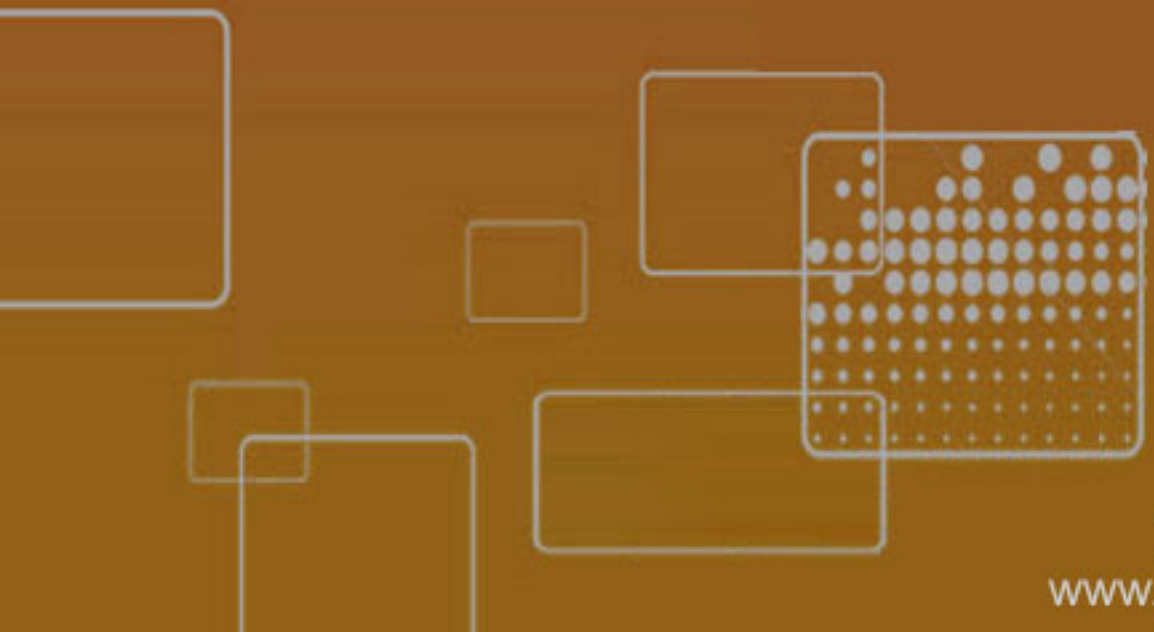
ISSN 2277-8616

International Journal of Scientific & Technology Research

e-publication, Volume 7, Issue 4
April 2018 Edition
ISSN 2277-8616



IJSTR
www.ijstr.org

Performance Assessment Of An Imperceptible And Robust Secured E-Voting Model

Olaniyi Olayemi M, Arulogun Oladiran T, Omidiora Elijah O, Okediran Oladotun O

Abstract: In this paper, we present the performance assessment of an imperceptible and robust secured stegano-cryptographic model of electronic voting. The Performance analysis was achieved based on the degree to which the model meets the generic and functional requirements of secured e-voting system: authentication, integrity, confidentiality and verifiability as well as other functional security requirements of a secured voting using five-point psychometric analysis. The result of the quantitative evaluation of the model assert that the model possessed capacity to guarantee and validate voter's for who they said they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process in developing country where digital divide is significant.

Index Terms: Steganography, Information Systems Security, E-voting, Information hiding, Authentication, Confidentiality, Integrity, Verifiability, Cryptography

1 INTRODUCTION

A vital part of every democratic process of governance is voting, as such, the security, efficiency and reliability of this decision making process is critical for peaceful resolution of the struggle of political power between the leaders and followers [18].The challenge of existing voting systems in most developing countries ranges from rigging to wide scale fraud, denial of vote re-counting and impossibility of absolute monitoring of the electoral system [6],[9],[21].This has resulted to intolerably high rate of electoral corruption and question the principle of fair democratic governance. Thus, there is the need to formulate and develop mechanisms for electronic elections which can guarantee transparency, enforces fairness and secure all phases of electioneering processes. To fulfill this objective, design and development of secure and scalable electronic voting systems has been an active research endeavor in the last decade using different Information hiding and privacy technologies. In [16], a survey of cryptographic techniques used for e-voting systems was presented. In [19], a survey of existing cryptographic and stegano-cryptographic models of secure e-voting systems for credible democratic governance and proposition was made for platform adaptable, robust and imperceptible secure e-voting model for developing countries like Nigeria. In [9], Multifactor Authentication schemes using Smart Card, Fingerprint Biometrics and Personal Identification Number (PIN) were used to provide security and convenience in e-voting system.

