Vol 5. No. 6. Dec 2012 ISSN 2006-1781
African Journal of Computing & ICT

www.ajocict.net

Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting

[1]Olaniyi, O.M, [2]Arulogun O. T. and [3]Omidiora E.O,
[1]Department of Computer Engineering
Federal University of Technology, Minna , Nigeria.
[2&3]Department of Computer Science and Engineering
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
mikail.olaniyi@futminna.edu.ng, arulogundiran@gmail.com and eoomidiora@lautech.edu.ng

ABSTRACT
The widespread adoption of Information and Communication Technologies in governance over the years by electronic government has influenced democratic decision making through electronic voting (e-voting).E-voting provides increased participation of populace, reduced cost, decreased cases of invalid votes and support basis of democracy. However, e-voting systems are generally prone to security risks ranging from unauthorized casting of votes; Impersonation of voters by an attacker; Electronic ballot stuffing; Attack due to Denial of Service (DoS) and Distributed Denial of Service (DDOS) to the voting channel; Modification of vote and Deletion of valid votes. We present architecture for the development of an improved Stegano-Cryptographic model for electronic voting. The successful implementation and evaluation of the model will permit the government agency to know their degree of preparedness to organize free, fair and credible elections in future electronic democratic dispensation.

Keywords- E-voting System, Steganography, Cryptography, Biometrics, Security.

1. INTRODUCTION

The power of opinion expression capabilities and trustworthy elections is the bedrock of democratic societies. Election, the gateway of confidential democratic governance, is the fundamental instrument and most acceptable means around which people convey their views to their government by democratic process [1].The democratic process rests on a fair, universally accessible voting system through which all citizens can easily and accurately cast a vote [4]. Voting, an indispensable feature of democracy is a method by which a group of people express their opinion over who will lead them for a specific period of time via electoral process. Usually correctness, robustness to fraudulent behaviors, coherence, consistency, security and transparency of voting are all key requirements for the integrity of an election process [24].

Traditionally, the process of voting is not only cumbersome as the voters are expected to vote in person, the cost and process of manual voting are increasing geometrically and tedious to execute [17]. This has resulted into declining participation rate due to inconvenience of current classical/manual system of voting like inaccuracy in ballot counting and delayed announcement of election results [18]; Loss of significant time during ballot counting [3]; Unacceptable percentages of lost, stolen and miscounted ballot papers, votes loss through unclear or invalid ballot marks and limited accommodations for people with disabilities [2]; Under-age voting, counting error, complicity of the security agencies and absence or late arrival of election materials[24][36].

Nowadays, the development and widespread use of Information and Communication Technologies (ICT) is linked to the proper execution of democratic rights and thus, ICT is changing democratic decision making through electronic democracy(e-democracy).E-democracy has become a necessity in the era of Computing and Information Technology. Electronic voting (E- voting) as one of the paramount pillars of e-democracy is the use of computerized voting equipment to cast and tabulate ballots in a trustable manner [6]. Electronic systems are used to register voters, count ballots and record votes [38].E-voting can be identified in six ways [15]: Poll site Direct Recording Electronic (DRE) voting, remote Internet based voting, Optical Scanning Systems, Voter Verified Audit Trail (VVAT), Voting Kiosk, and Non-Internet Remote Voting.

Remote electronic system of voting offers multiple advantages compare to traditional paper-based voting with the following[41;24;36] :1)Increased participation in democratic governance as more citizens have access to express their opinion;2)Reduced costs as the materials required for printing and distributing ballots as well as the manpower required to govern poll sites are considerably reduced;3)Flexible as it can be tailored to support multiple languages and permit up-to-date minute ballot modifications.4)Greater speed and accuracy in placing and tallying votes as e-voting step by step processes help minimize the number of miscast and rejected votes;5)Lower election fraud in endangered countries with young democracies;6)Deliver voting results reliably and more quickly.

According to literature, the design of secure voting system must satisfy a number of competing criteria [35][36][34][19]. These requirements give an avenue for a free, fair, credible and confidential election. These requirements by [36] are grouped into generic and system specific; by [19] as functional and non-functional requirements. Considering e-voting from generic point of view, the following requirements are necessary: a) ***Security***: Votes should not be manipulated during the whole process of voting; b) ***Confidentiality***: No one should access any information about the voter's vote so as not to be able to alter it; ***Privacy***: No one should be able to link the voter to this vote after casting a vote. c.) ***Authenticity***: Only eligible voters can cast their votes. d.) ***Integrity/accuracy***: Votes cast cannot be altered by an attacker. All valid votes must be counted, whereas all invalid votes must not be discarded; e) ***Convenience***: Voters should be able to cast votes quickly with minimal equipment or skills; f.)***Democracy***: Permits only eligible voters to vote only once; g) ***Verifiability:*** Voting systems should be verified so as to have confidence that they meet necessary criteria.

In other for above ideals of genuine election to provide confidence and enable a peaceful resolution of the struggle for political power between the leaders and followers in democratic governance; all aspects of elections process must be directly observable by the candidates, the official observers and the people themselves. For people to be directly observable; transparency, integrity of electoral process, security of lives and the process of elections must be fair and guaranteed. Therefore, for e-voting system too bridge gap created by classical traditional method of conducting genuine elections, a list of security requirements that constitutes a must for voting must be observed. Without these requirements, rigging, fraud and corruption in electoral process will occur. These fundamental requirements include: confidentiality, integrity, authentication and verifiability/non-repudiation [1][18].

