Securing Electronic Voting System Using Crystographic Technique

By

Oke, B. A., *Olaniyi, O. M., **Aboaba, A. A., and ***Arulogun, O. T.
*Department of Computer Engineering,
Federal University of Technology Minna, Niger State Nigeria
**Department of Computer Engineering,
University of Maiduguri, Borno State, Nigeria.
***Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
Email: oke.pg612187@st.futminna.edu.ng

BSTRACT

The aim of this paper is to design a secure electronic voting system that is based upon the electoral process for developing countries. The concept of voters' information processing and storage arose immediate fears about election data security and privacy. If the voter's choice is accessed by an illegitimate party, it may lead to malicious attack and any alteration of election results can affect the integrity of election. The need to secure electronic voting system through protection of voters' data, confidentiality of casted vote during and after election becomes imminent. This paper addresses confidentiality and post-election auditing issues in electronic voting system using crystographic technique (a combination of cryptography and steganography). Electronic ballot confidentiality was addressed using crystographic algorithm involving synergistic combination of an enhanced Advance Encryption Standard (E-AES) and Space Insertion Text Semagram and post auditing issue of counted ballot was technically addressed with SHA-256 cryptographic Hash function. Performance evaluation of these techniques show that the developed integrated techniques can effectively handle confidentiality and post election auditng verification issues in electronic voting systems in digitally divided poll sites electoral votng scenerio.

Keywords: Confidentiality, Electronic Voting, Authentication, Security, AES, Auditng.

INTRODUCTION

One basic feature of democracy that cuts across all divides of people is the act of election. Free and fair elections are the basis of true democracy. Democracy thus encourages individual freedom according to the rule of law, so that people may act and express themselves as they choose (Ofori-Dwumfuo *et al.,* 2011) Today, there is a wide understanding that traditional voting systems should be computerized to reduce the vote counting time, provide evidence that a vote is being correctly accounted for, reduce fraud, remove errors in filling out ballots, and improve system usability (Santin *et al.,* 2008).

Many services that once required a voter to physically present himself at a counter and fill out paper forms have now been made available in digitalized form, where, after some kind of authentication, the same service is done over a digital medium (Bokslag *et al.*, 2016). The advantages

are numerous and significant, as it is more convenient for the voters and digital information is far more suitable for automated processing. Electronic voting was introduced with the objective of reducing electoral challenges such as mass ballot paper stuffing, rigging, intimidation, and omission of valid voters from the voters list, errors due to miscomputation and forged results, snatching of ballot boxes, impersonation, and inflation of election results.

These electoral challenges not only weaken public trust in democratic institutions but also adversely affect the provision of public goods (Debnath *et al.*, 2017). As a consequence, it is only fair that one starts thinking about an electronic equivalent for manual voting. Most countries still use paper ballots which are counted by manually after the voting period ends (Bokslag *et al.,* 2016). This obviously has drawbacks: paper is wasted, manual vote counting takes time and is potentially more error-prone than electronic vote counting. As tempting as electronic voting may seem, it is important to realize the potential risks and drawbacks. The possibility to cast a vote, and the confidence that all votes are being taken into account in an honest manner is one of the main pillars of a modern democracy. The advantages and risks of electronic voting is one that cannot be over emphasized. Thus, it deserves careful thought. E-voting is often seen as a tool for advancing democracy, building trust in electoral management, adding credibility to election results and increasing the overall efficiency of the electoral process. The technology is evolving fast and election managers, observers, international organizations, vendors and standardization bodies are continuously updating their methodologies and approaches to ensure the confidentiality of votes. Properly implemented, e-voting solutions can eradicate certain common avenues of fraud, speed up the processing of results, increase accessibility and make voting more convenient for voters in some cases, when used over a series of electoral events, possibly even reducing the cost of elections or referendums in the long term. The inherent challenges of e-voting are considerable and linked to the complexities of electronic systems and procedures. Many e-voting solutions lack transparency for voters and even for election administrators (Wolf *et al.,* 2011). Most e-voting solutions are only fully understood by a small number of experts and the integrity of the electoral process relies largely on a small group of system operators instead of thousands of poll workers. If not carefully planned and designed, the introduction of e-voting can undermine confidence in the whole electoral process. It is therefore important to devote adequate time and resources to considering its introduction and looking at previous experiences of electronic voting.

Due to the requirement to protect the secrecy of the vote, security of the voter's identity and the vote cast need to be guaranteed. This is in itself a challenge as standard information system are inherently design for tracking and monitoring transactions that happen on them. More importantly, breaking the link between voter and vote means that the examination of an e-voting system after an election cannot prove directly that every vote was indeed counted and tallied as cast (Wolf et al., 2011). Without such mechanisms, manipulated or incorrect results produced by an e-voting.

This paper addresses confidentiality and post auditing issues in electronic voting system using Crystographic technique and SHA 256. Crystography involves the synergistic combination of schemes of cryptography and data hiding steganography for proper enhancement of security communications over public network (Gabriel *et al.,* 2013; Olaniyi *et al.,* 2015). Crystography in the context of this paper, involves securing voters details and votes using Enhanced Advance

Encryption Standard (AES) algorithm and Space insertion Text Steganographic algorithm,Semagram, and post auditing issue of counted ballot was technically addressed with SHA-256 cryptographic Hash function.

REVIEW OF INFORMATION SECURITY TECHNIQUES USED IN E-VOTING SYSTEMS

Information or communication security is as old as these two concepts (Cryptography and Steganography) themselves. Several algorithms have been put forward to secure information while communicating it. Especially in the area of voting system, the algorithms have been employed to provide voting anonymity, ballot secrecy, and voters' privacy. Cryptography is necessary for protecting privilege information when communicating over an unsecured or untrusted medium. Cryptography makes a message unreadable to a third party, however, it does not hide the existence of the message to the third party. In cryptography, an unencrypted data is referred to as plaintext, which is encrypted into cipher text. The cipher text is in turn decrypted into usable plaintext. The encryption and decryption are based upon the type of cryptography scheme being employed and some form of key. This process is written in equation (1)

$$C = E_k(P) \qquad (1)$$
$$P = D_k(C)$$

Where P is the plaintext, C is the cipher text, E is the encryption method, D is the decryption method, and k is the key. Cryptography according to the type of key used could be; public key, secret key and hash functions cryptography. It has also been widely used in e-voting system (Moayed *et al.,* 2008; Mursi *et al.*, 2015; Olaniyi et al., 2015; Olaniyi *et al.*, 2013; Usha *et al.*, 2011).
The techniques of information hiding (Steganography) can be grouped as shown in Figure 1.