- *Olaniyi O.M is currently at Computer Engineering Department, Federal University of Technology, Minna, Nigeria. E-mail: mikail.olaniyi@futminna.edu.ng*
- *Arulogun O.T, Omidiora E.O and Okediran O.O are currently at Department of Computer Science and Engineering Ladoke Akintola University of Technology, Ogbomoso, Nigeria,.*
  E-mail: otarulogun@lautech.edu.ng , eoomidiora@lautech.edu.ng and oookediran@lautech.edu.ng
- *(This information is optional; change it according to your need.)*

Similar Multifactor Authentication mechanism using Visual Challenge grid mechanism, one-time personal identification short message service (OTP-SMS) and cryptographic hash functions were used to provide authentication and integrity security requirements to e-voting systems in [20].In[7], a multi layer, secure web based e-voting system was proposed using biometric and wavelet based image watermarking technique in YCgCb color space. Also, several research papers proposed reliability and confidentiality in e-voting systems by using verifiable receipts and steganography to protect the privacy and secrecy of the voters and electronic ballot in [16],[3] and [11]. In this paper, we present quantitative performance assessment of our imperceptible and robust secured model of electronic voting proposed in [19] and [21] using psychometric analysis. The current modified open ballot system of election in Nigeria was studied and secured e-voting systems using modified stegano-cryptographic schemes was designed and developed using information hiding techniques and software engineering process models. Voters of acceptable age range were then asked to use the developed secured voting system based the e-voting model. Relevant data were captured and analyzed using descriptive data analysis in Statistical Package for Social Sciences (SPSS) environment. An imperceptible and robust secured e-voting model for democratic governance has been quantitatively assessed for developing counties with the view of asserting the degree the model fulfill fundamental and social security requirements require for the conduct of free, fair, credible and genuine e-elections. The rest of the paper is organized into the following: Section 2 describes basics of Information Hiding and Privacy Technologies; Section 3 describes methodologies adopted to achieve to carry out the research; Section 4 presents the results and discussion of the model quantitative assessments and sections 5 concludes and provide the gap intended to fill the future.

2 INFORMATION HIDING AND PRIVACY TECHNOLOGIES

From literatures, the security ideals of different Information security and privacy technologies have been proved with data encryption schemes. In practice, different data cryptographic standards like Data Encryption Standard (DES), and Advanced Encryption Standard (AES), Rivest-Sharma-Adleman (RSA), have not only been adequate but are not very efficient in the encryption of large volume of digital data[1],[25][19]. This can be addressed by complementing data encryption with data

hiding. Information hiding has been used to enhance security level of data encryption systems. The main driving force of information hiding is concern over copyright; such as audio, video and other works available in digital form, the ease with which unauthorised copies can be made and the need to identify violators and prosecute them [25]. Military communications system makes increasing use information hiding. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography[17]. Steganography comes from the Greek words "*stegos*", meaning cover and "*grafia*" meaning writing which literally mean 'covered writing' is about hiding information in other information. Other Information hiding technologies include cryptography and watermarking. Cryptography is the science of transmitting scrambled data in an effort to secure communications from an eavesdropper despite his awareness of the data transmission [20]. In most cases, sending encrypted data over wireless channel may draw attention, while invisible communication will not. The combination of steganography and cryptography by data encryption can enhance the security level in communications security [10].Watermarking is an information hiding technique for protection of the copyright of digital product from digital production and data safety maintenance. Its applications range from copyright protection, telemedicine, copyright protection and in secured in e-voting systems.

3 MATERIALS AND METHODS

In this section, brief description of the model architectural design, performance assessment factors, research questions, data collection instrument, method, tools for data analysis are discussed.