This paper presents the application of steganography and cryptography to the design and development of an improved stegano-cryptographically model for secure electronic voting. The model is proposed for secure remote electronic voting system with the view of increasing participation, confidence and trustworthiness in electronic democracy, protects voter's against intimidation, provide sufficient evidence to convince the electorate to vote, convince the losing candidate that he actually lost as a result of conducted, free, fair, credible and genuine elections.

2. RELATED WORKS

There are quite a few literatures which exist in the area of security in electronic voting systems. The framework for mobile multilingual e-voting system on which the security measure in [21] and [40] may be built was proposed in [37]. Due to the problems of the existing manual voting system in most developing nations, this framework was introduced. The multilingual framework enables citizen to choose the language they best understand which will increase the turnout of voters as communication barriers will be broken.

Although, voters turnout will increase based on this proposed framework, security of vote over the wireless channel is not guaranteed and as a result the integrity of votes can be compromised. Similar reference framework was proposed in [41] with the view that secure voting protocols can only fulfill their objectives to electronic voting systems with the cooperation of voting authorities termed as O***rganizations***; ***Data*** in the form of digital certificates and electronic ballot paper; ***Functions*** in the name of the core algorithms for vote encoding and decoding, signature algorithms and anonymous channels of transmission and ***Digital Infrastructure*** in form of Computer Hardware and Software. Design tasks and security analysis of electronic voting systems have to take account these important elements.

According to [40], there is a great need for e-voting and security in e-voting systems. There is necessity to implement an additional layer of security technology to tackle the risks posed by electronic voting and ensure security requirements such as voters' privacy and vote integrity. Different mechanisms to ensure security of voting systems such as: Personal Identification Number or password, encryption, digital signature, smart cards and biometric identifiers were proposed. The design of secure electronic voting system according to literature must satisfy a number of security competing criteria [35][36][34][19].

These security requirements give an avenue for a free, fair, credible and confidential election. Existing secure models for e-voting relies on the technology of cryptography by encryption. These models can be classified into authoritative and non-authoritative models [28]. The non authoritative model like [13] is fewer while the authoritative models can be categorized by different technologies into three schemes. These schemes are Homomorphic scheme such as [5,30,31,10]; the blind signature such as [9,43,7,16,50]; and the mix net scheme such as [32,27,45] .

However, these encryption algorithms have not only been proved unreliable as computing power keeps increasing [42][44], they have been crypt- analytically found to be vulnerable to attacks ranging from brute force attack, timing attack, session hijacking replay attack , cipher-text-only, known-plaintext, chosen-plain text attack a, chosen-plain text and trapdoor problem[23][21]. Moreover usage of cryptography alone for the transmission of votes over insecure wireless medium through remote internet voting would undoubtedly threaten the integrity of democratic elections as attention of adversaries are drawn to access and attack the data being transmitted. Since secure e-voting system must embrace secrecy of vote, combining the merit of multimedia data security obtainable from essentials features of encryption schemes by cryptography with steganography can play a major role in shielding the vote casted by remote voters in cyberspace to secure the privacy, confidentiality and integrity of electronic voting.

Related works in literature in application of stegano-cryptographic modelling from generic point of view to security issue electronic voting domain exist. In [26], both techniques were integrated into a multi-layer data security model of secret communication. The model cryptographic process was carried out using symmetric block ciphers with linear algebraic equation for message encryption while the steganographic process embedded the block cipher text obtained from cryptographic process into the cover image to produce stego image using Least Significant Bit (LSB) Image domain, Image Steganography. The result of simulations of the resultant bitmap based Stego-image using Matlab shows a promising result with a significant difference of the Peak Signal to Noise Ratio (PSNR) and Signal to Noise Ratio (SNR) of the stego image and the original image.

However, [26] steganographic process was carried out in image domain using LSB steganography on bitmap format (the Leena Image) which have low robustness against statistical attack from statistical steganalyst and low robustness against image manipulation which might destroy the hidden message from its destination[29].Also, LSB steganography on bitmap format is generally suitable for application where focus is only on the amount of information to be transmitted and not on the secrecy of the transmitted information due to above deficiency defeating the efficiency of the [26] crypto –steganographic model.
Biometric online voting scheme based on Stegano-cryptographic modeling technique was proposed to the problem of authentication requirement of a voting system [48]. The scheme uses the principle of LSB based Image steganography as cover object and secret key generated through cryptographic hash function for the scheme cryptography. The scheme is based in the assumption that the voter's biometric fingerprint information, personal Identification Number and account creation of the vote are securely generated, collected and available online for election. The performance of the algorithm was analyzed and the result revealed that the scheme does not give any chance to steganalytic tools to search and predict set of modification of attack. In [49], a secured electronic voting system was proposed using the Stegano-Cryptographic modeling technique. The system was implemented around the principles of secret ballot theory, image steganography, visual cryptography and threshold decryption cryptosystems in Java.