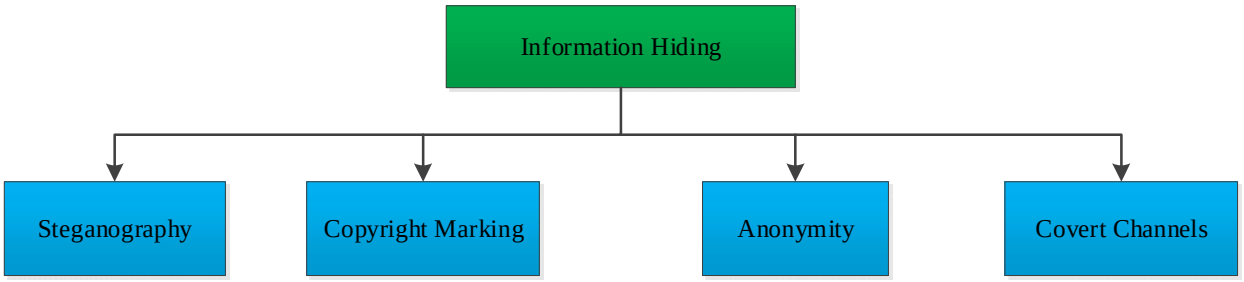

Figure 1: Types of Information hiding Techniques

Steganography and copyright marking can further be divided into other types. Steganography could be technical or linguistic, while copyright marking could be robust or fragile watermarking. Out of these categories, steganography and watermarking approaches are widely used in the literature (Gunjal *et al.*, 2012; Gunjal *et al.*, 2010; Olaniyi *et al.*, 2016). In this paper, format-based steganography was used due to its simplicity, requires less lines of instruction and memory capacity.

One major limitation of all encryption systems is that the output data (the cipher text), if intercepted, alerts the intruder to the fact that the information being transmitted may be of some importance and that it is thereby worth attacking. It is therefore of significant value if a method

can be found that allows data to be transmitted by embedding it in non-sensitive information after it has been encrypted. Steganography is the art of covered or hidden writing. The tenacity of steganography in covert communication is to hide a message from a third party. It differs from cryptography which is the art of secret writing. Most digital steganography techniques employ graphical images or audio files as the carrier medium through the use of least significant bit substitution or overwriting. The concept of steganography has found widespread use in e-voting (Olaniyi *et al.*, 2015; Osho *et al.*, 2015; Rura *et al.*,2011; Usha et al., 2011) due to the need to provide a secure e-voting system over unsecure wireless network.

Text steganography can involve either changing the formatting of an existing text, or changing words within a text, or generating random character sequences as well as using context-free grammars to generate readable texts. It has an advantage in that storing text file requires less memory and it is faster as well as easier communication makes it preferable to other types of steganographic methods (Koluguri *et al.*, 2014). The methods which change the format of the text, Format based steganography, usually has large capacity for hiding information. (Roy *et al.*, 2011) used a text steganography algorithm using combination of line shifting and word shifting with high capacity of cover object. The method has a good hiding capacity as it hides more than one bit of data in each line of cover text. (Por *et al.*, 2008) used an approach for text steganography involving a combination of inter-word spacing and inter-paragraph spacing with the aim of increasing the hiding capacity of the traditional space insertion method. The approach has an advantage of being able to provide six different embedding capacities depending on the size of the secret message.

Crystography emphasizes the synergistic combination of information hiding techniques of steganography and cryptography for enhancing the security of communications over enterprise network (Gabriel *et al.,* 2013; Olaniyi *et al.*, 2015). In (Olaniyi *et al.,* 2015), the authors used a generic security requirements for e-voting system using modified stegano-cryptographic approach.. The approach ensures that the following e-voting requirements were met: availability, authenticity, privacy, confidentiality, accuracy, and integrity. The model is based on the assumption that an electorate has a unique national identification number prior to registration procedure. The model cannot handle the issue of coercibility of voters and bribery. Same authors used an enhanced stegano-cryptographic model for secure e-voting system (Olaniyi *et al.*, 2015), however, authentication process takes more time as the voter will have to wait to receive a one-time-pin password via SMS as well as post-election auditing was not considered. A combination of steganography and cryptography will be use in this paper to enhance security requirement of ballot confdentilaity and secrecy as well as post electoral verification of counted votes. However, unlike previous work where audio and image steganography were used (Rura et al., 2011), this paper used text steganography. This will aid the consumption of less memory, faster and easier communication. In this paper, a digital message hiding scheme is proposed for the combination of steganography and cryptography, crypt-steganography or crystography using Enhanced Advance Encryption Standard algorithm and Space insertion Text Steganographic algorithm. The combination of these two techniques satisfies the requirements such as enhanced security, robustness between sender and receiver and requires less instruction line and low memory capacity which are essential consideration during hardware design.

Auditing the traditional paper voting system is unlike auditing the e-voting system. While major work has been done on auditing of election results of the traditional voting system, few works have focused on the auditability of e-voting. Peisert *et al.* (2009) discusses the need for a forensic audit trail (FAT) which can assist auditors to analyze the actions of e-voting systems. The work only presented a framework which is yet to be implemented. A secured and auditable e-voting system using stock indices was used by Clark *et al.,* (2007). An e-voting procedure using multi-part ballot mode (M-NOTE) was used by Pan *et al.,* (2015). The system provides voters an enhanced way to cast and edit their vote with great level of anonymity. M-NOTE provided an outstanding secured level thus reducing the possibility of ballot reconstruction and manipulation of voting results. However, the system requires some level of technical-know-how from the voters. This will thus reduce the level of participation from the eligible voters. It could also lead to vote coercion as people with less technical-know-how will require the help of some other people to cast their vote. Cunha *et al.* (2006), proposed a method used for auditing an e-voting system for the Portuguese parliament election. Several criteria and sub-criteria were defined for the auditing process and each sub-criteria were assigned a weight obtained using Analytical Hierarchy Process (AHP). At the end of the voting process, an interview conducted on the voters showed that 80.5 % of the voters trusted the security of the e-voting system. The audit approach used did not produce a final ranking of the system. In addition, the auditing process has too much of human involvement. Chondros *et al.* (2016) used D-DEMOS, a distributed end-to-end verifiable e-voting system which allows voters to verify their vote or outsource auditing to a third party if the need arise. Though voters can self-verify their votes, separate auditors are still required to verify the election process. Though their system is end-to-end verifiable thus providing assurance to voters that their votes have been well recorded, it will require voting through the internet which can lead to low level of participation in developing countries of high level of digital divide.

While steganography conceals the existence of a message, cryptography renders a message unintelligible. In this paper, ballot confidentilaity are ensured by handling all messages to be transmitted and stored locally in form of text for achievng the merit of less memory, faster as well as easier communication compare to technical steganographic methods in (Olaniyi *et al., 2015*). These will be key in using the keypad unit of the Polling Unit system. During election, voters' ballot will be save locally and sent to the server in form of text message. Therefore, a combination of text steganography and cryptography is used as opposed to many work in the literature where audio or image steganography were used (Olaniyi *et al.,* 2015; Rura *et al*., 2011; Usha *et al.*, 2011). In particular, space insertion steganography and enhanced AES was used as the cryptographic method leading to a Crystographic model. The message is first encrypted using enhanced AES, while space insertion technique is applied to the obtained cipher text to hide the message. After this, the message is then hashed on the server and transmitted to the collation unit.

