International Journal of

Information and Computer Security

Editor-in-Chief:
Associate Prof. Raylin Tso

Visit www.inderscience.com/ijics

for more information and sample articles

INDERSCIENCE
PUBLISHERS
www.inderscience.com

Scope of the Journal

ISSN: 1744-1765 (Print), ISSN: 1744-1773 (Online)

Computer security has been a major concern since the 1950s. The ubiquity of the internet has engendered the prevalence of information sharing among networked users and organisations. This has rendered possible countless invasions of privacy/security worldwide. This risk has generated enormous concern about information and computer security among businesses, governments, legislators, academics, researchers, scientists and the public. IJICS is a double-blind refereed, authoritative reference addressing development of information/computer security in information technology, political science, informatics, sociology, engineering and science.

Topics covered include:

- Assurance and integrity of service
- Computer crime prevention/detection, computer forensics and security
- Confidentiality protection, cryptography and data protection
- Database and data security, denial of service protection
- E-commerce security, e-surveillance
- Fraud/hacker/terrorism detection/ prevention, information warfare, national security
- Information ethics
- Information privacy issues, information systems/information security, sharing
- Internet abuse, network intruder prevention, internet/network security
- Malicious code/unauthorised access protection, transaction security, virus/worm controls
- Risk management, safety-critical systems
- Secure communications technology and computer systems
- Security control measures, policy models and mechanisms
- Software and hardware architectures
- Wireless/mobile network security

Not sure if this title is the one for you?

Visit the journal homepage at **www.inderscience.com/ijics** where you can:

- View sample articles in full text HTML or PDF format
- Sign up for our free table of contents new issue alerts via e-mail or RSS
- View editorial board details
- Find out about how to submit your papers
- Find out about subscription options, in print, online or as part of a journals collection

You can order online at **www.inderscienceonline.com** or download an order form from **www.inderscience.com/subform.**

This title is part of the Computing and Mathematics Collection (see **www.inderscience.com/cm**). For library collection subscriptions or for a free institutional online trial, please contact **subs@inderscience.com.**

International Journal of Information and Computer Security

This journal also publishes Open Access articles

Editor in Chief: Associate Prof. Raylin Tso
ISSN online: 1744-1773
ISSN print: 1744-1765
4 issues per year
Subscription price

Calls for papers

Computer security has been a major concern since the 1950s. The ubiquity of the internet has engendered the prevalence of information sharing among networked users and organisations. This has rendered possible countless invasions of privacy/security worldwide. This risk has generated enormous concern about information and computer security among businesses, governments, legislators, academics, researchers, scientists and the public. *IJICS* is a double-blind refereed, authoritative reference addressing development of information/computer security in information technology, political science, informatics, sociology, engineering and science.

Sign up for new issue alerts
Subscribe/buy articles/issues
View sample issue
Latest issue contents
Forthcoming articles
Journal information in easy print format (PDF)

Publishing with Inderscience: ethical guidelines (PDF)
View all calls for papers
Recommend to a librarian
Feedback to Editor

Find related journals
Find articles and other searches

Keep up-to-date
Our Blog
Follow us on Twitter
Visit us on Facebook
Join us on Google+
Our Newsletter (subscribe for free)
RSS Feeds
New issue alerts
SHARE

About this journal Editorial Board Submitting articles

Topics covered include

- Assurance and integrity of service
- Computer crime prevention/detection, computer forensics and security
- Confidentiality protection, cryptography and data protection
- Database and data security, denial of service protection
- E-commerce security, e-surveillance
- Fraud/hacker/terrorism detection/prevention, information warfare, national security
- Information ethics
- Information privacy issues, information systems/information security, sharing
- Internet abuse, network intruder prevention, internet/network security
- Malicious code/unauthorised access protection, transaction security, virus/worm controls
- Risk management, safety-critical systems
- Secure communications technology and computer systems
- Security control measures, policy models and mechanisms
- Software and hardware architectures
- Wireless/mobile network security

More on this journal...

Browse issues

Vol. 10
Vol. 9
Vol. 8
Vol. 7
Vol. 6
Vol. 5

More volumes...

Get Permission
More on permissions

IJICS is indexed in:

- Scopus (Elsevier)
- Compendex [formerly Ei] (Elsevier)
- ACM Digital Library
- cnpLINKer (CNPIEC)
- DBLP Computer Science Bibliography

More indexes...

IJICS is listed in:

- Australian Business Deans Council Journal Rankings List
- The BFI lists

More journal lists/directories...

Journal news

New Editor for International Journal of Information and Computer Security

Associate Prof. Raylin Tso from National Chengchi University in Taiwan has been appointed to take over editorship of the International Journal of Information and Computer Security.

International Journal of Information and Computer Security

2015 Vol. 7 No. 1

Implementing generic security requirements in e-voting using modified stegano-cryptographic approach

Olayemi M. Olaniyi*

Department of Computer Engineering,
Federal University of Technology,
P. M. B. 65, Minna, Niger-state, Nigeria
Email: mikail.olaniyi@futminna.edu.ng
*Corresponding author

Oladiran T. Arulogun, Oluwasayo E. Omidiora and Oladotun O. Okediran

Department of Computer Science and Engineering,
Ladoke Akintola University of Technology,
P. M. B. 4000, Ogbomoso, Oyo State, Nigeria
Email: otarulogun@lautech.edu.ng
Email: eoomidiora@lautech.edu.ng
Email: oookediran@lautech.edu.ng

Abstract: Various information hiding techniques based on steganography, cryptography, and watermarking have been formulated in literatures to secure e-democratic decision making. The existing stegano-cryptographic models for secure e-voting are vulnerable to attacks and thus, can be manipulated by an eavesdropper. In this paper, we present an imperceptible stegano-cryptographic model for securing generic security requirements of e-voting systems. The purpose is to model a secure e-electronic voting capable of delivering credible, fair and transparent future e-democratic decision making in developing countries like Nigeria. The model was implemented on our framework for secure e-voting using Java programming language and Oracle database management system. The results of the study after qualitative performance evaluation of the model affirm that the model could serve as a platform for delivery of e-democratic decision making of high electoral integrity and political trustworthiness in developing countries with significant digital divides.

Keywords: e-voting; stego image; authentication; confidentiality; integrity; verifiability; wavelet; RSA; ECC; security; requirements; credible; fair; e-election.

Reference to this paper should be made as follows: Olaniyi, O.M., Arulogun, O.T., Omidiora, O.E. and Okediran, O.O. (2015) 'Implementing generic security requirements in e-voting using modified stegano-cryptographic approach', *Int. J. Information and Computer Security*, Vol. 7, No. 1, pp.64–90.

Biographical notes: Olayemi M. Olaniyi is a Lecturer in the Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BTech in 2005 and MSc in 2011 in Computer Engineering and Electronic and Computer Engineering respectively. He is currently a doctoral student at the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He has published in reputable journals and learned conferences. His areas of research include information and computer security, intelligent systems, embedded systems and telemedicine.

Oladiran T. Arulogun is a Senior Lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He was a Visiting Research Scholar at Hasso-Plattner Institute, Potsdam, Germany in 2012. He has published in reputable journals and learned conferences. His research interests include networks security, Mobile IPv6, wireless sensor network and its applications.

Oluwasayo E. Omidiora is currently a Professor of Computer Engineering in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with BSc Computer Engineering in 1991. He obtained his MSc and PhD in 1998 and 2006 respectively. He has published in reputable journals and learned conferences. His research interests are in soft computing and biometrics systems.

Oladotun O. Okediran is a Lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with BTech in Computer Engineering, MTech and PhD in 2002, 2008 and 2011 respectively. He has published in reputable journals. His research interests include: computational optimisation, e-commerce, biometrics-based algorithms and their applications to e-voting systems.

This paper is a revised and expanded version of a paper entitled ‘Design of a secure model for electronic voting system using stegano-cryptographic approach’ presented at the 7th International Conference on ICT Applications, National Defence College Abuja, FCT, Nigeria, 2–6 September 2012.

1 Introduction

The rapid application of information and communication technology (ICT) and diffusion of internet in all facets of life has provided several potential benefits including improved efficiency, convenience with reduced costs and economical governmental services to the populace (Olaniyi et al., 2013b). With ICT, populace has the capacity to be engaged in governance, particularly in all areas of political process such as the generation of information, enhanced deliberation among citizens, and most importantly, enhanced participation in democratic decision making (Briony, 2003). ICT is one of the best means of bridging the communication gaps between the people and the government. Through the internet, there is possibility for government to communicate with the citizens of the nation more effectively, and also aid the communication between citizens and their fellow citizens to discuss political and governmental issues (Azeta et al., 2013). Electronic voting (e-voting) as an important e-participatory governmental service has

attracted attention as cost effective and electronic decision making alternative to conventional voting for increase citizens' participation.