3.1 MODEL ARCHITECTURAL DESIGN

The secured e-voting model presented in [18],[19] and [21] combines multi-layer data security(steganography and cryptography), multi media (Image and video), and multi-domain (Spatial and Frequency) to solve the problem of authentication, integrity, confidentiality, verifiability of secure electronic voting in pre electoral, electoral and post electoral phase of e-democratic decision making. The model shown in Figure 1, view electioneering process in three phases: The pre-election phase; the election phase and the post- election phase. This architecture provides greater application high flexibility and efficiency, since each tier runs on a separate machine to improve the system performance. The pre-election phase involves the registration of all entities that will enable the outcome of the election, such entities are: Voters information, administrators, Candidates and Parties information, which are all stored in the database. The election phase involves ballot submission of electronic vote casting and vote security, such that the vote is encrypted with the RSA encryption algorithm specifically for poll site and kiosk e-voting scenario while the ECC encryption algorithm is specifically meant for remote mobile voting scenario. The encrypted text (handled as bit) is embedded in a random multimedia graphics generated by the system using both image and video steganographic techniques and is then sent to the server. The voter's fingerprint pattern and accurate response of the voter to both dynamically generated grid questions and mobile short message service (SMS) are used to authenticate the voter to validate the identity of the voter [18]. The post-election phase is where the vote casted is extracted from the stego object and decrypted using the extraction technique of the Image and Video steganographic technique as well as and decryption definitions of appropriate cryptosystem (RSA or ECC based on voting scenario), and then final results are retrieved, collated, and processed. At this phase, electronic votes are counted and final results are retrieved and displayed for voters[19].

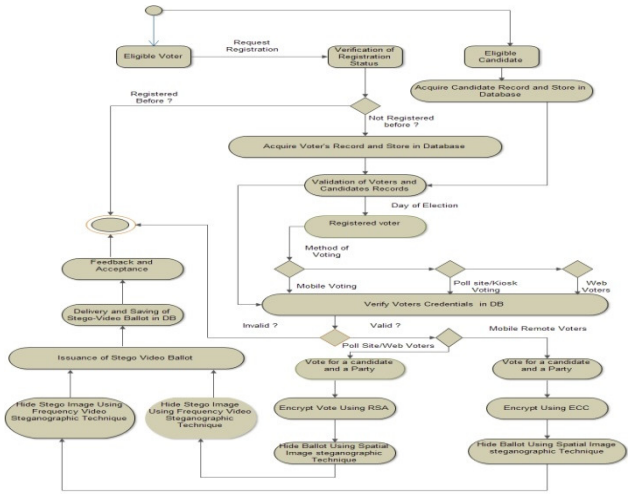


Figure 1: Stegano-Cryptographic Model of Secure E-voting (Source:[19])

3.2 PERFORMANCE ASSESSMENT FACTORS AND RESEARCH QUESTIONS

The security requirements of an e-voting system are evaluated based on the underlying voting models such as Blind signatures, Homomorphic and Mix-nets. These underlying voting models in most cases involve authority for enforcing security and orderliness in the voting process [15]**.** The authoritative models have been proved unreliable as computing power keeps increasing [11][24].When designed around cryptography; they are cryptanalytically found to be vulnerable to attacks ranging from brute force attack, timing attack, session hijacking, replay attack, known-plaintext and chosen-plain text attack [12][14] and trapdoor problem [13]. Authoritative models designed around hybrid stegano-cryptographic models attempted covert communication using only one media to hide voter's electronic ballot which can easily be manipulated by an eavesdropper. Considering these limitations of authoritative models of e-voting from the voter's end, the network and at voting system's end, the following fundamental technical security issues are pertinent:

- **i.** Could voters be verified to be who they claimed they are? i.e. Authentication issue
- **ii.** Could vote casted remain secret? i.e. Issue of confidentiality
- **iii.** Could votes remain unaltered? i.e. Issue of Integrity issue.
- **iv.** Could votes be counted and audited accurately? Issue of Non-Repudiation

Also the following social factors issues are pertinent:

- **i.** Could e-voting system developed on the model allow multiple voting? i.e. democratic issue

ii. Could e-voting system developed on the model eliminate rigging attributed to conventional voting? i.e. Issue of rigging?
iii. Could the e-voting model enhance citizen participation?
iv. Could the developed secured e-voting model drive free, fair and credible e-governance?