The author's proposed system provided a secure voting mechanism to the basic requirements of a secure voting system as well as non-functional requirements like uncoercibility, receipt-freeness and universal verifiability by experimentation with two different steganographic tools, F5 and Outguess on five different types of images. The results of the experimentation show that slight changes exist between original images and stego images after secret message is embedded. Our proposition is premised along the exploration of multi layer: steganographic and cryptographic techniques of data security and multimedia: Image and video approach to the problem of authentication, integrity, confidentiality, non-repudiation to the problem of electronic voting for electronic democracy in developing countries.

3. CRYPTOGRAPHY AND CRYPTOGRAPHIC MODELS FOR E-VOTING SYSTEMS

Cryptography is the science of securing data communication in the presence of an adversary. By cryptography sensitive information can be stored and transmitted across insecure networks in manner such that unintended antagonist cannot read the information except the intended recipient [39]. Cryptographic objectives encompass using mathematical techniques to all aspect of Information security from confidentiality, entity authentication and origin authentication and data integrity [14]. Usually Party A, the sender, sends secret message to Party B, the intended receiver, over a communication line which may be tapped by an adversary [17].

3.1 Components of Cryptography

Cryptography encompasses many problems including authentication, encryption, key distribution, and decryption. The traditional solution to these problems achieved through Private key Encryption (PKE). PKE involves the meeting and agreement of Party A and Party B on a pair of encryption and decryption algorithms Ɛ and D as well as common secret S, called Key, prior to remote transmission of sensitive information. The adversary may have the knowledge of Ɛ and D but does not know S. After the prior meeting, Party A encrypts message m by computing the ciphertext c=Ɛ(S,m) and sends c to B. Upon reception of an encrypted message c, Party B decrypts c by computing m=D(S,c).The adversary who does not know S should not be able to determine message m from cipher text c [38;48].This is illustrated in the Figure 1

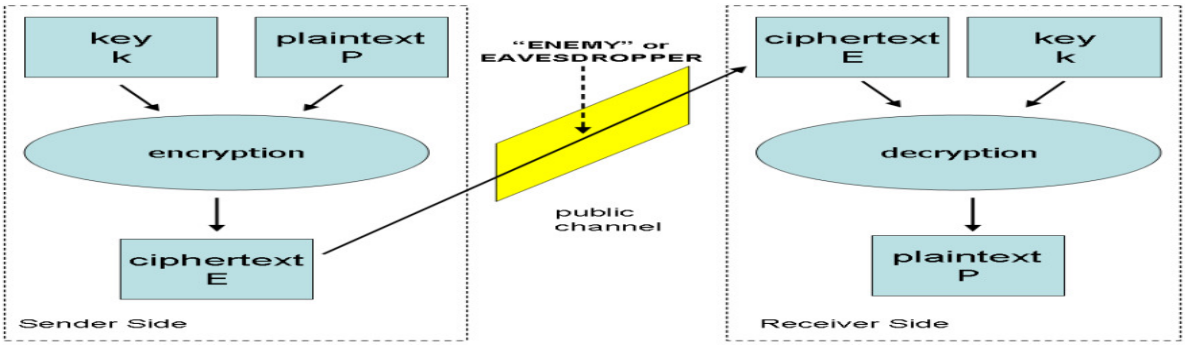

Fig 1: Symmetric-Key Cryptographic model (Source [14])

In secure e-voting domain, after first cryptographic models for electronic elections was published [10][13][5] several schemes have been proposed in literature to deal with the security problems in electronic voting. In [34][1], four proposed generic cryptographic models for secure electronic voting were compared amongst their core properties of universal verifiability, support for write-in ballot, efficient voting, efficient tallying and large scale election support were carried out. Findings of comparisons in [34][1] was that blind signature model is the most efficient cryptographic model for secure electronic voting as it supports more core properties desirable for secure e-voting. General framework of Cryptographic model to secure electronic voting system is shown in Figure 2:

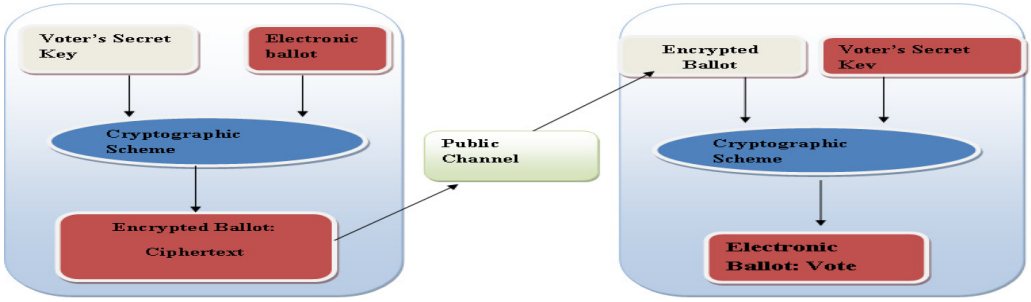

Figure 2: General Framework Cryptographic Model to Secure E-voting

3.2 STEGANOGRAPHY AND STEGANOGRAPHIC MODELS FOR E-VOTING SYSTEMS

Steganography is the science of concealing digital information within electronic files like image, sound, an article, a shopping list such that no-one determines that the hidden communication is taking place [30][22]. The technique secure data by obscuring and embedding the content in another media called carrier in which the information is saved for transmission. The technique of data security by simple encryption is not sufficient anymore as technology of Super Information Highway evolves. An encrypted data could easily be suspicious.[49].Compare to cryptography which focuses on keeping the contents of message secret by scrambling messages so it cannot be understood though its existence may be detected, Steganography focuses on keeping the existence of message secret by striving to hide the presence of the message itself from an observer so there is no knowledge of the existence of the message in the first place [22].Both technologies can be combined to produce better protection of the information [46].