However, despite this value added advantages of e-voting to democratic process. The lack of trust in ICT and the internet as a safe medium to conduct secure transactions had had serious impacts in any effort to convert current conventional democratic procedure to electronic voting system since voting is a critical phase of democratic process (Antonio et al., 2007). In most developing countries like Nigeria; political, social, insecurity and electoral corruption discourage the electorate from getting involved in electoral decision making. From the various elections conducted since independence, about half the number of registered voters actually voted during elections. In addition, less than half of those who voted were involved in participatory governance (Azeta et al., 2013). Electioneering process in Nigeria is characterised with several irregularities, ranging from ballot box snatching and stuffing and weak electoral act (Olaniyi et al., 2011; Abdulhamid et al., 2013). This is due to current manual method of electoral process which inevitably leads to questionable electoral results (Olaniyi et al., 2012; Abdulhamid et al., 2013).

The adoption of e-voting in developing countries must be designed around increased citizens' trust. The notion of trust in complex distributed information system like e-voting is difficult to establish. This is due to the fact that, e-participation in e-voting involves complex duplex interactions between electorate and computer systems. Trust as a critical social property between actors-human and computer systems could be established *if and only if*, actors are convinced that the e-voting procedure complies with certain previously agreed trust properties (Antonio et al., 2007). These previously agreed trust properties according to Antonio et al. (2007) pragmatic definition is:

> "Trust of a party A in a party B for a service X is the measurable belief of A in that B will behave dependably for a specified period within a specified context".

In e-voting domain, ***A*** is the voter, ***B*** is the e-voting system and ***X*** is the e-voting service. Most importantly, by *dependably* the basic generic requirements for secure e-voting system (Antonio et al., 2007). These requirements are democracy, privacy, confidentiality, integrity, authentication, receipt-freeness, verifiability and uncoercibility (Ibrahim et al., 2003; Antonio et al., 2007; Abo-Rizka and Ghounam, 2007; Okediran et al., 2011; Olaniyi et al., 2013a). The notion of trust in e-voting systems is a property of system that emerges in the minds of electorate based on systematic process and manifests itself in their willingness to use the system in order to participate in electronic decision making process (Antonio et al., 2007). 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 (Meng, 2009). The authoritative models for secure e-voting systems:

- have been proved unreliable as computing power keeps increasing (Si and Li, 2005; Wang et al., 2004)
- are based on cryptography which 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 (Longe et al., 2008; Longe, 2011) and trapdoor problem (Longe et al., 2010)

- could threaten the integrity of democratic elections as attention of adversaries are drawn to access and attack the data being transmitted using cryptography alone for the transmission of votes over insecure wireless medium through remote internet voting (Olaniyi et al., 2012).

Considering these limitations of authoritative models of e-voting systems from the voter's end, the network and at voting system's end, the following generic security issues are pertinent: voter's true identity and validation-*authentication*; secrecy of electronic ballot-*confidentiality*; the *integrity* of ballot over electronic medium; electronic ballot *verification and auditing* during and after electioneering processes. These challenges in authoritative cryptographic models alone in electronic voting contributed to the exploration of modified hybrid technique of steganography and cryptography to the problem of insecurity in electronic voting in this paper. Steganography is the science of hiding and transmitting data through innocuous carrier in an effort to conceal the existence of data from an eavesdropper while cryptography is the science of transmitting scrambled data in an effort to secure communications from an eavesdropper despite his awareness of the data transmission. In most cases, sending encrypted data over wireless channel may draw attention, while invisible communications will not draw attention (Olaniyi et al., 2012). The combination of both techniques for secure multilayer data communication can be used for stronger mechanism of protecting and preserving the integrity of information from an adversary (Nagham et al., 2012).

This paper explores multi-layer data security (steganography and cryptography), with multiple media (image and video) and multiple domains (spatial and frequency) approach to the problem of authentication, integrity, confidentiality, verifiability issues in secure electronic voting. The rest of the paper is organised as follows: related works are presented in Section 2. The model design and development are presented in section in Section 3. Model simulations though prototype development is presented in Section 4 and some concluding remarks are made in Section 5.

2 Related works

A number of related works exist in literature in the area of application of cryptography, steganography and combination of both to secure electronic voting systems for the delivery of credible electronic democratic governance.

Okediran et al. (2011) proposed the requirement, design and implementation of a generic e-voting system. The security consideration of the model was based on RSA cryptosystem for end to end ballot security and firewalls in form of proxy server. The security consideration of the model was limited to large key size of RSA which requires large amount of computing time and large storage size on both mobile and electronic voting devices. In Sodiya et al. (2011), authors designed architecture for secure e-voting to ensure privacy, receipt-freeness and non-coercion. The model explore points from (x, y) coordinates of elliptic curve and probabilistic encryption to prevent problems of anonymity ,coercion and bribery in e-voting system. The model is an authoritative cryptographic model which can compromise the integrity of democratic elections as attention of an adversary is drawn to access and attack the vote being transmitted. In Tohari et al. (2009), authors proposed secured mobile voting scheme to meet mobile device better computing performance as well as integrity, confidentiality and anonymity

requirements of mobile voting system. The scheme increased in mobile computing performance at no expense of the integrity and confidentiality security level of mobile voting system performance to similar proposition in Light and David (2008). Authentication of the voter was not considered in the scheme. This inevitably threatens absolute security requirements of the proposed scheme.

Similar cryptographic models of secure voting systems were proposed in Li and Hwang (2012). Authors proposed an improved secure e-voting scheme to compensate for limitations of e-voting scheme proposed in Chang and Lee (2006). Also, Sujata and Banshidhar (2010), authors proposed multi-authority e-voting protocol based on blind signature to meet security requirements of privacy, anonymity, eligibility, fairness, verifiability and uniqueness of secure e-voting. Li and Hwang (2012) and Sujata and Banshidhar (2010) propositions are authoritative cryptographic models and thus limited to similar presentation in Sodiya et al. (2011). Authors in Gina et al. (2010) proposed identity-based cryptographic e-voting protocol based on two bilinear pairing to meet privacy, eligibility, and transparency, accuracy, and uniqueness requirement of secure e-voting. The protocol uses threshold encryption scheme and blind signature bilinear cryptographic primitives as main construction blocks. The proposition in Gina et al. (2010) is also limited to similar presentation in Sodiya et al. (2011).

When merits of data security obtainable from essentials features of cryptography models of e-voting are combined with steganographic models; electronic ballot casted by remote voters in cyberspace are secure to ensure privacy, confidentiality and integrity security requirements of electronic voting (Olaniyi et al., 2012).

There exists related works in literature an application of stegano-cryptographic modelling from generic point of view to security issue electronic voting. In Katiyar et al. (2011), authors integrated both steganographic and cryptographic techniques to solve authentication security requirements of an online e-voting system using both secret key and voters biometric fingerprint template as the cover. Authors in Katiyar et al. (2011) improved on Bloisi and Locci (2007) method by embedding Voter's Unique Identification Number and System generated and SHA256 hashed secret key created during registration on voters fingerprint template as unique final stego image.

Also, in Mallick and Kamilla (2011), authors combined both steganographic and cryptographic techniques to solve confidentiality and integrity security requirements of secure voting. However, the adopted steganographic technique has low robustness against statistical attack from statistical steganalyst, low robustness against image manipulation which might destroy the hidden message from its destination (Morkel et al., 2010). Authors in Prabha and Ramamoorthy (2012) improved on Katiyar et al. (2011) hashing speed limitation by replacing MD5 with SHA 256 and authenticating voters with biometric Iris. Authors in Rura et al. (2011) proposed a secured electronic voting system to the basic requirements of a secure voting system as well as non-functional requirements like un-coercibility, receipt-freeness and universal verifiability by experimentation with two different steganographic tools, F5 and outguess on five different types of images. The proposed model Stego medium is unilateral and prone to statistical attack.

In Sulthana and Kanmani (2011), authors proposed secure online voting scheme with both facial biometric integrated with fingerprint authentication and video steganography for authentication requirement of secure remote e-voting. The model is mobile device platform unfriendly as the model is based on RSA with large key size which requires both large amount of computing time and consumes large storage size on mobile voting

device. Authors in Linu and Anilkumar (2012) proposed multimodal face and fingerprint biometric and multilayer techniques to the problem of authentication in online e-voting system. The strength of the model lies in the nexus combination of voter's facial image and fingerprint samples as well as MD5 hashing algorithm for higher degree of authentication in the security of e-system. However, the model lacks verifiability requirement of secured e-voting system and stego object medium is unilateral.