MATERIALS AND METHOD

The secure electronic voting system consists of both hardware and software parts integrated together. The hardware component of this system consists of the ATMEGA328P and ATMEGA16 Microcontrollers, CD4052 Port Multiplexer, Fingerprint Module, GSM Module. Smart Card Reader, Display Unit, LEDs, Key Pad and Electronic ballot interface.

System Hardware Design Consideration

No separate system is required for registration and voting. Registration process is made easy with the help of both the keypad and display units. The MFA (combination of biometric and smart card), RF, and GSM communication unit are connected to the processing unit (ATmega microcontroller) via a serial port multiplexer. This was necessary because the microcontroller has only one serial interface. Two different processors are used, one as the central processor while the other process the input from the user keypad. The central processor serves to monitor and process all connected units. RAM and flash memory was considered in selecting the microcontroller used for this task. A microcontroller with large I/O was selected to handle the keypad unit.

The complete circuitry also includes the e-ballot unit. After authentication, the voter is ready to cast his/her vote. This is done by simply clicking on the fingerprint icon in front of the party which the voter is voting for. If the voter is eligible, the green LED comes ON and the user votes by pressing in front of his or her party of interest. In the case where the user is unauthorized, the red LED comes ON and an alarm is sounded to bring the attention of security personnel. After voting, a local copy of users' vote is saved while an encrypted version is sent to the collation unit. After considering the different modules and component parts of the secured e-voting system, the complete circuit design of the secured e-voting system and e-ballot unit is as shown in Figure 2 and Figure 3.

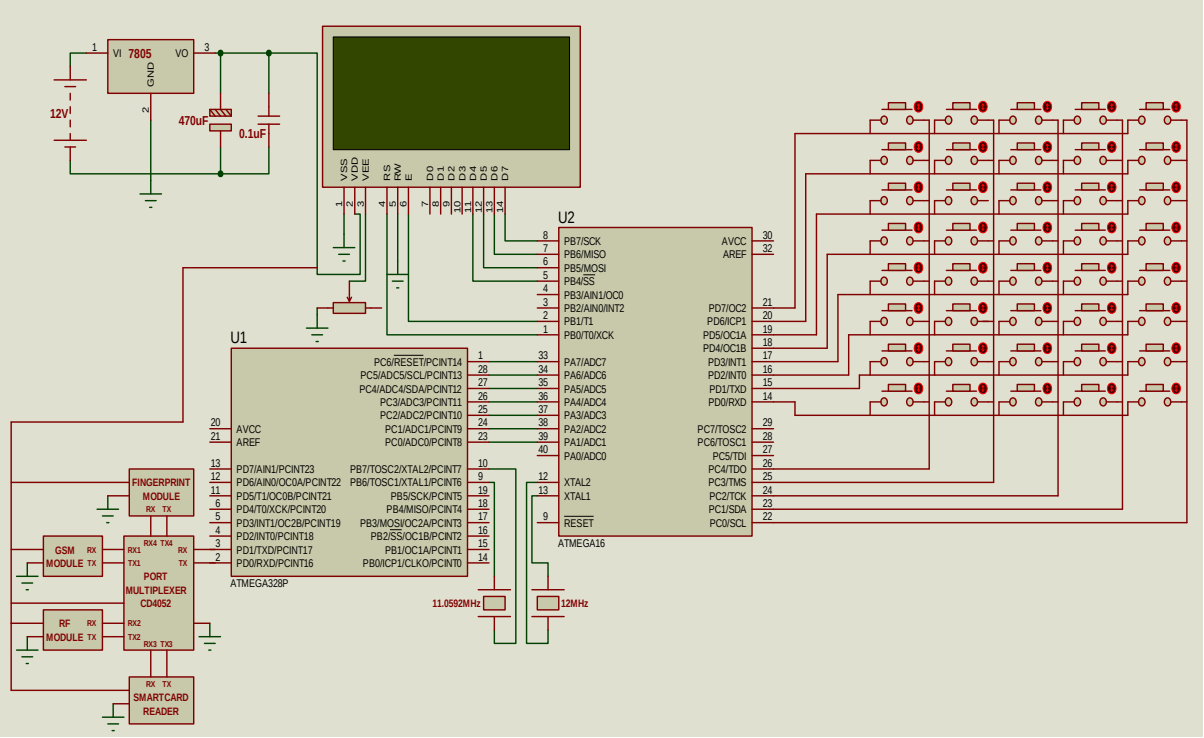

Figure 2: Complete circuit diagram of the Polling unit section of the secured e-voting system

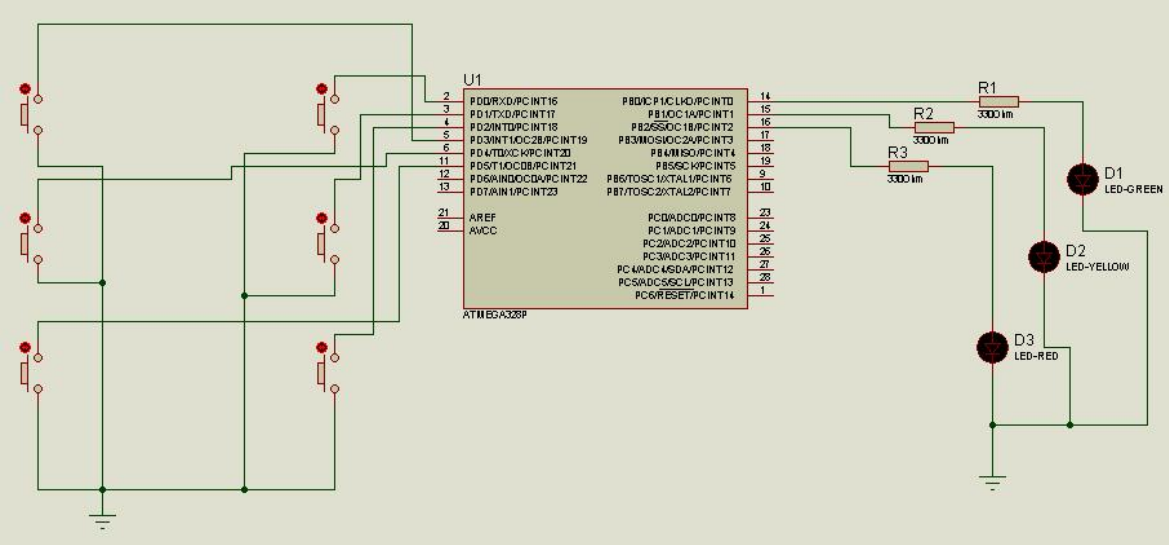

Figure 3: Circuit diagram of e-ballot unit

Resistors R1-R3 can be calculated as in equation (2).

$$V_{«c} = V_R + V_{LED}$$
$$= I_{LED}(R + R_{LED}) \qquad (2)$$
$$R = \frac{V_{«c} - I_{LED}R_{LED}}{I_{LED}}$$

where V_μ is the voltage from the microcontroller port, I_L is the maximum current the LED can withstand, R_L is the resistance of the LED. Thus, the protection resistor is calculated as in equation (3).

$$R = \frac{4.95 - 2}{10 \times 10^{-3}} = 295\Omega \qquad (3)$$

where the output of the microcontroller port is 4.95 V, and voltage drop of 2 V drops across the LED with current of 10 mA. Therefore, from Figure 3, R1-3 use resistance value of 300 ohms.