The modern formulation of steganography to an application area is given in terms of prisoners' problem in which Alice (the sender) and Bob (the receiver), the two inmates wishes to communicate to formulate an escape plan without the knowledge of wendy, the prison warden. Supposing Alice sends secret message M to Bob using steganophic process, he chooses a cover medium which can be image, video and audio C. The steganographic algorithm employed as shown in figure 3 identifies C's redundant bit and embed it to a chosen media, for instance image, to create a Stego Image, S, by replacing these redundant bit with data from Message M. The Stego image S is transmitted over insecure wireless link under the monitoring of Wendy to the receiver Bob only if Wendy has no suspicion of it [14]. The process of embedding the privilege data for transmission in public channel represents a critical task for steganographic system because the stego Image S must be as similar as possible to the chosen cover media for the avoidance of the eavesdropper.

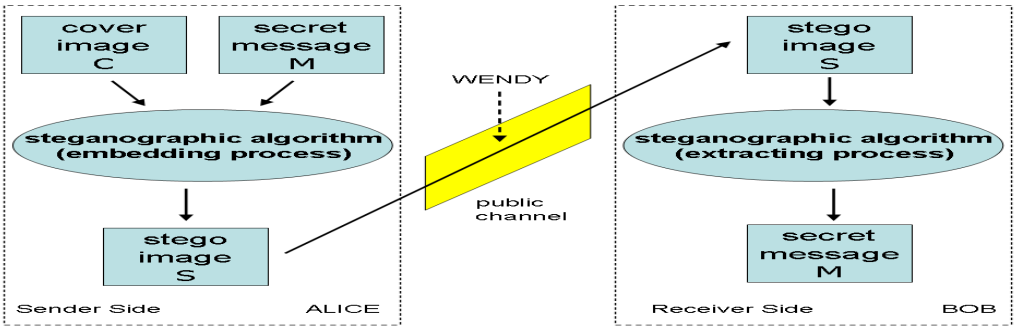

Figure 3: General Steganographic Model (Source from [14])

In secure e-voting domain, the steganographic message consists of the secret message, the electronic ballot, the cover data and the stego message. The secret message is the part of the message intended to be hidden, the cover data refers to the container for hiding the secret message and the stego message is the final product of steganography. The general framework for steganography to electronic voting is shown in Figure 4:

Some of the techniques used in steganography are domain tools such as Least Significant Bit (LSB) insertion, noise manipulation, and transform domain that involve manipulation algorithms and image transformation such as discrete cosine transformation and wavelet transformation. However there are techniques that share the characteristic of both of the image and domain tools such as patchwork, pattern block encoding, spread spectrum methods and masking [49].

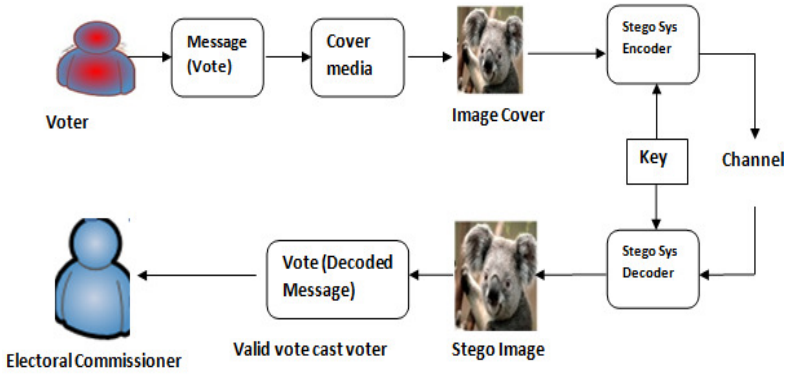

Figure 4: General framework of Steganography to E-voting (Adapted from [22])

4.0 STEGANO-CRYPTOGRAPHIC MODELLING TECHNIQUE

Stegano-Cryptographic modeling technique involves the combination of the two principal Information Security Technologies-Cryptography and Steganography to the problem of security in an application area. Considering Figure 3 and Figure 4, features peculiar to both information security techniques unify into this model called Stegano-cryptographic model or stego-cryptographic model shown in Figure 5. This new relationship exists as result of mapping between the plaintext P and Message M, Cipher Text E and Stego Media S and Cryptographic Key K and the Stego Key K.