Our model proposition is premised along improving the platform limitation in Okediran et al. (2011) by limiting RSA cryptosystem to poll site and kiosk-based e-voting scenario while ECC cryptosystem is adopted for mobile e-voting for speed and storage size design considerations and ballot integrity through cryptograghy. Further confidentiality, privacy and secrecy of e-ballot are accomplished by multi domain and multimedia improvement to Katiyar et al. (2011), proposition using scattered LSB image steganographic in spatial domain and integer to integer wavelet video steganography technique in frequency domain. Concurrent combination of multi domain in our proposition gives a model with high impercibility index and high robustness to attack from an adversary. Election insecurity in most developing countries like Nigeria is organically linked to broader insecurity, which are usually exacerbated during electoral period. This insecurity is rooted in the evolution of Nigeria's political economy, which also shapes the character of the Nigerian state and its ruling class (Orji and Uzodi, 2012). The electorate does not have a proper platform to clearly express his or her views, opinions and ideas in the light of moving the nation forward. Access to government officials is low and interaction among players in the national democratic setup is lacking. This has led to lack of patriotism and national cooperation. The government on the hand lacks probity, transparency and accountability in running the affairs of the Nigerian state (Azeta et al., 2013). Therefore, proper participation of the populace in future electoral decision making requires adoption of ICT through secured e-voting devoid of fraud. This is *sine qua non* to the delivery of credible election of high electoral integrity and political trustworthiness which is the gateway for e-democratic governance, political stability and national development.

The following deductions are established from the literature reviewed and they form the basis of the model proposed for the delivery of credible, fair and transparent e-democratic decision making in developing countries like Nigeria.

- Information hiding is an emerging research area for information security and privacy can be used to overcome insecurity threats in e-democratic decision making process through e-voting.
- Steganography is not intended to replace cryptography but rather to complement it (Adnaan Mohsin and Wafaa Mustafa, 2010). The difference between both methods of secure communication is the suspicion factor. While the former conceals message meant for communication, the latter scrambles the message between the sender and the message recipient. The hybrid implementation of both increases the amount of security in an application area (Nagham et al., 2012; Reddy and Raja, 2012).
- Secure electronic voting system must meet a list of generic security requirements to avoid scope for rigging, fraud and corruption in electoral process. These requirements include: confidentiality, integrity, authentication and verifiability/ non-repudiation (Abo-Rizka and Ghounam, 2007; Ibrahim et al., 2003; Antonio et al., 2007; Okediran et al., 2011; Olaniyi et al., 2013b).

- Existing stegano-cryptographic models in the reviewed literatures attempted to meet one or two of these requirements in piece-meal. None attempted to meet all these four security requirements at pre-election phase, election phase and post-election phase of democratic decision making through e-voting.
- Existing stegano-cryptographic models attempted covert communication using only one media to hide voter's electronic ballot.
- There is the need for e-voting with multi-layer (steganography and cryptography) data security, multimedia (Image and video) and multi domain (spatial and frequency) capability to ensure generic security requirements of secure e-voting.

3 Model design and development

3.1 Model requirements definition

As established in Section 2, our model would cater for the following fundamental requirements of secure e-voting from generic point of view: *confidentiality*, *authenticity*, *integrity/accuracy*, *democracy* and *verifiability*. The developed secure e-voting system based on our stegano-cryptographic model would:

a *be democratic*: permits only eligible voters to vote only once

b *ensure authenticity*: verify voters to be who they claimed they are

c *ensure privacy/confidentiality*: neither authorities nor anyone else can link any e-ballot to the voter who cast it, thus, all electronic ballot must be secret

d *accurate/integrity*: ensures impossibility for a vote to be altered and for a validated vote to be eliminated from the final tally

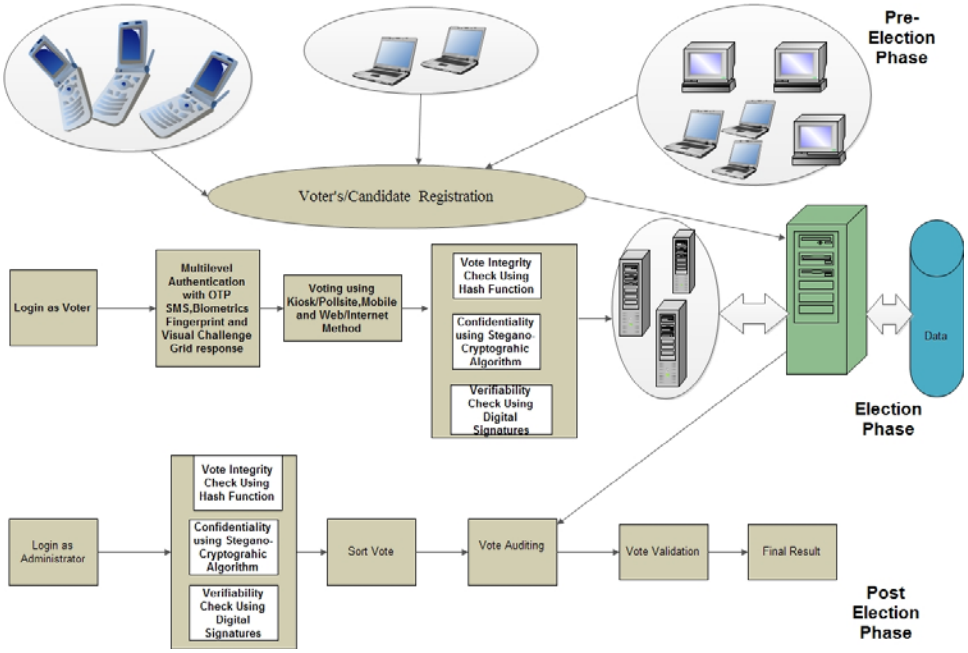
e *ensures verifiability*: vote can independently be verified and audited accurately.

3.2 Model architecture

Our model combines multi-layer (steganography and cryptography) data security, multimedia (image and video), and multi-domain (spatial and frequency) to solve the problem of authentication, integrity, confidentiality, non-repudiation in our developed framework of secure electronic voting in pre electoral, electoral and post electoral phase of e-democratic decision making. The framework of our secure e-voting is based on three-tier client-server architecture of Organisation of Advancement Structured Information Standard (OASIS, 2006) paradigm. The OASIS consortium standardisation of secure e-voting architecture is based on formal modelling and risk assessment architectures designed around electronic markup language (EML) and threat evaluation techniques. A three-tier is a client-server architecture in which the presentation, the application, processing, and the data management are logically separate processes. The tiers areas are shown in Figure 1. The pre-election phase, the election phase and the post-election phase. 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 takes care of the ballot submission in 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 voting for speed and storage size design consideration. The encrypted voters' intent (message) 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 and validate the identity of the voter. 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 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.

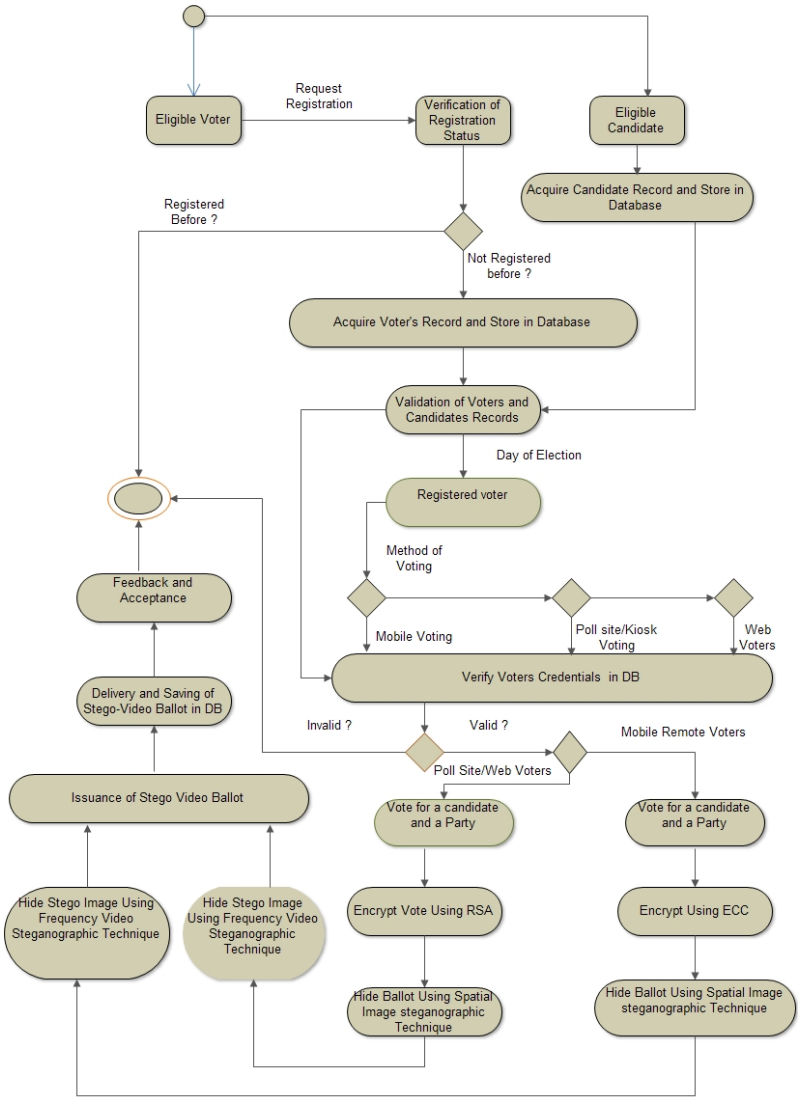
Figure 1 Framework of secured e-voting model (see online version for colours)



