computer Logic, Learning Pascal Made Easy, A Handbook on Symbolic Logic and BASIC Programming Language.

How to cite this paper: Adewale Olumide S., Boyinbode Olutayo K., Salako E. Adekunle, "An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.13, No.5, pp. 24-37, 2021. DOI: 10.5815/ijieeb.2021.05.03