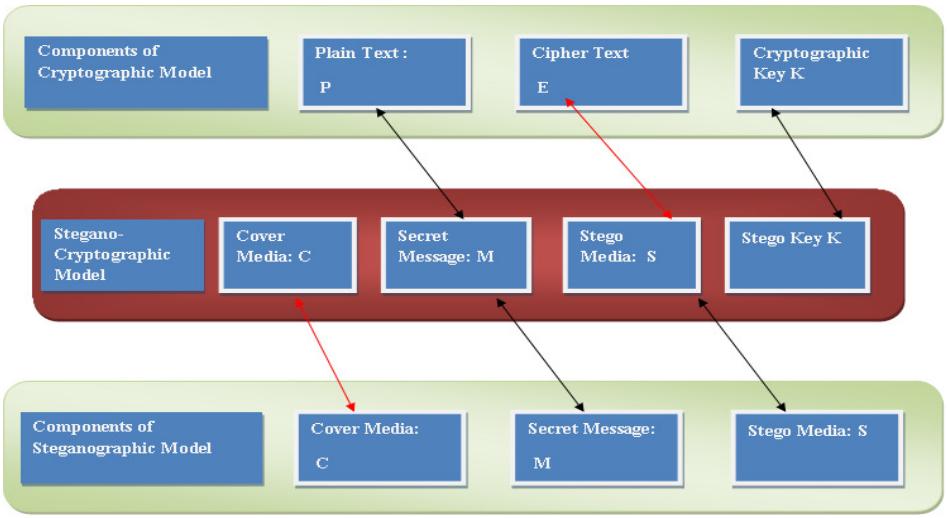

Figure 5: General Stegano-Cryptographic Model Mapping from Steganography and Cryptography (Adapted from [14])

The stegano-cryptographic model results as a hybrid model with the addition of a new element: the Stego key K, giving the unifying model the cryptographic functionality while preserving the desired steganographic attributes. The hybrid model embedding process yields Stego Media S exploiting not only Cover Media C's bits but also K's ones as shown in Figure 6.Therefore by Figure 6, Alice (the sender) will have the privilege to embed the secret message M (that is, the plaintext) into the Cover media C (through steganographic process) encrypting Message M by the Cryptographic key K (Through cryptographic process) simultaneously. At the receiver side, Bob will be able to recover Secret Message *M* through Stego Media *S* and Stego *K*. In addition, Wendy will neither detect that Secret Messsage *M* is embedded in Stego Media *S* nor be able to access the content of the secret message M [14].Figure 6 shows a classical example for an image based Stegano-Cryptographic Model:

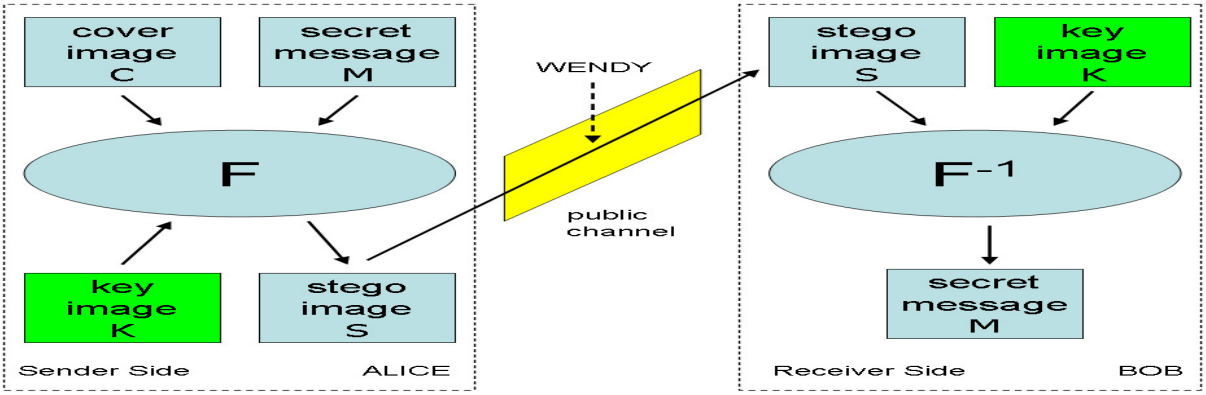

Figure 6: General Framework of Image Based Stegano- Cryptographic model (Source [14])

In secure electronic voting application, the voter's electronic intent, vote is first encrypted using an encryption algorithm. The encrypted message is then embedded into a stego media which can be image, video and audio depending on the steganographic technique using a stego-key. The stego media is then sent through a communication channel.

The secret key is used to extract the hidden message from the stego media using the decryption algorithm. For instance in image steganographic application, the integrity of a voter and his vote is assured with the encryption of the message (vote) and then embedding of the encrypted message inside a 24-bit cover image. A secret key used for the stego-system encoder is then passed through the communication channel. At the voters administrator end, the secret key is used to extract the hidden message from the stego-image as shown in Figure 7.

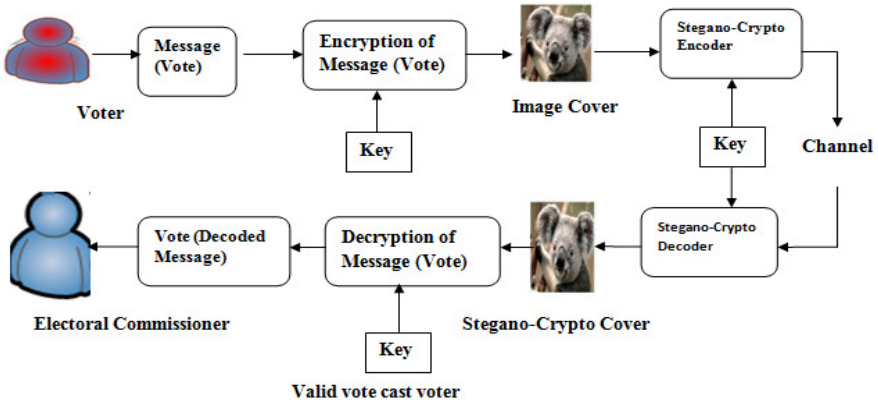

Figure 7: Stegano-Cryptographic Modeling Technique in Secure E-voting.