Source: Olaniyi et al. (2013b)

Our modified stegano-cryptographic model for secure e-voting is shown in Figure 2. The model is based on the assumption that an electorate has a unique national identification number prior to registration procedure. The unique identification number together with electorate bio-data, phone number and biometric fingerprints are enrolled and stored in the database. The registered electorate has a unique system generated voter identification number stored in the database for verification of electorate credentials during voting phase.

Figure 2 Modified stegano-cryptographic model of secure e-voting (see online version for colours)

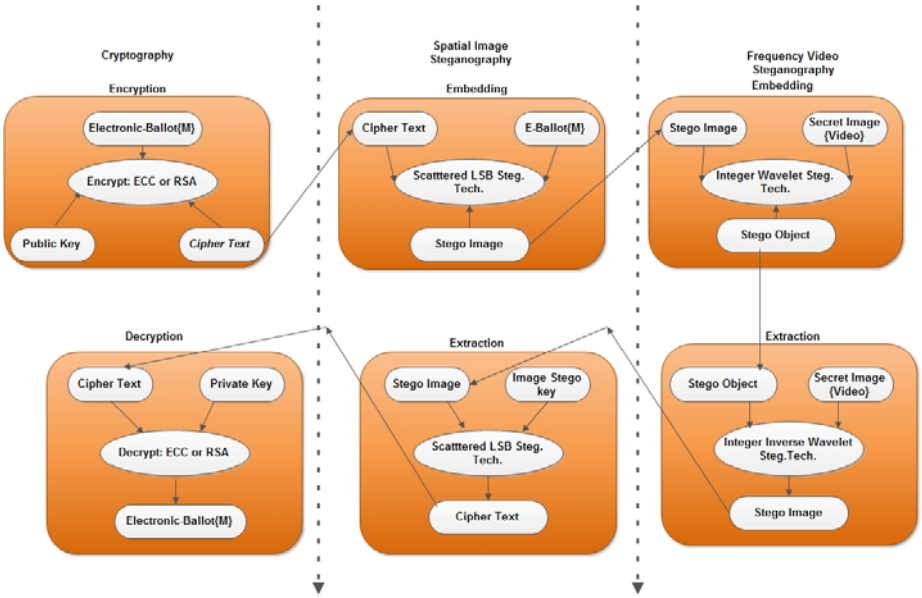


Source: Olaniyi et al. (2013b)

The model is designed around three voting scenarios: the remote mobile voting, web/internet voting and kiosk/polls site voting. The mobile terminal voter casts vote using his credential which is verified using both two-way, one-time SMS code and accurate response to visual challenge response from the grid. The mobile voter is validated by accurate comparison of remotely entered one-time SMS code; accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish remote voters are who they claim they are. The mobile ballot is thus encrypted using elliptic curve cryptographic technique to obtain cipher text for speed and memory constraints reasons of mobile device. The cipher text is

hidden into randomly generated image using modified LSB spatial image steganographic technique as shown in Figure 3 to produce stego-image. Further confidentiality of the vote in the stego-image is achieved through further hiding of vote in a video cover using integer to integer wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator. A multimedia improvement to similar presentation as does in Katiyar et al. (2011).

Figure 3 Modified stegano-cryptographic model of secure e-voting- confidentiality check (see online version for colours)



Remote web voting from voting device (PC/mobile device) is accomplished through secured uniform resource locator (URL) address of the secure e-voting system. The voting application runs remotely on the remote voter's device. The credential of remote web voter is verified using both two-way one-time SMS code and accurate response to visual challenge response from the grid. The web voter is validated by accurate comparison of remotely entered one-time SMS code; accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish remote voters are who they claim they are. The ballot is encrypted using RSA cryptographic technique to obtain cipher text. The cipher text is hidden into system generated picture using modified LSB spatial image steganographic technique as shown in Figure 3 to produce stego-image. Further confidentiality of the vote in the stego-image is achieved through further hiding of vote in a video cover using integer to integer wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator.

Consequently, poll site/kiosk voters cast electronic ballots at designated poll sites. Using fingerprint scanner, the voter credentials is verified in conjunction with accurate response to visual challenge response from the grid. The poll site voter is validated by accurate comparison of fingerprint of voter with template available in the database;

accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish poll site voters are who they claim they are (Olaniyi et al., 2013a). The ballot is encrypted using RSA cryptographic technique to obtain cipher text. The cipher text is hidden into system generated picture using modified LSB spatial image steganographic technique as shown in Figure 3 to produce stego-image. For further confidentiality of the vote, the stego-image is further hidden into a video cover using frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator. At the administrator end, the administrator recovers vote M by performing integer inverse wavelet transform on the stego object with the secret image to retrieved the cipher text from the stego image (S). Also using modified least significant bit (LSB) extraction steganographic algorithm, the cipher text is extracted from the stego image using the stego key K (the stego key). The final cipher text is then decrypted using either RSA or ECC decryption algorithms to get the final message M (vote) without the knowledge of an adversary who will neither detect that M is embedded in S nor be able to access the content of the secret message. Considerations for memory resources and multiple computational requirements of RSA were taken by limiting RSA cryptosystem ONLY for both poll site and kiosk e-voting and ECC cryptosystems for mobile voting. This is due to the fact that secure e-voting system must ensure verifiability of the casted votes through necessary security procedure. Our secure e-voting model in Figure 1 verifies casted vote through exploration of digital signature privileges of RSA at the post electoral phase through verification of hashed vote with encrypted vote (Olaniyi et al., 2013a). An improvement over similar model in Okediran et al. (2011). The concurrent combination of spatial and frequency steganographic technique in our model leads to the development of a model with high imperceptibility index, high robustness to attacks and high payload capacity in multimedia cover.

3.3 Mathematical modelling and underlying algorithm development

3.3.1 Cryptographic definition and algorithm development of the e-voting model for kiosk and poll site scenario

The definition of the cryptographic strength of the model for the electronic voting system is based on RSA cryptosystem. Supposing two random numbers p and q are chosen, then n, d and e can be computed from the public key (n, e) and private key (n, d).

$$S = (M, C, K, M, C, e, d, E, D) \tag{1}$$

Let the public key cryptosystem S be RSA from 1 as:

$$RSA = (M, C, K, M, C, e, d, N, E, D) \tag{2}$$

Then, the encryption function of message M (i.e., ballot vote) to cipher text C, i.e.:

$$E_{e,N} : M \to C$$

Using the public-key (e, N), and $M \in M$ maps to $C \in C$ in equation (1) is:

$$C \equiv M^e \bmod N \tag{3}$$

Also the decryption function of cipher text C (i.e., encrypted vote) to ballot vote M, i.e.:

$$D_{d,N} : C \to M$$

Using the private key (d, N), and $C \in C$ maps to $M \in M$ in equation (1) is given as:

$$M \equiv C^d \equiv (M^e)^d \pmod{N} \tag{4}$$

Thus, the developed algorithm to equation (3) as well as equation (4) is:

```
To encrypt a Message M using the public key (n, e);
Input: Given parameters, Encryption (M, n, e)
n = (Integer) M
{
if ((M > 0) and (M < n))
Output cipher text C: C = (M^e) * (mod (n))
Return C
}
To decrypt the ciphertext, C using the private key:
Input: Given parameters decryption (C, n, d)
{
Output Ballot Vote M: M = (C^d) * (mod(n))
Return M
}
```

3.3.2 Cryptographic definition and algorithm of the mobile voting system for remote mobile voting scenario

The definition of the cryptographic strength of the model for the mobile voting system is based on ECC cryptosystem's difficulty of solving the elliptic curve discrete logarithm problem (ECDLP). Due to resource constraints nature of mobile clients, mobile voting has more challenges than the common e-voting systems in the area of performance and security. For mobile voting system to meet security requirements of electronic voting while compensating for its inherent resources limitation necessitates securing data transfer from the mobile devices to the voting administrator using ECC in this model definition.