As soon as the processing unit receives the voter's vote, the electronic ballot comprising of the voter's details and copy of vote is prepared. It is then encrypted using Crystography, and sent to the voting server. A SHA256 digest of the crystographically encrypted version is also created and sent to the coalition unit. This is particularly needed during the auditing stage.

System Software Design Consideration

This paper focus on authentication, issues in verifying and validating eligible registered voters using Smart card readers (SCRs), a low power technological device for the accreditation of voters through Permanent Voter's Cards (PVC). Confidentiality of vote was improved on using Crystographic model (a combination of AES and text steganography). For vote auditing, the SHA-256 algorithm was adopted. The methodology taxonomy of the secure electronic voting system is summarized in Figure 4.

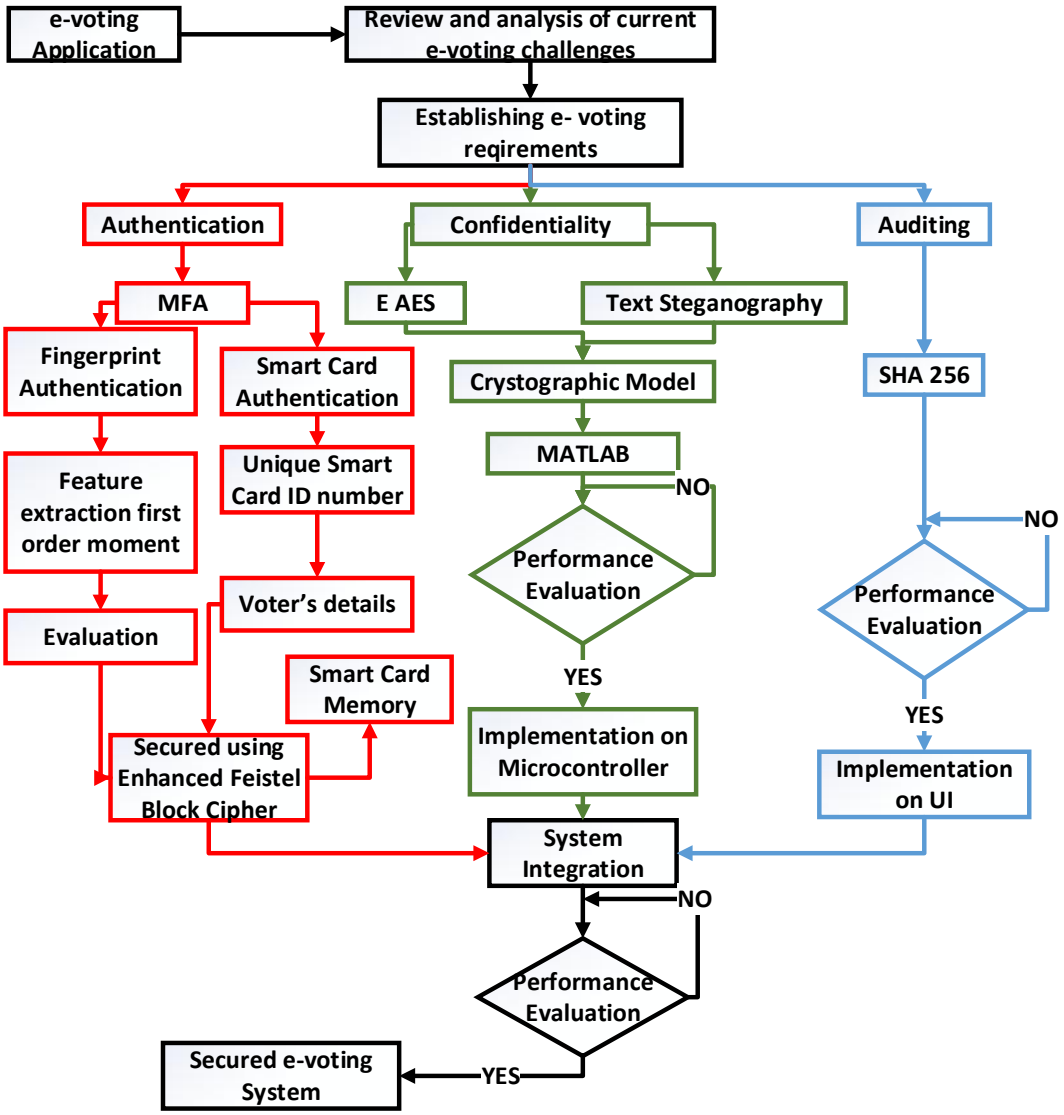

Figure 4: Methodology Taxonomy

Enhanced Advanced Encryption Standard (AES)

The Advance Encryption Standard (AES), unlike the Feistel block cipher, makes use of four different operations: byte substitution (SubBytes), byte permutation (ShiftRows), arithmetic operation over a finite field (MixColumns) and exclusive OR operation with the round key (AddRoundKey). The traditional AES algorithm accepts an input of 128 bits (16 bytes) data to produce a 16 bytes cipher text.

However, this input size of data is not enough to handle each voter's details in the secure e-voting system. Thus, the traditional AES structure was enhanced to accommodate the voter's details. In the enhanced structure, the size of the incoming voter's details is first computed. The voter's details is then divided into block of 16 bytes. In case a particular block is not up to 16 bytes, such block is zero padded to make up 16 bytes before processing. This process is summarized in Figure 5.