5. RESEARCH DIRECTION

In this research, our aim is to develop a robust multi layer (steganography and cryptography) data security, multi domain (Image, video and/ or audio) model to the problem of fundamental security issues of authentication, integrity, confidentiality and non-repudiation requirements of secured electronic voting system.

To achieve this, a study of the underlying principles of various cryptographic models for e-voting like Blind Signature, Homomorphic, Mix-net and verifiable secret sharing ; various underlying Cryptosystems like RSA Cipher and ECC Cipher and various techniques of image and voice steganography will be carried out. The performance analysis of the final multi-layer, multi domain model will be carried on an electronic voting system to reveal its vulnerability to fundamental security issues of authentication, integrity, confidentiality and non-repudiation requirements in secured e-voting system. The architecture of our proposed model is shown in figure 8:

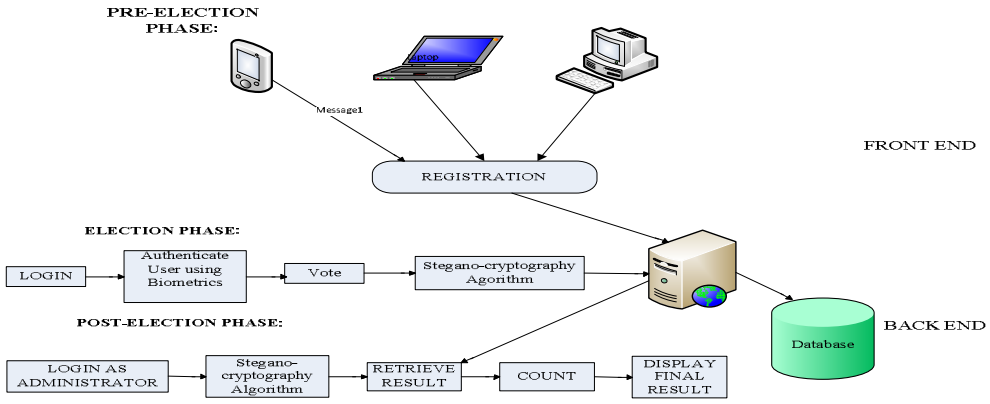

Figure 8: Architecture of the proposed model of Secured E-Voting System

The architecture chosen for the proposed model is client--server architecture based on three-tier architecture. A three-tier is a client–server architecture in which the presentation, the application processing, and the data management are logically separate processes. The model will be simulated using Java Programming Language and Oracle Database Management System. The model will be evaluated to verify and ascertain its stability against established fundamental security requirements of secured e-voting system.

6. CONCLUSION

Proper administration of elections is central to democracy. The electronic administration of elections by electronic voting must provide a list of security requirements for fair and transparent democratic decision making. Without these requirements, rigging, fraud and corruption in electoral process will occur. The proposed architecture of an improved stegano-cryptographic secured model for e-voting turns attention to data hiding techniques in steganography and cryptography in building stronger scheme that combines the strength of both information security and privacy technologies.

The model will evaluate security issues on electronic voting and predict the performance of stegano-cryptographic secured electronic voting system for future electronic democracy. Our research agenda is premised towards the development of a robust security model for electronic voting using principles of Biometrics, Steganography and Cryptography. The improved stegano-cryptographically model will verify voters as who they claimed they are, prevent fraud in form of addition and deletion of ballot (vote) over an insecure wireless networks, protect voters privacy, ensures confidentiality and uncoercibility which are essential to security requirements of remote electronic voting systems. The outcome will be a benchmark for relevant government electoral agency (like INEC in Nigeria) to know their degree of preparedness to envisage performance metrics require to organize free, fair and credible elections in future democratic dispensation. At this stage, the research is open to suggestions and criticisms.

REFERENCES

[1]Abo-Rizka M and Ghounam H.R(2007), A Novel in E-voting in Egypt, International Journal of Computer Science and Network Security ,Vol.7,No.11,pp226-234.

[2]Ayannuga O.O and Folorunso O (2010), Electronic Voter's Authentication Management System (eVams), Proceedings of 23rd National Conference of Nigeria Computer Society July 26th -30 th 2010,Volume 21,pp105-110.

[3]Akinyede R.O (2010), Nigerian Voting System: Present and Future States, Proceedings of 23rd National Conference of Nigeria Computer Society July 26th -30 th, Volume 21,pp77-81.

[4]Bannet J, Price D.W, Rudys A, Singer J and Wallach S.D(2004), Hack-a-vote: Security Issues with Electronic Voting Systems, IEEE Security and Privacy-IEEE Computer Society available at http://www.computer.org/security/

[5]Benaloh, J. (1987),"Verifiable Secret Elections", PhD Thesis,Yale University, New Haven.