The definition for encryption and decryption of message, m (vote in this case) over an elliptic curve was achieved by encoding and decoding vote as an x – y point P_m on elliptic curve E. To encrypt a message P_m to voting authority, a random positive integer k is chosen to produce cipher text, z_m defined as:

$$Z_m = \{Kp, P_m + KQ\} \tag{5}$$

where Q is voting authority's public key.

The voter transmits the point:

$$\boldsymbol{Z}1 = K * P \text{ and } \boldsymbol{Z}2 = P_m + kQ \text{ to the } Z \text{ voting authority.} \tag{6}$$

To decrypt the cipher text consequently, the voting authority multiplies the first point in the pair by his private key, (i.e., $d * kP$) and subtract the result from the second point ($P_m + kQ$) as:

$$P_m + k * Q - d * KP \tag{7}$$

But $Q = d * P$.

Thus, equation (7) is:

$$P_m + K(d * P) - d(k * P) = P_m \tag{8}$$

Thus the algorithm adopted for *elliptic curve encryption* based on equation (6) is:

Input: Elliptic curve domain parameters (p, E, P, n), public key Q, plain text m

Output: Cipher text Zm

Begin

Let vote cast be represented as a point Pm in E (Fp)

Let d ∈ R [1, n – 1]

Compute Z1 = k * P

Compute Z2 = Pm + K * Q

Return (Z1, Z2)

End

And the algorithm adopted for *elliptic curve decryption* based on equation (8) is:

Input: Elliptic curve domain parameters (p, E, P, n), public key Q, cipher text Zm

Output: Plain text Pm

Begin

Compute Pm = Z2 – d * Z1

Return Pm

End

3.3.3 Steganographic definition and algorithm for electronic voting

3.3.3.1 Spatial image domain

The approach of image steganographic technique adopted was the modified LSB. The technique consists of two parts namely the embedding and the extraction part. The bit of the image to be used for steganography (cover media) is first extracted to allow for the hiding of the byte values of the text strings randomly in the byte values of the image. The following steps were used to implement the adopted modified random LSB image steganographic method:

1 read the cover image and ciphered message which is to be hidden in the cover image

2 convert text message in binary

3 calculate LSB of each pixels of cover image

4 replace LSB of cover image with each bit of secret message one by one randomly

5 output stego image.

Embedding algorithm

These were transformed to embedding algorithm as:

Input: Cover image C, Ciphered message M

Output: Stego image S

Choose a subset of cover elements such that $\{e_1, e_2, e_3, e_4, , , , e_{1m}\}$

Perform the substitution operation LSB $(C_{ei}) = M_i$ (M_i can be either 1 or 0).

For i = 1 to length (M) Do

Compute e_1 where to store the i^{th} message bit of m

$M_i \leftarrow$ LSB $(M_i) = C_{ei}$

End for

Extracting algorithm

The general procedure of extracting encrypted vote is:

1 read the stego image

2 calculate LSB of each pixels of stego image

3 retrieve cipher text bits and convert each 8 bit into character.

The extraction algorithm from above procedure thus is:

Input: Stego-image S

Output: Ciphered message M

For i =1 to length (M) Do

C_{ei} LSB $(C_{ei}) = M_i$

End for

3.3.3.2 Frequency video domain

The integer wavelet transform (IWT) approach of frequency steganographic technique is adopted based on wavelet's hidden message perceptually invisibility, statistically undetectability and difficulty in payload extraction during transit (Cheddad et al., 2008). In order to prevent loss of payload hidden in the stego image in spatial domain, an invertible integer to integer discrete wavelet transform (IIIDWT) is adopted for video frequency steganography. Figure 4(a) shows the embedding algorithm merging wavelets decomposition of the normalised version of the cover image (from sample video frame) and secret image (spatial stego image) into single fused result (stego video), the payload. Both cover image and secret image are transformed into IWT domain. Further application of IWT on the payload increases the security level. The single fused resultant matrix is obtained based on the addition of wavelet coefficient of the respective sub bands of the cover images and secret image as stated in equation (9):

$$f(x, y) = \alpha C(x, y) + \beta P(x, y) \tag{9}$$

$$\alpha + \beta = 1 \tag{10}$$

where F is modified IWT coefficients, C is the original IWT and P is the approximation band DWT coefficients of the payload. The fusion parameters, alpha (α) and beta (β), are the embedding strength factors chosen such that the payload is not predominantly seen in the final stego image frame. Also $C(x, y)$ is the cover image and $P(x, y)$ is the secret image (Reddy and Raja, 2012).

The embedding algorithm at wavelet transform domain thus is:

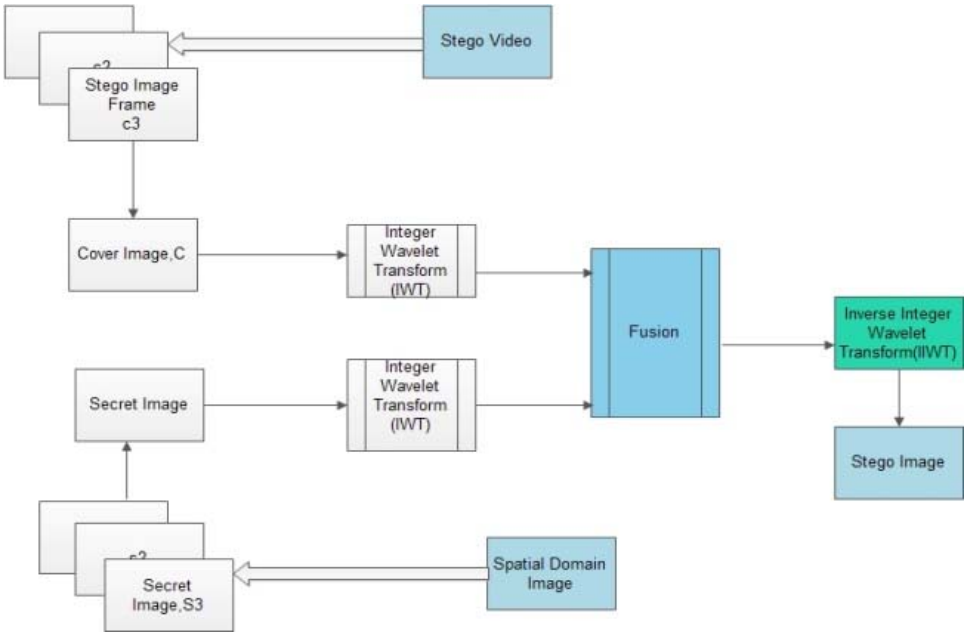
Input: Cover image frame from video file, C and spatial image as payload P	
Output: Stego image S	
Step 1	Get a video of extension as input of time two seconds
Step 2	Get sequence of cover image, c from step 1
Step 3	Take one frame as the cover image, c from step 2 and hide secret spatial image (payload image), p, into cover image from step 2
Step 4	Apply IWT on the cover image, c and payload image, p using Haar wavelet
Step 5	Apply two levels IWT on the approximate band of the fused image obtained
Step 6	Apply inverse IWT on the fused image
Step 7	Stego image frame, S, is obtained

Consequently, Figure 4(b) shows the retrieval algorithm for getting the secret image from the stego video (stego image frame). The stego image is normalised and inverse integer wavelet transform (IIWT) is taken. The data extraction process involves subtracting the IWT coefficient of the original cover image from IWT coefficient of the stego image frame, S. The first step of IIWT on these coefficients is applied by second IIWT in order to retrieve the coefficient of the secret image as shown in Figure 4(b).