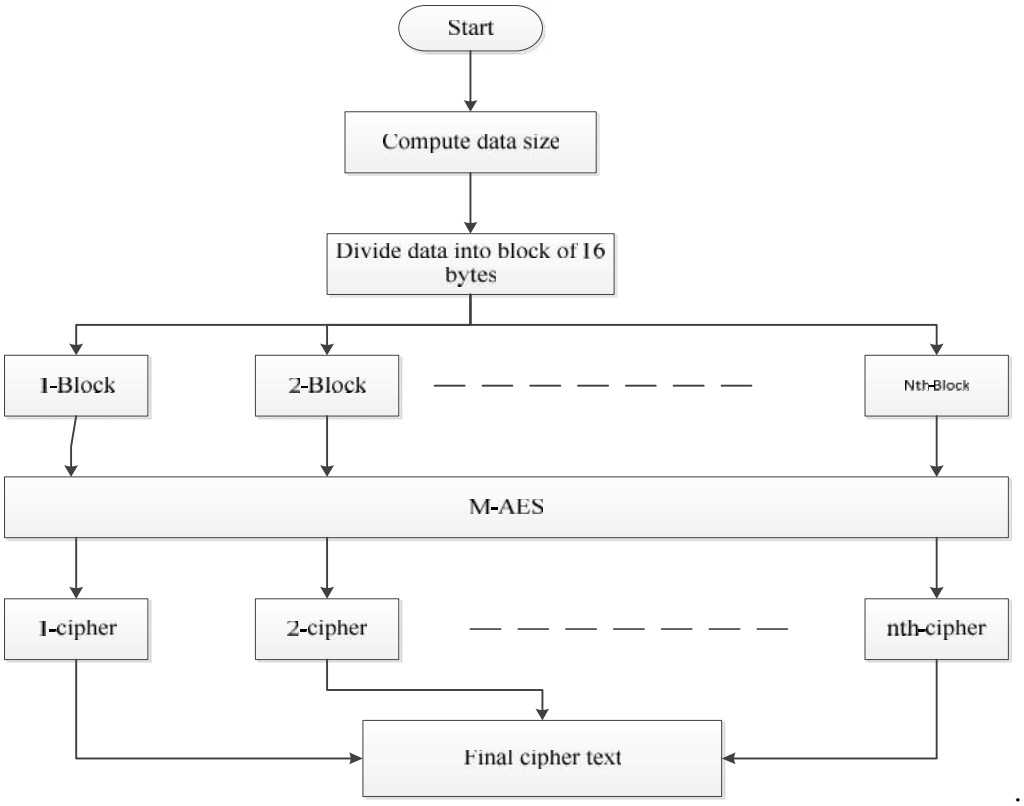

Figure 5: Block diagram of the enhanced AES structure.

A typical voter's details and vote goes beyond the size of the plain text (16 bytes) presented which is the size the traditional AES algorithm works on. Thus, the AES algorithm was enhanced.

Text Steganography using Space Insertion Techniques

Text Steganography is the most difficult kind of Steganography; this is due to the lack of redundant information in a text file, while there is a lot of redundancy in a picture, video or a sound file, which can be utilized in Steganography (Stallings, 2000). Text Steganography can involve anything from changing the formatting of an existing text, to changing words within a text, to generating random character sequences or using context free grammars to generate readable texts. Storing text file require less memory and its faster as well as easy communication makes it preferable to other types of steganographic methods. Format based steganography uses the physical formatting of text as a space in which to hide information.

It generally modifies existing text in order to hide the steganography text. Space insertion text steganography have been used in this work. The output of the encryption stage serves as input to the text steganography algorithm. Considering a ciphertext "FEAD5FA9263FCC98CA61650881B67E59" obtained from the plain text "This is CPE Dept", the stego-text obtained after applying space insertion will look like "FEAD5209263FCC20CA6165208 1B67209". The hexadecimal number in red is the ASCII code for blank space. Thus, an eavesdropper who is able to receive the latter will probably get the message

"Ñƒ¶?E¨Z%Îù|Èwû C" after decryption. The combination of the encryption algorithm and text steganography leads to the crystographic model shown in Figure 6.

During the voting stage, each eligible voter requires his/her smart card and fingerprint to cast vote. On arriving the polling unit, the following algorithm takes place.

Input Place fingerprint and authentication on the device for authentication
Process Compare voter's data with registered data
Authenticate voter and verify if he/she has vote before
If *authentic*
Process: Proceed to the electronic ballot board
Process: Present smart card for the second time
Process: Record voter's ballot
Process: Apply Enhanced AES and text steganography
Output: Send voter's details and ballot to voting server
Output: Record digital receipt on smart card
End

The encrypted vote is transmitted to the voting server. A digital receipt, indicating a successful voting, is printed on the voter's smart card. Any further attempt to vote by such user will be denied by the system. Figure 7 shows the architecture diagram of the voting stage.

.