[6]Cetinkaya ,O and Koc, M,L(2009),Practical Aspects of DynaVote E-voting Protocol,Electronic Journal of E-Government, Volume 7Issue 4,pp327-338.

[7]Cranor, L.R. and Cytron, R.K. (1996) "Design and Implementation of a Practical Security-Conscious Electronic Polling System,", Washington University: Computer Science Technical Report.

[8] Ciprian Stănică-Ezeanu (2008), "E-Voting Security", Buletinul Universităţii Petrol – Gaze din Ploieşti, Vol. LX (2), pp 93-97.

[9] Chung-Ta L and Min Shang H (2012)," Security Enhancement of Chang-Lee Anonymous E-voting Scheme", International Journal of Smart Home,Vol.6 No2,pp45-52.

[10]Chaum D. (1981), "Untraceable electronic mail return addresses and digital psedonymns", Communications of the ACM, Vol 24(2) ,pp84-86.

[11]Chaum D. (1983),"Blind Signatures for untraceable payments", In Proceedings of Cryptology, pp:199-203, Plenum Press, NewYork.

[12] Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa(1993),"Efficient anonymous channel and all/nothing election scheme," In *Proceeding of Advances Cryptology - EUROCRYPT'93*, pp.248–259, 1993.

[13]DeMillo, R. A., Lynch, N. A. M. Merritt,(1982) "Cryptographic Protocols," In *Proceeding of 14th Annual ACM Symposium on Theory of Computing*, pp.383-400.

[14]Domenico B. and Luca I. (2007), "Image Based Steganography and Cryptography" Institute for Systems and Technologies of Information, Control and Communication , pp 127-134.

[15]Enguehard C (2008),Transparency in Electronic Voting: The Great Challenge, Proceeding of International Political Association(IPSA) Conference on E-democracy-State of the art and future agenda, Stellenbosch University, South Africa,22-28 January,2008.

[16]Fujioka A., Okamoto T., and Ohta K.(1992), "A Practical Secret Voting Scheme for Large Scale Elections. In Advances in Cryptology , AUSCRYPT '92, pp. 244-251.

[17]Goldwasser S and Bellare M(2001),"Lecture Notes on Cryptography", MIT, Cambridge.

[18]Ibrahim S, Kamat M, Salleh M, and Abdul Aziz S (2003), Secure voting using blind signature *available at URL http://eprints.utm.my/3262/1/IEEE02-EVS_full_paper_ver14Nov.pdf* Retrieved on November17th 2011.

[19]Kalaichevi V and Chandrasekaran R.M (2011),Secured Single Transcation E-Voting Protocol: Design and Implementation, European Journal of Scientific Research,Vol 51 No2,pp276-284.

[20] Lambrinoudakis C, Gritzallis D, Tsoumas V, Karyda M and Ikonomopulos (2003), Secure- Electronic Voting : The Current Landscape, Advances in Information Security, Volume 7,No 2,pp 101-122 Available at http://www.springerlink.com/content/j4402372h6256372.pdf

[21] Longe O.B., Boateng R., Dada E.G., Olaniyan O. and Olaseni O. (2010), "Stegacrypt: A Reduced Least Significant Bit Insertion Rate Carrier for Transmitting Embedded Information", Journal of Computer Science and Its Applications, Vol. 17(1), pp 1 – 11.

[22]Longe, O.B. (2011c). 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.

[23]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,3rd International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2008), Volume III, pp150-154, 21st -25th September 2011, Obafemi Awolowo University,Ile-Ife, Osun State, Nigeria.

[24] Manish K, Suresh K.T, Hanumanthappa. M, Evangelin G.D,(2005), Secure Mobile Based Voting System, Retrieved online at http:// www.iceg.net/2008/books/2/35_324_350.pdf on November17th 2011.

[25]Malkawi M, Khasaweh M K., and Al-Jarrah O, (2009), ”Modelling and Simulation of a Robust E-voting System”, Communication of Information Management Association(IBIMA) Journal, Volume 8, pp 198-206.

[26]Mallick P K and Kamilla (2011),Crypto Steganography Using linear Equation, International Journal of Computer and Communication Technology, Volume 2 Issue8,pp106-112.

[27]Markus M , and Patrick H,(1996) “Some remarks on a receipt-free and universally verifiable mix-type voting scheme,” In *Proceedings of ASIACRYPT ’96*, LNCS 1163,pp.125–132,1996.

[28]Meng B (2009), “A Secure Internet Voting Protocol Based on Non Interactive Deniable Authentication Protocol and Proof protocol that two Cipher Texts are Encryption of the Same Text”, Journal Of Networks, Vol. 4(5), pp370-377.

[29]Morkel T,Eloff J.H.P and Olivier M.S(2010),”An overview of Image steganography”, Department of Computer Science,University of Pretoria,South Africa.Retrived online at http http://martinolivier.com/open/stegoverview.pdf on 4th June 2012

[30]Popa R, (1998) ,”An Analysis of Steganographic System”, The "Politechnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.

[31] Ronald C, Matthew K.,Franklin, Berry S, and Moti Y(1996), Multi-authority Secret-ballot elections with linear work, In Advances in Cryptology, EUROCRYPT '96, v ol.1070 of LNCS, pp.72-83.Springer-Verlag,

[32]Ronald C, Rosario G, and Berry Schoenmakers (1997), ” A Secure and optimally efficient multi-authority election Scheme”. In advances in Cryptology-Eurocrypt 97,pp 103-118,Springer Verlag,LNCS.