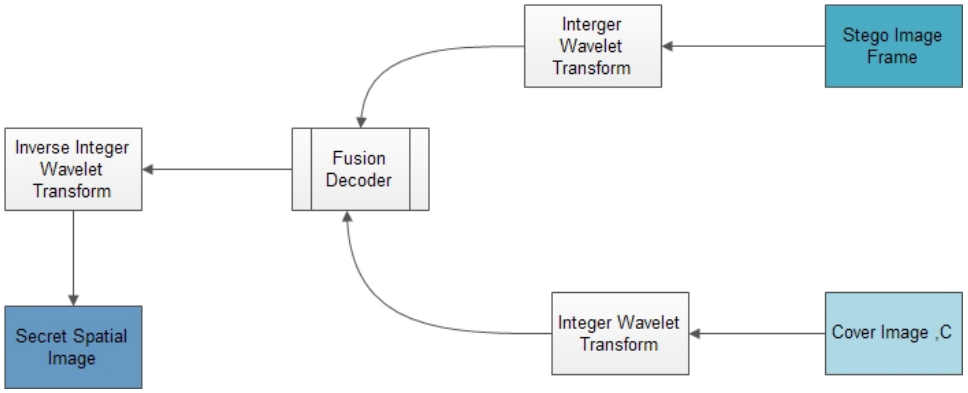
The extraction algorithm at wavelet transform domain thus is:

Input: Stego image frame, S	
Output: Payload, P, spatial stego image	
Step 1	Get the stego image frame S as the input to the decoder.
Step 2	Apply the IIDWT for the original cover image and the stego image.
Step 3	Subtract IIDWT coefficients of cover image, c from IWT coefficients of stego image frames to get the IWT coefficient of only p.
Step 4	Apply IIWT to all sub bands of payload P.
Step 5	The secret spatial image P is obtained.

Figure 4 (a) Stego image fusion encoding process and (b) stego image fusion decoding process (see online version for colours)



(a)



(b)

4 Model simulation and performance evaluation

4.1 Model simulation

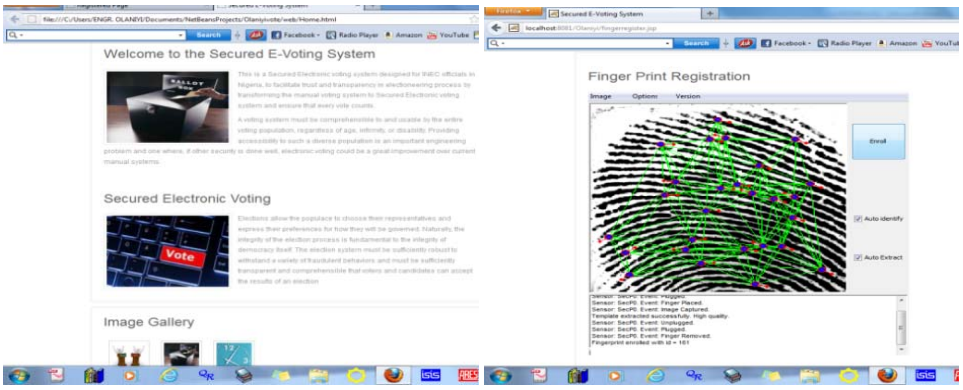
The model was simulated using Java Programming Language and Oracle 10g Database Management System (DBMS) through Evolutionary Spiral and Unified Software Process

Models. Selected qualified voters were asked to enrol data for this study through interaction with the sample secure e-voting system developed based on the architecture shown in Figure 1. The system graphical user interface (GUI) of the voting system required the voters to enrol their unique physiological biometric fingerprint, their biological data and vote using their preferred platform. The data collected are responses of the voters to the following decision variables involving the voters and voting software system: voter's personal information data, voter's fingerprint; voter's response to real time intelligent question on the grid. The developed secured e-voting systems based on the modified stegano-cryptographic e-voting model consists of the client end and back end subsystems.

4.1.1 Voter's registration subsystem

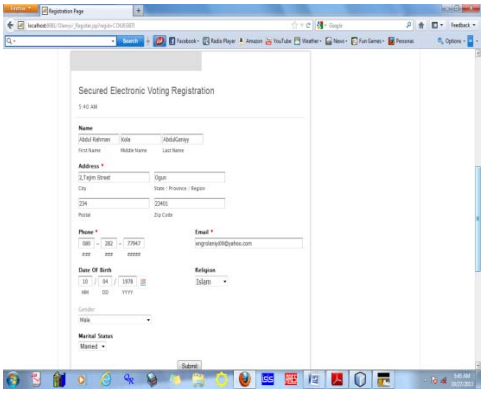
The voter's registration subsystem in Figure 5(a) registers the eligible voters with enrolment of his/her fingerprint prior to voting in Figure 5(b) against the voter's biodata information in Figure 5(c). The registration process is restricted to the designated voter's registration centre for the enforcement of legislation and social registration frameworks such as under-age voting and multiple voters' registration. Upon submission of voters biodata in Figure 5(c), an SMS containing the unique voter's one-time PIN short message service (OTP-SMS) shown in Figure 5(d) is sent to the voter's mobile phone. Consequently, the voter's OTP-SMS as well as Visual Grid information required to provide response during voting is sent to electronic mail address of the voter as an alternate electronic receipt for successful voter's registration shown in Figure 5(e). The developed client end of modified stegano-cryptographic model for secure e-voting system uses a centralised database system in real time.

Figure 5 (a) Registration subsystem (b) Fingerprint enrolment subsystem (c) Voters' biodata GUI (d) Mobile authentication credential (e) Valid registration receipt (f) Kiosk voting Platform GUI (g) Biometric fingerprint validation GUI (h) Multifactor authentication GUI (i) Presidential voting GUI (j) Gubernatorial voting GUI (k) Successful gubernatorial voting GUI (l) Unsuccessful gubernatorial voting GUI (m) E-voting auditing GUI (see online version for colours)

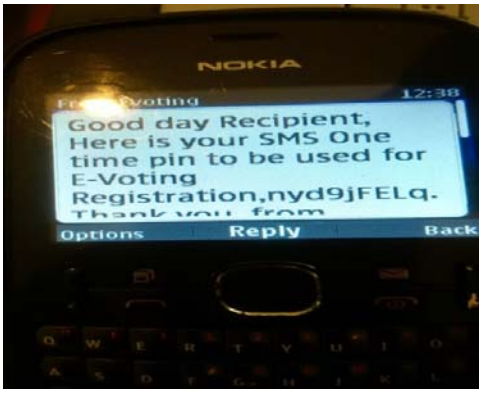


(a) (b)

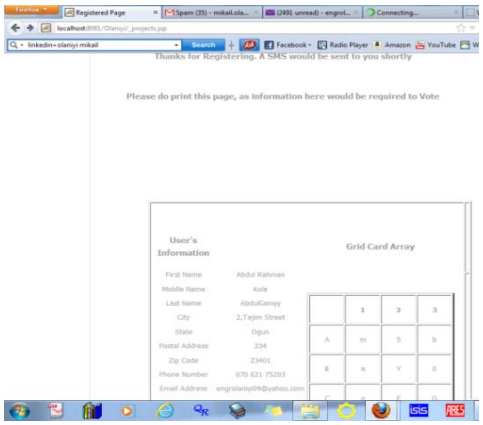
Figure 5 (a) Registration subsystem (b) Fingerprint enrolment subsystem (c) Voters' biodata GUI (d) Mobile authentication credential (e) Valid registration receipt (f) Kiosk voting Platform GUI (g) Biometric fingerprint validation GUI (h) Multifactor authentication GUI (i) Presidential voting GUI (j) Gubernatorial voting GUI (k) Successful gubernatorial voting GUI (l) Unsuccessful gubernatorial voting GUI (m) E-voting auditing GUI (continued) (see online version for colours)



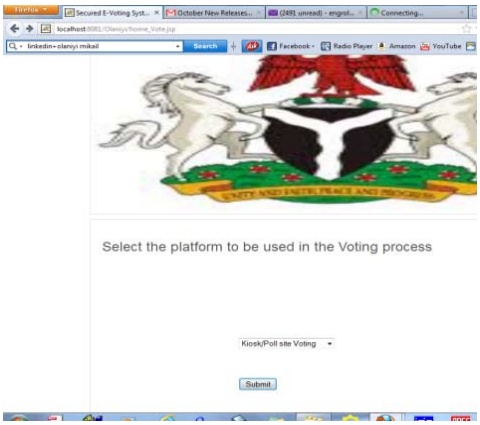
(c)



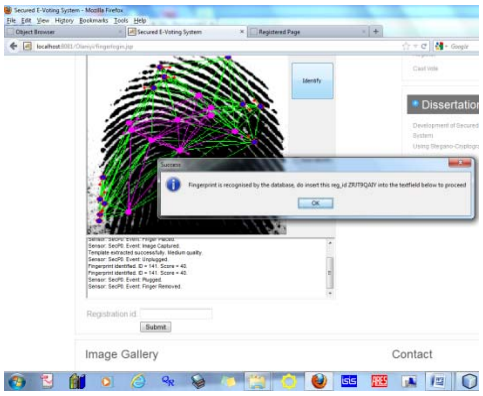
(d)