3.3 STUDY AREA AND SAMPLE SIZE

The study population comprises of voter's of acceptable age range within campus environment at the department of Computer Science and Engineering, LAUTECH Ogbomoso in Oyo State, Nigeria and Computer Engineering department of Federal University of Technology, Minna, Niger state Nigeria. Purposive sample technique is adopted to aid the ease of data collection of the members (users) of the sample size. The users sampled are students, lecturers and technical staffs that are eligible to vote (18 yrs and above) and electorate of current conventional voting system in Nigeria. A total of one hundred and ten (110) sample users perceptive analysis form (questionnaire) were distributed for assessment of the e-voting model after exercising pre-election process: voter's registration; election process-Voting and post election process-verifiability on the developed secured in e-voting system based on e-voting model. User's were asked to assess the developed e-voting model both for technical and social factors in section 3.2 that can significantly influence the assertion that the model possessed capacity to guarantee and validate voter's for who they said they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process.

3.4 DATA COLLECTION INSTRUMENT

A well structured user's perceptive analysis form (questionnaire) was designed to capture both technical and social factors of free, fair and credible e-voting system. The questionnaire was tested and validated for reliability using Cronbach's alpha test in SPSS environment. The interpretation of the assessment using [18] benchmark is provided for different technical and social factors in section 3.4.1

3.4.1 RELIABILITY ANALYSIS OF DATA COLLECTION INSTRUMENT

The reliability analysis using Cronbach's alpha test in SPSS environment was used to measure the internal consistency of the administered questionnaire to ensure that the research security questions reliably measure security requirement of secure e-voting system from the perception of the respondent. Author in [5] developed procedure to measure the internal consistency of the administered instrument in a survey research. Authors in [4] had proposed four different points of reliability: Excellent ranges (0.90 and above), High (0.70-0.90), High moderate (0.50-0.70) and low (0.50 and below).The findings of reliability analysis for the assessment of fundamental and functional security requirements of e-voting system developed based on the model is summarized in section 4.

3.5 METHOD AND TOOLS FOR DATA ANALYSIS

Of the one hundred and ten (110) users assessed, only one hundred and two (102) responses were received from users from the duly filled user perceptive analysis forms(questionnaires) and primary data from the duly filled questionnaires was captured, compiled and analysed using SPSS version 11.5 for Windows environment using descriptive data analysis. The descriptive survey was adopted to infer the perception of the entire population based on the opinion of a representative sample the target population. Four performance evaluation metrics which are System Degree of Voter's Verification and Validation (SD3V), System Degree of Integrity (SDI) and System Auditabillity Index (SAI) and System Confidentiality Index (SCI) were formulated to evaluate the degree of security of the model in Statistical Package for Social Sciences (SPSS). Voters express their feelings about the degree to which the developed e-voting model fulfills these technical security requirements using the following Likert linguistic (LL) values: 'Strongly Disagree (SD)', 'Disagree(D)', 'Neutral(N)', 'Agree(A)' and 'Strongly Agree(SA)'. These linguistic labels and values describe the performance of the developed e-voting model is presented in Table 1. Survey targets were set for each evaluation parameter of the develop model for secure e-voting system. These give an objective assessment of the adequacy of the system to be considered secure for driving transparent and trustworthiness in e-democratic decision making.

Table 1: Linguistic Labels and value for the developed e-voting model performance

LL	SD	D	N	A	SA
Values	1	2	3	4	5

.

4. RESULTS AND DISCUSSION

The performance assessment of the developed stegano-cryptographic e-voting model was evaluated for authentication, secrecy, confidentiality, verifiability and functional security requirements of a secured e-voting system quantitatively through perceptive assessment of these qualities by users of acceptable age range (18years and above) by administration of user perceptive form (questionnaire). The assessment form contains the established four fundamental security requirements of a secured e-voting system as well as other functional parameters such as scope for multiple registration, rigging, method of voting, technical requirements of these methods of voting, democracy, participatory effect of implementing the developed e-voting as well as of possibility of the developed model to drive a free, fair and credible secure e-democratic transition. Considering each of the elicitated security requirements in these responses, findings from the assessment of the authentication security requirement of the developed e-voting model revealed that over ninety percent (94.1%) of the respondents cumulatively agreed that the developed e-voting model could verify and validate remote voters identity for whom they claim they are. The findings of voter's secrecy and confidentiality security assessment revealed that over eighty percent (87.20%) cumulatively agreed that developed secured e-voting model could preserve the secrecy and confidentiality of the voter. The verifiability security assessment revealed that over ninety percent (93.10%) cumulatively agreed that developed secured e-voting model could allow voters to verify their electronic ballot in the tally. Functional security requirements of secured e-voting system such as tendency for multiple voting by voter was assessed and findings revealed that over seventy