[33] Kazue S and Joe K,(1995),“Receipt-free mix-type voting scheme,” In *Proceeding of EUROCRYPT ’95*, LNCS 921,pp.393–403

[34]NSF (2001),” Report on the National Workshop on Internet Voting: Issues and Research Agenda” , National Science Foundation, Retrieved at http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

[35] Okediran O. O, Omidiora E.O, Olabiyisi S.O, and Ganiyu R A (2011),” A Comparative Study of Generic Cryptographic models for Secure Electronic Voting”, British Journals of Science Vol1No2, pp 135-142.

[36] Okediran O. O, Omidiora E.O, Olabiyisi S.O, Ganiyu R A and Alo OO(2011),” A framework for a Multifaceted Electronic Voting System, International Journal of Applied Sciences,USA,Vol1 No4, pp 135-142.

[37] Olaniyi, O.M, Adewumi D.O, Oluwatosin E.A, Arulogun, O. T and Bashorun M.A (2011),” Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance” .African Journal of Computing and ICTs, Vol. 4, No. 3. Issue 2, pp 23 – 32.

[38] Olaniyan O.M, Mapayi T, Adejumo S.A (2011), “A Proposed Multiple Scan Biometric-Based System for Electronic Voting” , African Journal of Computing and ICT September 2011, Vol. 4(2), pp 9 – 16.

[39] PGP Corporation (2003),”An Introduction to Cryptography”, PGP Corporation, USA.

[40] Sonja H. (2004), “E-Voting and Biometric Systems?” Proceedings of the first international workshop, “Electronic Voting in Europe: Technology, Law, Politics and Society”, 2nd- 4th July 2004, Beautiful Castle Hofen, Europe, pp 63-72.

[41] Schryen G, (2004),”Security Aspects of Internet Voting”, Proceeding of 37th Annual Hawaii International Conference on System Sciences(HICSS ‘04),Volume 5,pp. 50-61.

[42] Si H and Li C(2005),Maintaining Information Security in E-Government through Steganology, *available at URLwww.igi-global.com/chapter/encyclopedia-digital-government/11652.pdf*

[43]Sujata M and Banshidhar M(2010),”A Secure Multi authority Electronic Voting Protocol based on Blind Signature”,Proceeding of the IEEE International Conference on Advances in Computer Engineering,pp 271-273.

[44] 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

[45]Emmanouil M, Mike B, and Vassilios C(2001), “Receipt-freeness in large-scale elections without untappable channels,” In *Proceeding of I3E*,pp.683–694,2001.

[46]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 Tehnology,IEEE Computer Society,pp 288-291.

[47]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), IEEE,September 25-28,2011,Langwi,Malaysia.

[48]Hoffstein J,Pipher J and Sivermann J(2008),”An Introduction to Mathematical Cryptography”, Springer,USA.

[49]Muhalim M A, Subariah I, Mazleena S and Mohd R K (2003),"Information HidingUsing Steagnography",Faculty of Computer System and Information System, Department of Computer Science and Communication ,Universiti Technologi Malaysia

[50] Wen-Sheng J, Chin-Laung L, and Pei-Ling Y,(2002), "A verifiable multi-authorities secret elections allowing abstaining from voting", Computer Journal 45(6),pp.672-682.

Authors' Brief

Olaniyi O. Mikail is a Lecturer in the Department of Computer Engineering, Federal University of Technology, and Minna, Niger State. He had his First Degree in Computer Engineering at the Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria and M.Sc. Degree in Electronic and Computer Engineering at Lagos State University, Lagos. He is currently a doctoral student at the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He is a member of International Association of Engineers and Computer Scientists and Registered with the Council of Regulation of Engineering in Nigeria. He has published in reputable journals and learned conferences. His areas of research includes: Intelligent Systems, Computer Security, E-Governance, and Telemedicine. He can be reached on the cyberspace at engrolaniyi09@yahoo.com & Http://www.olaniyimikail.webs.com.

Arulogun O. T. is a Senior Lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He is currently a visiting scholar at Hasso-Plattner Institute, Potsdam, Germany. He has published in reputable journals and learned conferences. His research interests include networks security, mobile IPv6, wireless sensor network and its applications. He belongs to the following Professional bodies: Computer Professionals (Registration) Council of Nigeria; Registered Engineer, COREN and International Electrical/Electronic Engineers (IEEE). He can be reached on the cyberspace at otarulogun@lautech.edu.ng

Omidiora E. O. is currently a Reader in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Sc. Computer Engineering from Obafemi Awolowo University, Ile-Ife, Nigeria. He bagged M.Sc. Computer Science from University of Lagos, Nigeria and Ph.D Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He has published in reputable journals and learned conferences. His research interests include: The study of Biometric Systems, Computational Complexity measures and Soft Computing. He belongs to the following professional bodies: Full Member, Computer Professionals (Registration) Council of Nigeria; Corporate Member, Nigeria Society of Engineers; Register Engineer, COREN and . His contact email addresses are omidiorasayo@yahoo.co.uk and eoomidiora@lautech.edu.ng