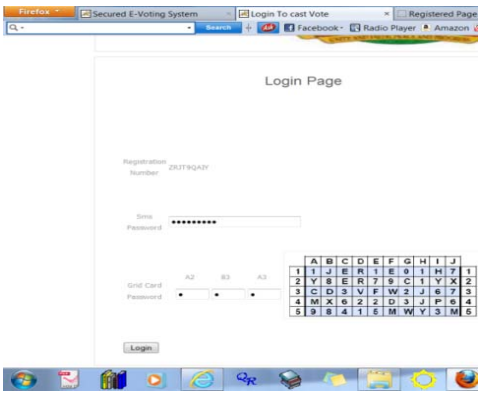
(e)



(f)

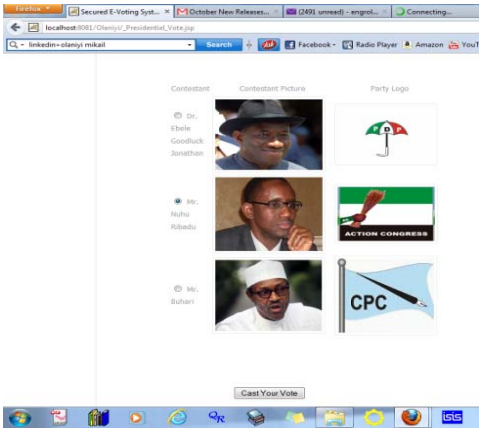


(g)

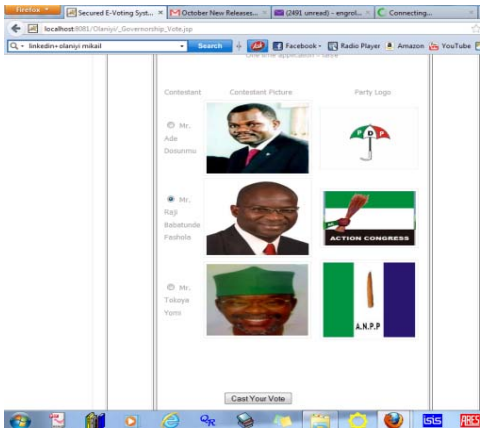


(h)

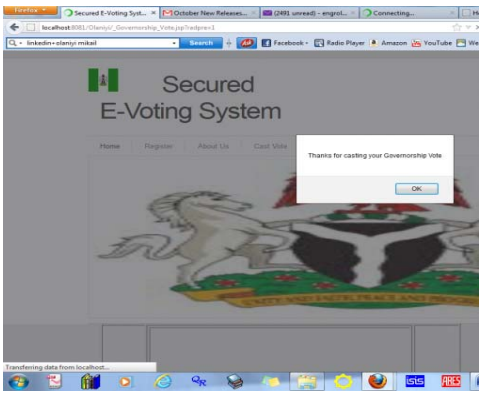
Figure 5 (a) Registration subsystem (b) Fingerprint enrolment subsystem (c) Voters' biodata GUI (d) Mobile authentication credential (e) Valid registration receipt (f) Kiosk voting Platform GUI (g) Biometric fingerprint validation GUI (h) Multifactor authentication GUI (i) Presidential voting GUI (j) Gubernatorial voting GUI (k) Successful gubernatorial voting GUI (l) Unsuccessful gubernatorial voting GUI (m) E-voting auditing GUI (continued) (see online version for colours)



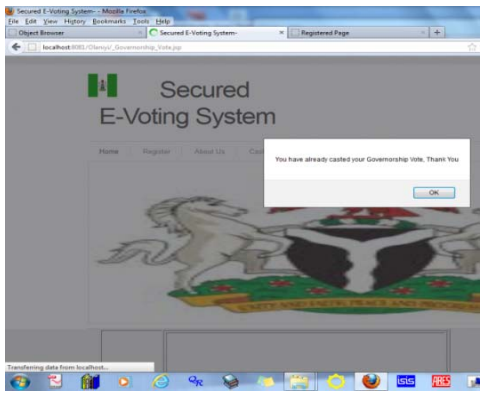
(i)



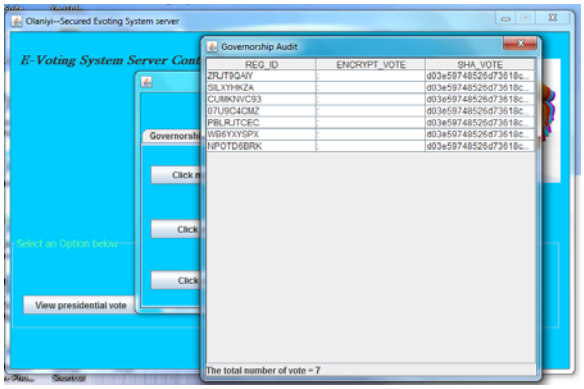
(j)



(k)



(l)



(m)

Figure 5(f) shows the interface for kiosk/poll e-voting scenario. The interface prompts the registered voter to select this option before the evaluation of the authentication security requirement of the e-voting. Figure 5(g) verifies at physiological level the authenticity of the voter in real time through the comparison of the voter's biometric fingerprint with the available fingerprint template available at the secured e-voting database. Upon successful matching of the voter's fingerprint with unique template in the database, the voters unique identification is made available for the next level of voter's authentication otherwise the secured e-voting system denies the voter next phase of voting.

Figure 5(h) depicts the next level of authentication of the one-time SMS and visual request to the grid. The OTP-SMS provided in Figure 5(d) to the mobile device of the registered voter is required for this purpose. Successful matching of the voters finger print to the template available in the database, one-time SMS and accurate response to visual challenge requests in Figure 5(h) guarantees the voters the opportunity to casts vote in either presidential or gubernatorial elections as shown in Figure 5(i) or 5(j) respectively. As shown in Figure 5(i) and Figure 5(j), authenticated voter could casts only one vote for a candidate in either presidential or gubernatorial elections respectively. Figure 5(k) shows the secure e-voting interface for successful completion of gubernatorial election. Figure 5(l) shows the denial of multiple voting by an erring voter in a gubernatorial election in poll site/kiosk voting scenario. In Figure 5(m), electronic ballot casted can be audited to verify its inclusion in the finally tally to declare the final winner of an e-election through voting.

4.2 Performance evaluation

The developed model performance was evaluated by subjecting the model final spatial stego object (image) for steganalytic detection through stego object stability against chi-square attacks and dictionary attacks using StegSecret and StegDetect steganalytic detectors as well as histogram analysis of the stego image in comparison with the cover image for different pixel levels in an ImageJ image processing analytical tool.

The goal of steganalysis is to identify suspected digital media, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Steganalysis detector attempts to detect the presence or absence of a covert message when presented with a stego object. The developed stegano-cryptographic model for e-voting system was evaluated for confidentiality requirement of secure e-voting system through evaluation of impercibility metric of steganographic system. StegDetect detector detects images that have content hidden with JSteg, JPHide and OutGuess 0.13b (steganographic tools) and any invisible steganographic technique in digital media especially the joint photographic experts group (JPEG) typed image.

For the evaluation, the final stego-image after encryption of the electronic ballot of a particular candidate hidden inside a cover image was scanned for possible detection by StegDetect with sensitivity level of 1.00, 5.00 and 9.00 as shown in Figure 6. The higher the index level of sensitivity of the suite, the higher the level of detection of the stego image. For each jpeg image found in the secure electronic voting system folder, *C:\users\Engr Olaniyi\desktop\Olaniyi*, StegDetect displays the output from possible steganographic systems found in each image or *negative* if no steganographic content could not be detected. StegDetect expresses the level of confidence of the detection with one to three stars.

As shown in Figure 6, the developed model stego image named, *C:\users\Engr Olaniyi\Olaniyi\Web\StegoImage.jpg* was *negatively detected* by StegDetect indicating that the StegDetect could not detect the content (encrypted electronic ballot-vote) embedded in the stego Image and therefore could not launch the brute force attack against the stego-image. Therefore, the developed modified stegano-cryptographic technique for e-voting system is truly secured since the stego-image is highly imperceptible.