(75.50%), cumulatively disagreed that the developed secure e-voting model could allow multiple voting. Other functional security requirements of secured e-voting system such as scope elimination of Rigging, Participatory Effect to e-governance and capacity for the developed secured e-voting model to drive free, fair and credible e-governance were assessed and findings revealed that over seventy (75.50%), over eighty(84.30%),over Ninety (91.20%) and Ninety percent (96.10%) respectively cumulatively agreed that the developed secure e-voting model could eliminate rigging, increase citizen participation and drive free, fair and credible e-governance in Nigeria if implemented. These fundamental and functional security requirements of e-voting system assessed are graphically depicted in the bar chart representation presented in Figure 2.

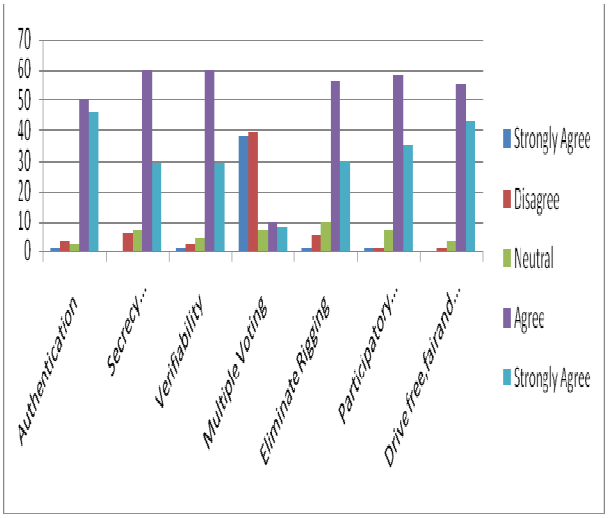


Fig 2: Results of performance assessment of technical and functional requirements of an imperceptible and robust model of secured e-voting

Table 2 depicts the summary of the performance evaluation parameters obtained for the developed secure e-voting model with the user rating surpassing the set targets for the four cases. This shows that the developed model for secured e-voting system has an appreciable attribute of secure e-voting system with high degree of integrity and remote voter's verification and validation relevant for the delivery of transparent, free, fair and credible electronic democratic decision making in the developing countries where significant digital divides exist. The system's degree of confidentiality and auditabillity are equally of appreciable index rate with capacity for increasing the voter's confidence through post electoral ballot verification and ensuring that no one can read the electronic ballot except the voting authority through the developed stegano-cryptographic technique. The respondent's rating of the secure-evoting system based on the stegano-cryptograhic technique for System Degree of Voter's Verification and Validation(SD3V),System Degree of Integrity(SDI) and System Auditability Index (SAI) are high compare to System Confidentiality Index(SCI).This was due to novelty and secretive of the underlying voting technique of the secure e-voting system. Consideration was given to this factor before setting lower response design for the evaluation of the confidentiality security requirement of the developed secure e-voting model. The bar chart representation of Figure 3 shows the performance evaluation of these four formulated parameters of secure e-voting system for the developed e-voting model. Preliminary experimental validation of the technique presented in [18] was used to establish the novelty of the developed secure e-voting model.

Table 2: Summary of Evaluation metrics for the developed secure e-voting model

Performance Evaluation Metric	Response Design Target	Number of Respondents	Response Mean
System Degree of Voter's Verification and Validation(SD3V)	>4	102	4.34
System Confidentiality Index(SCI)	>3	102	4.09
System Degree of Integrity (SDI)	>4	102	4.22
System Auditability Index(SAI)	>4	102	4.23

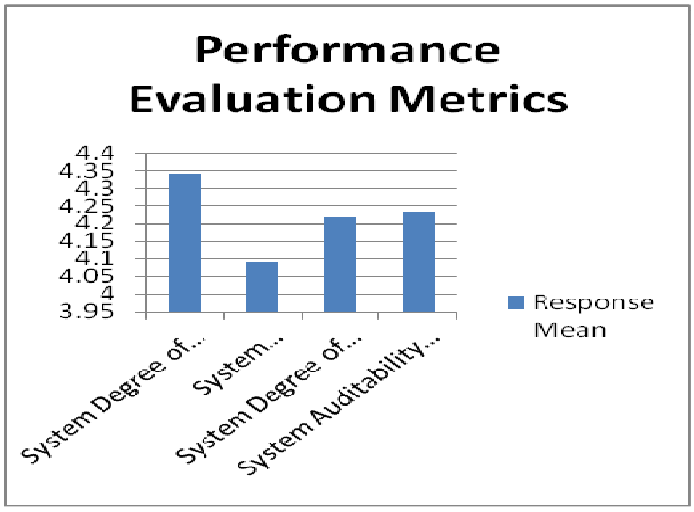


Figure 3: Graphical Representation of Performance Evaluation Metrics of the developed Secure E-voting Model in Table 2