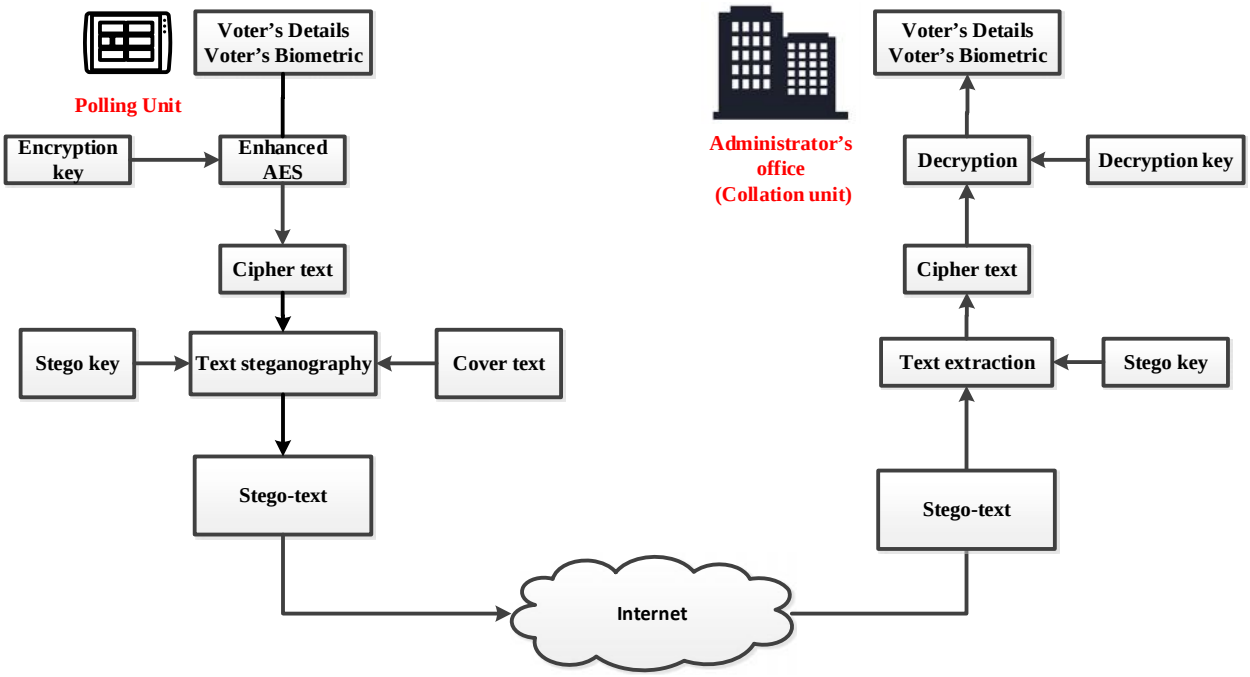

Figure 6: The crystographic model using Enhanced AES and text steganography

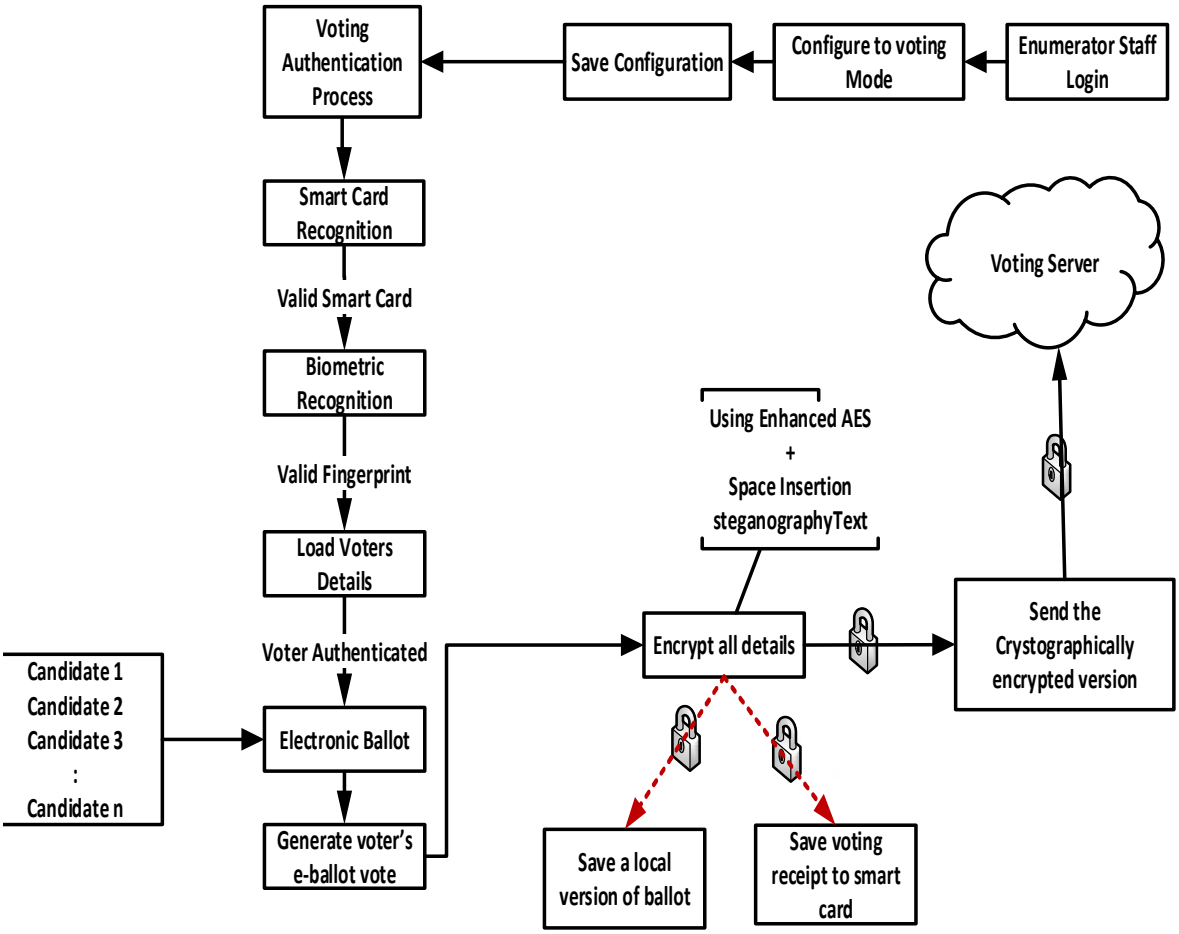

Figure 7: Architecture diagram of secure electronic voting stage

Encryption process
Initialization: Generate AES parameters such as Key (K), S-Box, etc. **Input:** voter's details **Output:** cipher text Compute length of voter's details If length > allowable size Reject voter's details Else Compute number of space to insert Convert input to hexadecimal Divide data into block of 16 bytes Compute cipher text Insert space randomly in cipher text

Record location of inserted space as Stego key
End

Decryption Process

Input: Cipher text, K and Stego key
Output: Voter's details
Remove inserted space using Stego key
Divide cipher text into block of 16 bytes
Perform inverse process of AES on each block using K
Store voter's details
End

Post-Election Auditing Countermeasure Design

[23], used a secure and observable auditing of electronic voting system using stock indices. The approach relies on the ability to conduct random ballot audit in an unbiased manner in other to establish election integrity. However, this technique cannot suit Nigeria election setup which is divided along regions and different constituencies. It has been suggested that any procedure for making a random selection for auditing in a voting system should satisfy four criteria (Cordero *et al.,* 2006):

1. Simplicity- easy to perform and understand the procedure involved.
2. Verifiability- there must be a procedure to verify the integrity of the auditing procedure
3. Robustness- It should be impossible for anyone, including the election officials, to predetermine which ballots will be audited.
4. Efficiency- it should require less time to conduct.

[23], used a secure and observable auditing of electronic voting system using stock indices. The approach relies on the ability to conduct random ballot audit in an unbiased manner in other to establish election integrity. However, this technique cannot suit Nigeria election setup which is divided along regions and different constituencies. Thus in this paper, hash crytographic function is adapted to technically handled post electoral auditing. A hash function maps a variable-length message into a fixed-length hash value, or message digest. Almost all cryptographic hash functions involve the iterative use of a compression function. The compression function used in secure hash algorithms falls into one of two categories: a function specifically designed for the hash function or an algorithm based on a symmetric block cipher. SHA and Whirlpool are examples of these two approaches, respectively [28].

The most widely used hash function has been the Secure Hash Algorithm (SHA). Table 1 shows comparison between the different SHA algorithms. SHA-1 produces a hash value of 160 bits,

however it is fast being replaced by SHA-2 family which comprises of SHA-256, SHA-384, and SHA-512. SHA-224 is a revised version of SHA-1.

Table 1: Comparison of SHA parameters

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message digest size	160	224	256	384	512
Message size	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Block size	32	32	32	64	64
Number of steps	80	64	64	80	80

All sizes are measured in bits

SHA-1 requires more steps, however, it has the least size of message digest. This would have been a better choice in the e-voting system considering the hardware memory requirement, however, SHA-1 is vulnerable to attack. No successful attacks have yet been reported on SHA-2 hash function. Consequently, the SHA-256 (a member of SHA-2) is used in this paper for the auditing process of the secure e-voting system. It has a message digest size of 256 bits with less number of steps when compared with SHA-1.

SHA-256 algorithm is used for validating the voter's vote. After a vote is casted at the polling unit, the voter's ballot is encrypted and sent to the server. The original encrypted voter's ballot is hashed, and a hashed version is transmitted to the collation unit. The collation unit algorithm verifies the integrity of the received voter's ballot before considering it a valid vote else it is discarded. The flow chart is shown in the Figure 8.

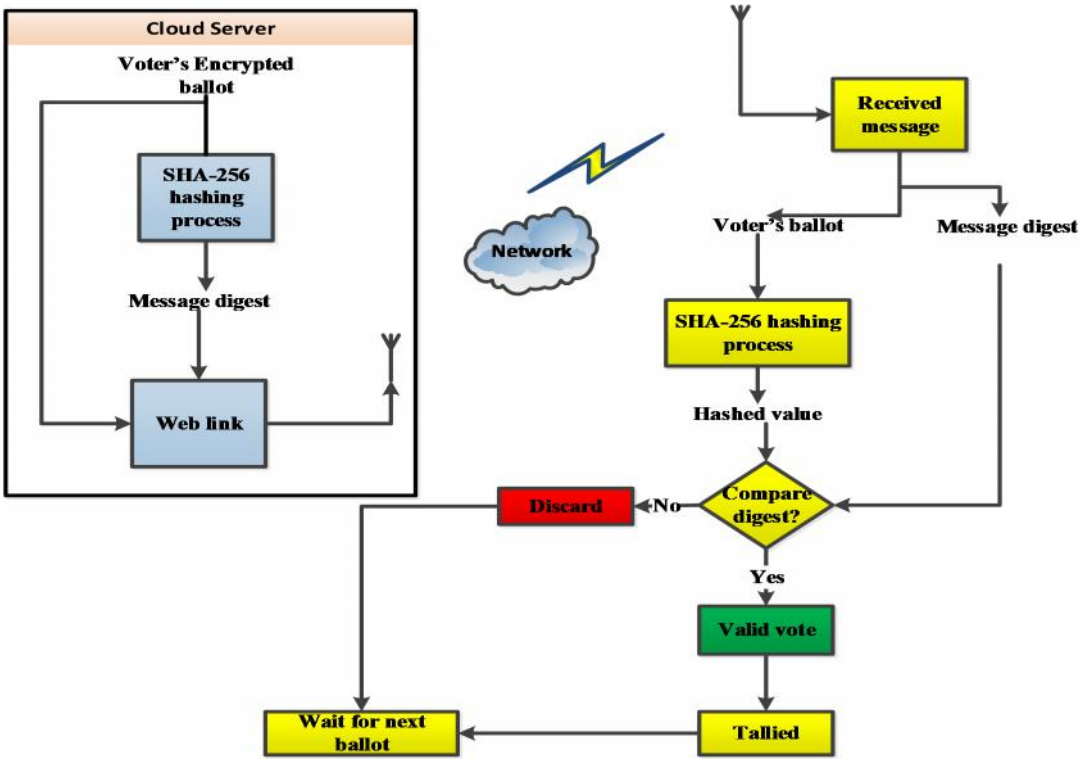

Figure 8: Flowchart of auditing process

RESULTS AND DISCUSSION

Performance Evaluation of Enhanced Advance Encryption Standard

The Enhanced AES algorithm discussed was implemented and tested on an arbitrary 16 bytes data. The time taken for all the various functions involved in the process to be executed were noted. The summary of the execution time for both the traditional AES and enhanced AES is as shown in Figure 9.

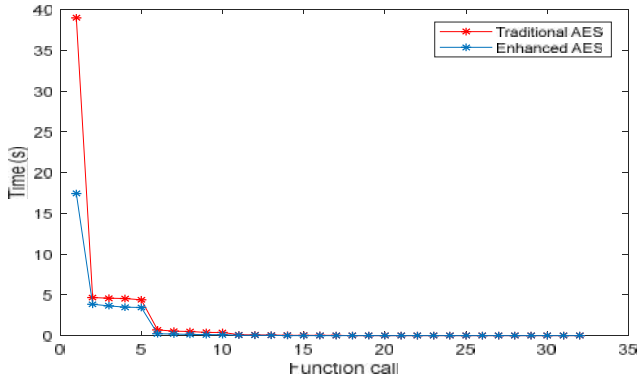

Figure 9: Performance summary of the enhanced AES algorithm and traditional AES

Comparing the run of the enhanced AES with the traditional AES in carrying out the same task as used in this paper, it was observed that the traditional approach takes close to 40s to run the same task that takes close to 20s in the enhanced version. Thus, the enhanced approach is approximately twice faster.

Performance Evaluation of Crystographic Technique

The enhanced AES receives a voter's details, compute its size and divide it into n-blocks of 16 bytes data to compute its cipher text. A typical voter's data is given in Table 2, followed by the results obtained in Table 3 and result obtained when space insertion not considered in Table 4.

Table 2: A typical voter's details

		Code
Voter's surname	Oke	
Other names	Babatope A	
Age		33
State of origin	Ekiti	13
Local govt. area	Ido-Osi.	08
Sex	Male	01
Fingerprint ID		45
Smart card number		12345
Polling unit number		234

Table 3: Results obtained from Table 2 voter's data

Initial plain text	**791071013232323232323232323232326697989711611111210132653232323232323313893039114103932323 2**
Cipher text	916552541013222023831021522212082919024926176241156881893021219443205741959521567211092055118249682521340203675199135171
Recovered plain text	**791071013232323232323232323232326697989711611111210132653232323232323313893039114103932323 2**

From Table 3, a one-to-one matching between the original plain text (voter's details) and the recovered plain text was observed, after the space insertion technique of text steganography was applied.

Table 4: Results obtained from Table 2 voter's data (when space insertion not considered)

Initial plain text	**791071013232323232323232323232326697989711611111210132653232323232323313893039114103932323 2**
Cipher text	916552541013222023831021522212082919024926176241156881893021219443205741959521567211092055118249682521340203675199135171
Recovered plain text without considering space insertion	**Ñƒ¶?E¨Z%Îù|Èwû C v ▪·9$!%⌐OμÄ▪ ö ├I?7'/!W^tc~ £YiÉ8&%6|\¶2**

From Table 4, a one-to-one matching between the original plain text (voter's details) and the recovered plain text was observed, after the space insertion technique of text was not considered. This technique enhances the confidentiality to be achieved. The enhanced AES and text steganography was also evaluated using the arithmetic mean formula given in equation (4).

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i \qquad (4)$$

The arithmetic mean *A* is the sum of the bytes of the cipher text output and divided by *n* the length of the file. The obtained arithmetic mean for the cipher text obtained using the voter's data in Table 2 was 125.42 *bits,* which is less than the ideal value of 127.5 *bits* (Sparrow *et al., 2016*).