The reliability analysis using Cronbach's alpha test in SPSS environment was used to measure the internal consistency of the administered questionnaire to ensure that the research security questions reliably measure security requirement of secure e-voting system developed around the model from the perception of the respondent. The findings of reliability analysis for the assessment of fundamental and functional security requirements of e-voting model are summarized in Table 3. The results of Cronbach's alpha test from the Table 3 were between 0.5769 in case two (core fundamental security requirements of e-voting system: authentication, confidentiality, verifiability and rigging) to 0.7012 in case three (Core fundamental security requirements of e-voting system:

authentication, confidentiality, verifiability , rigging as well as the capacity of the model to drive free, fair and credible e-governance) indicating that there is high level of internal consistency of the performance assessment of the security requirements of the developed secure e-voting model from the data obtained from the respondents.

Table 3: Reliability assessment of Security requirements of the developed secure e-voting model

Cases	Authentication	Confidentiality	Verifiability	Rigging	Participatory E-governance	Credible E-governance	Cronbach's Alpha	Hilton et al,.(2004) Interpret.
Case 1	Yes	Yes	Yes	No	No	Yes	**0.6289**	High Moderate
Case 2	Yes	Yes	Yes	No	No	No	**0.5769**	High Moderate
Case 3	Yes	Yes	Yes	Yes	No	Yes	**0.7012**	High
Case 4	Yes	Yes	Yes	Yes	Yes	Yes	**0.6318**	High Moderate

5. CONCLUSION AND FUTURE DIRECTION

This paper has successfully presented the architectural design and quantitative performance assessment of an imperceptible and robust modified stegano-cryptographic model of secured electronic voting for delivery of transparent and credible of e-democracy. The fundamental technical secured e-voting requirements of voter's authentication, vote confidentiality, vote integrity and verifiability as well as functional requirements of secure e-voting systems like scope for rigging, democracy are preferential assessment factors to impact electorate choice decision. The findings of this paper will make steganographers, software developers and government in making sound decision on what to consider in designing , developing and administration of secure e-voting systems for future free, fair and credible e-democratic decision making through e-voting. The developed secured electronic voting model in [18],[19],[20],[21] if implemented in future e-democratic decision making in developing countries will help increase the level of citizens' participation in the elections and ensure a better, faster, easier and more efficient means of voters' registration ,voting and auditing compare to existing manual method of voting. In future, further qualitative performance evaluation using several image quality metrics shall be carried out to further validate the developed e-voting model as an imperceptible and robust model whose principal strength lies in its double data layer, media and domain against any "Man-in-the-Middle" attack and eavesdropping of electronic ballot in future e-democratic dispensation in developing countries where issues of digital divide is significant.

REFERENCES

[1]. Alok K and Atul K (2011),"A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme" , International Journal of Technology And Engineering System(IJTES), Vol2.No1, pp8-11.

[2]. Amer A and El-gendy H, "Towards a Fraud prevention e-voting system", International Journal of Advanced Computer Science and Applications,Vol.4 No.4,pp147-149,2013.

[3]. Chaum D,(2004) "Secret Ballot receipts:True voter verifiable elections", IEEE Security and Privacy, Vol.2(1), pp38-47

[4]. Chang C and Lee J (2006), "An Anonymous Voting mechanism based on the key exchange Protocol", Elsevier Computer and Security Journal, Volume 25(4),pp 307-314.