Performance Evaluation of SHA256

The SHA 256 algorithm was implemented and tested on the cipher text in Table 3. The hash for cipher text is as shown below on Table 5

Table 5: Results obtained from Table 3 encrypted voter's data

Initial plain text	**916552541013222023831021522212082919024926176241156881893021219443205741959521567211092055118249682521340203675199135171**

Hash values (digests)	B7D2F1F4E8939A24F88C919DDF6BAE473EAC104EDCECEBFAF5584 72433BEC4ED

CONCLUSION

In this paper, a secure Electronic Voting using crystographic technique to addresses confidentiality issues for electronic voting system has been presented. An enhanced Advance Encryption Standard (E-AES) and Text Steganography was proposed to secure the data on transit on a public network, and a SHA256 cryptographic function for post-election audit. These three issues and their design consideration have been discussed in this paper.

The developed electronic voting system can further be improved upon by incorporating internet voting such that people who have the technical-know-how can vote from a remote location. Further improvement on this work in the area of Countermeasures against DoS and DDoS attacks: Denial of service (DoS) is an attack meant to bolt a network resources or make network resources inaccessible to its intending users. This is accomplished by flooding the target device with traffic and needless communication request that triggers a crash. Future study could provide mechanism to increase and protect the developed secured model for attacks due to DoS and DDoS

REFERENCES

Bokslag, W., & de Vries, M. (2016). Evaluating e-voting: theory and practice. *arXiv preprint arXiv:1602.02509*.

Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., … Roussopoulos, M. (2016). D-DEMOS: A Distributed, End-to-End Verifiable, Internet Voting System. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)* (pp. 711–720). IEEE. https://doi.org/10.1109/ICDCS.2016.56

Clark, J., Essex, A., & Adams, C. (2007). Secure and observable auditing of electronic voting systems using stock indices. In *Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on* (pp. 788–791). IEEE.

Cordero, A., Wagner, D., & Dill, D. (2006). The role of dice in election audits—extended abstract. In *IAVoSS Workshop on Trustworthy Elections*.

Cunha, J. F., Leitao, J. M., Faria, P. J., Monteiro, P. M., & Carravilla, A. M. (2006). A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament. In *2nd International workshop co-organized by council of Europe, ESF TED, IFIP WG 8.5 and E-Voting. August 2nd - 4th* (pp. 145–154). Bregenz, Austria: GI-Edition in Informatics Electronic Voting 2006.

Cordero, A., Wagner, D., & Dill, D. (2006). The role of dice in election audits—extended abstract. In *IAVoSS Workshop on Trustworthy Elections*.

Debnath, S., Kapoor, M., & Ravi, S. (2017). The Impact of Electronic Voting Machines on Electoral Frauds, Democracy, and Development.

Gabriel, A., Alese, B. K., Adetunmbi, A., & Adewale, O. S. (2013). *Post-Quantum Crystography: A combination of Post-Quantum Cryptography and Steganography.* Paper presented at the

Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for.

Gunjal, B. L., & Mali, S. N. (2012). Secure e-voting system with Biometric and Wavelet Based Watermarking Technique in Ycgcb color space.

Gunjal, B. L., & Manthalkar, R. R. (2010). *Discrete wavelet transform based strongly robust watermarking scheme for information hiding in digital images.* Paper presented at the Emerging Trends in Engineering and Technology (ICETET), 2010 3rd International Conference on.

Koluguri, A., Gouse, S., & Reddy, P. B. (2014). Text steganography methods and its tools. *International Journal of Advanced Scientific and Technical Research, 2*(4), 888-902.

Moayed, M. J., Ghani, A. A. A., & Mahmod, R. (2008). *A survey on cryptography algorithms in security of voting system approaches.* Paper presented at the Computational Sciences and Its Applications, 2008. ICCSA'08. International Conference on.

Mursi, M. F., Assassa, G. M., Abdelhafez, A. A., & Abosamra, K. M. (2015). *A secure and auditable cryptographic-based e-voting scheme.* Paper presented at the Mathematics and computers in sciences and in industry (MCSI), 2015 second international conference on.

Olaniyi, O., Arulogun, O., Omidiora, E., & Okediran, O. (2015). Enhanced stegano-cryptographic model for secure electronic voting. *Journal of Information Engineering and Applications, 5*(4).

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Oludotun, A. (2013). Design of secure electronic voting system using multifactor authentication and cryptographic Hash Functions.

Olaniyi, O. M., Folorunso, T. A., Aliyu, A., & Olugbenga, J. (2016). Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach. *International Journal of Information Engineering and Electronic Business, 8*(5), 9.

Osho, O., Yisa, V. L., & Jebutu, O. J. (2015). *E-voting in Nigeria: A survey of voters' perception of security and other trust factors.* Paper presented at the Cyberspace (CYBER-Abuja), 2015 International Conference on.

Ofori-Dwumfuo, G. and E. Paatey, *The design of an electronic voting system.* Research Journal of Information Technology, 2011. **3**(2): p. 91-98.

Pan, H., Hou, E., & Ansari, N. (2015). M-NOTE: A Multi-part ballot based E-voting system with clash attack protection. In *2015 IEEE International Conference on Communications (ICC)* (pp. 7433–7437). IEEE. https://doi.org/10.1109/ICC.2015.7249514

Peisert, S., Bishop, M., & Yasinsac, A. (2009). Vote Selling, Voter Anonymity, and Forensic Logging of Electronic Voting Machines. In *2009 42nd Hawaii International Conference on System Sciences* (pp. 1–10). IEEE. https://doi.org/10.1109/HICSS.2009.503 c

Por, L. Y., & Delina, B. (2008). *Information hiding: A new approach in text steganography.* Paper presented at the WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering.

Roy, S., & Manasmita, M. (2011). *A novel approach to format based text steganography.* Paper presented at the Proceedings of the 2011 International Conference on Communication, Computing & Security.

Rura, L., Issac, B., & Haldar, M. K. (2011). *Secure electronic voting system based on image steganography.* Paper presented at the Open Systems (ICOS), 2011 IEEE Conference on.

Santin, A.O., R.G. Costa, and C.A. Maziero, *A three-ballot-based secure electronic voting system.* IEEE Security & Privacy, 2008. **6**(3): p. 14-21.

Sparrow, R. D., Adekunle, A. A., Berry, R. J., & Farnish, R. J. (2016, April). A novel block cipher design paradigm for secured communication. In *Systems Conference (SysCon), 2016 Annual IEEE* (pp. 1-6). IEEE.

Stallings, W. (2000). *Network Security Essentials: Applications and Standards, 4/e*: Pearson Education India.

Usha, S., Kumar, G. S., & Boopathybagan, K. (2011). *A secure triple level encryption method using cryptography and steganography.* Paper presented at the Computer science and network technology (ICCSNT), 2011 international conference on.

Wolf, P., Nackerdien, R., & Tuccinardi, D. (2011). *Introducing Electronic Voting: Essential Considerations*: International Institute for Democracy and Electoral Assistance.

William, S. (1999). Cryptography and network security: principles and practice. *Prentice-Hall, Inc*, 23–50.