[5]. Cronbach, L.J. (1951), "Coefficient alpha and the internal structure of tests", Psychometrika, Vol. 22 (3),pp 297-334

[6]. Folorunso O, Ogunseye O. S,Okesola and Olaniyan (2010),Visualizing E-Voting results, Journal of Theoretical and Applied Information Technology,16(1),pp57-69

[7]. Gunjal b.l and Mali s. n. (2012), "Secure e-voting System with Biometric and Wavelet based watermarking technique in ycgcb color space", proceedings of iet international conference on information science and control engineering 2012 (icisce 2012), pp1-6

[8]. Hinton, P., Brownlow, C., McMurvay, I., and Cozens, B. (2004). "SPSS explained" , East Sussex, England: Routledge Inc.

[9]. John, N. S, Ayo, C K, Ndujuiba C, & Okereke C. E. 2013, Design and Implementation of a Unified e-ID Card for Secure Electronic Voting System (MUSES)" , International Journal of Computer and Information Technology (IJCIT), Vol.2 No 6,pp 1131-1135.

[10]. Katiyar S, Meka K R, Barbuiya F A, and Nandi S (2011), "Online Voting System Powered by Biometric Security Using Steganography", Proceedings of The Second International Conference on Emerging Applications of Information Technology, IEEE Computer Society, pp 288-291.

[11]. Lee Y, Kim S and Won D(2008),"How to Trust DRE voting Machines Preserving Voter Privacy ",IEEE International Conference on E-Business Engineering (ICEBE),pp302-307 [12] Longe O.B, Roberts A.B.C, Onifade O.F.W, Kaka O and Isiaka R.M (2008a), "Framework for the development of a Hybrid Chaotic Image Scheme for Multimedia Data Encryption", Third International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2008), Volume III, pp150-154,21st -25th September 2011,ObafemiAwolowoUniversity,Ile-Ife, Osun State, Nigeria.

[12]. Longe O.B, Boateng R, Dada E.G, Olaniyan and Olaseni O (2010), "Stegacrypt: A Reduced Least Significant Bit Insertion Rate Carrier for Transmitting Embedded Information", The Journal of Computer Science and its Application: An International Journal of the Nigeria Computer Society (NCS),Vol.17 No1, pp1-12.

[13]. Longe, O.B.(2011), "On the use of Image-based Spam Mails as Carriers for Covert Data Transmission", Computing and Information Systems Journal, Vol. 15. Issue 1, pp1-5.

[14]. Meng B (2009), "A Secure Internet Voting Protocol Based on Non Interactive Deniable Authentication Protocol and Proof protocol that two Cipher Texts areEncryption of the Same Text", Journal Of Networks, Vol. 4(5), pp 370-377.

[15]. Moayed, M.J., A. Abdul Ghani and R. Mahmod, "A survey on Cryptography Algorithms in Security of Voting System Approaches", International Conference on Computational Sciences and Its Applications(ICCSA), 2008, pp. 190 - 200

[16]. Muhalim M A, Subariah I, Mazleena S and Mohd R k(2003), "Information Hiding Using Steganography",Faculty of Computer System and Information System, Department of Computer Science Available at http://eprints.utm.my/4339/1/71847.pdf

[17]. Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O, "Performance Evaluation of modified Stegano-Cryptographic model for Secured E-Voting", 2014, International Journal of Multidisciplinary in Cryptology and Information Security(IJMCIS),Vol.3 No.1,pp 1 -8.

[18]. Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O, "A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System", 2013, Covenant Journal of Informatics and Communication Technology (CJICT),Vol. 1 No 2, pp 54-78.

[19]. Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Adeoye O Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions" , 2013, International Journal of Computer and Information Technology (IJCIT),Vol.2 No 6,pp 1122-[21] Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. (2012), " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach ", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89.

[20]. Rura L, Isaac B, and Haldar M K, (2011), "Secure Electronic Voting System Based on Image Steganography", Proceedings of IEEE Conference on Open systems (ICOS2011), pp 80-85

[21]. Si H and Li C(2005), "Maintaining Information Security in E-Government through Steganology" ,Available at URL: www.igi-global.com/chapter/encyclopedia-digital-government/11652.pdf

[22]. Wang, X, Feng, D,Lai, X, and Yu H(2004). "Collisions for Hash Functions MD4, MD5,HAVAL-128 and RIPEMD", Cryptology ePrint Archive, Report 2004/199.http://eprint.iacr.org/2004/199.pdf

[23]. Yang M, Trifas M, FranciaG, Chen L(2009), " Cryptographic and Steganographic approaches to Ensure Multimedia Information Security and Privacy", International Journal of Information Security and Privacy, Vol.3(3), pp 37-54.