Figure 6 Steganalytic investigation using StegDetect steganalytic detector (see online version for colours)

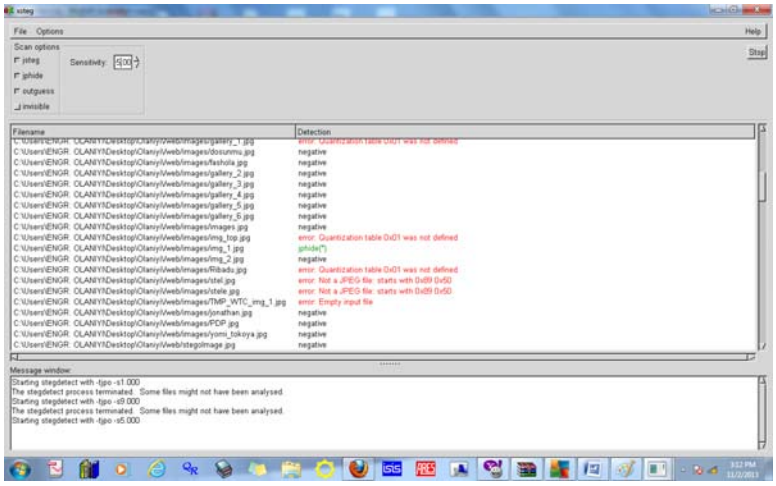
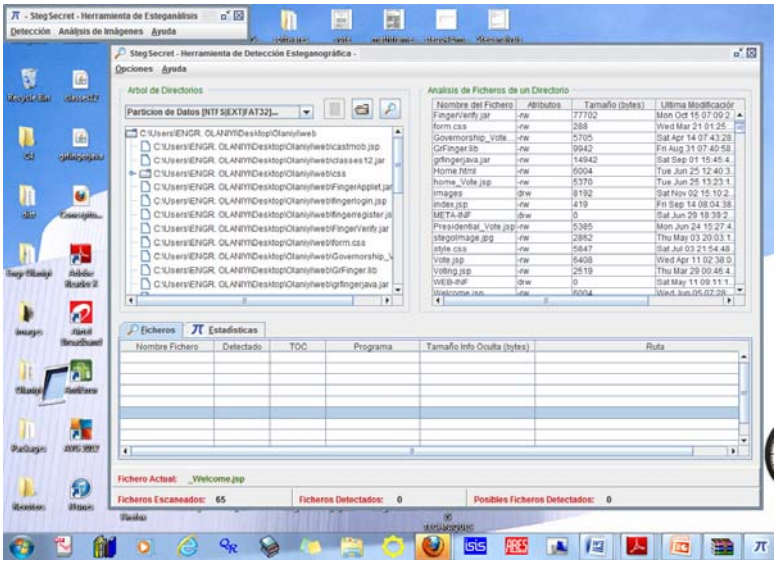


Figure 7 Steganalytic investigation using StegSecret steganalytic tool (see online version for colours)



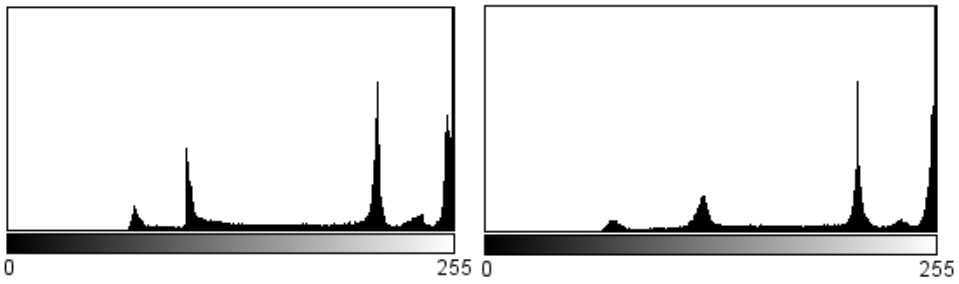
Similar result was obtained when the stego image in the same folder was scanned with StegSecret steganalysis tool shown in Figure 7. StegSecret is the name given to the open source steganalytic program developed to detect steganographic content in different digital media. As shown in Figure 7, the evaluation of the developed technique after scanning with StegSecret steganalytic tool depicts that the tool could not launch visual attacks and statistical attack such as chi square and RS attack for sequential LSB detection and estimation of pseudo LSB size respectively on the stego-image. Therefore, the developed modified stegano-cryptographic technique is perfectly imperceptible.

The security capability of the final stego image was analysed through histogram analysis of the stego image in comparison with the cover image for different pixels in ImageJ image processing analytical tool. The stego image and the cover image shown in Figure 8(a) and Figure 8(b). The corresponding histogram analysis of both the cover image and stego image at 256 * 256 pixels, 128 * 128 pixel and 64 * 64 pixels are shown in Figure 9, Figure 10 and Figure 11 respectively.

Figure 8 Stego and cover image (in greyscale), (a) cover image (8-bit, greyscale) (b) stego image (8-bit, greyscale)

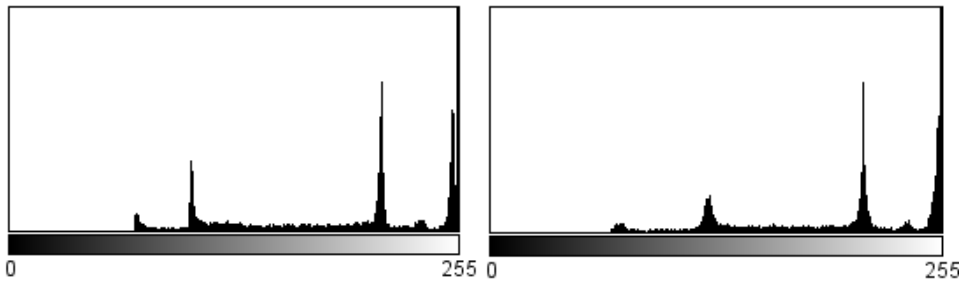
(a) (b)

Figure 9 Histogram of cover image and stego image at 256 * 256 pixels, (a) cover image (256 * 256 pixels) (b) stego image (256 * 256 pixels)



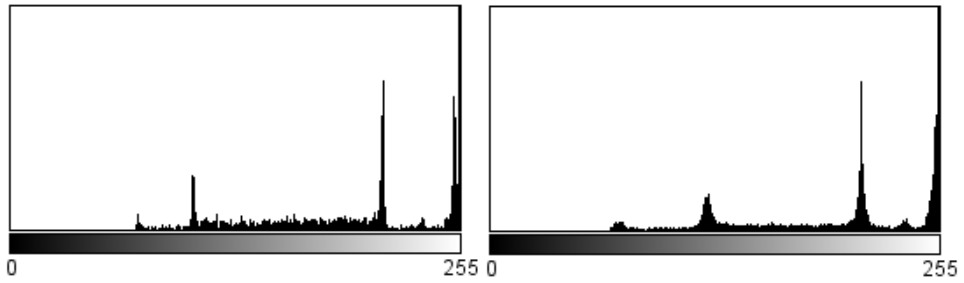
(a) (b)

Figure 10 Histogram of cover image and stego image at 128 * 128 pixels, (a) cover image (128 * 128 pixels) (b) stego image (128 * 128 pixels)



(a) (b)

Figure 11 Histogram of cover image and stego image at 64 * 64 pixels, (a) cover image (64 * 64 pixels) (b) stego image (64 * 64 pixels)



(a) (b)

Considering the histogram analysis of Figure 9 and Figure 10 and Figure 11, it can be inferred that there is only slight changes in the level of distortion of the altered stego image in comparison with the original cover image after embedding the electronic ballot of the voter in the cover image, even though that the stego image is doubly secured. The shows that stego image at these pixels value is imperceptibly secured for future e-democratic decision making.

5 Conclusions and recommendations for future work

The adoption of e-voting systems for electronic democratic decision making must be designed around a list of generic security requirements of authentication, confidentiality, integrity and verifiability. Without these requirements, rigging, fraud and corruption in electoral process will ultimately mar the integrity of the electioneering process. In this paper, we have presented the design and development of a modified stegano-cryptographic model for secure e-voting towards the delivery of future credible, fair and transparent electronic democratic decision making in the developing countries where significant digital divides exist like Nigeria. The delivery of free, fair and credible

elections by political scientist and development theorist is an impetus for an emergence of democratic governance, accountable and legitimate governments with the capacity to initiate and implement clearly articulated development programmes; empower the electorate to hold the government accountable and platform to demand strong credentials and feasible development agenda from prospective government officials.

The implementation of our secure e-voting model in future e-democratic making in developing countries like Nigeria through the power of Information and Communication Technologies would no doubt increase citizen participation in governance, build a stronger democracy and peaceful nationwide community. In future, the assessment of the impercibility and robustness of the modified stegano-cryptographic technique for secure e-evoting model would be carried using several image quality metrics and benchmarked with similar secure e-voting models in various domains. Also, other open issues include:

1 *Security against DoS and DDoS attacks*: Denial of service (DoS) is an attempt to make computing resource unavailable by saturating the target device with external bogus and unnecessary communications request. Although network filtering and cloud computing paradigm are suggested in literatures along aversion of this challenge, future research could provide mechanism to increase and protect the developed secured model for attacks due to DoS and DDoS.

2 *Voters' coercibility:* Although the developed e-voting model ensures voter's authentication and validation through multifactor authentication, an open issue of debate is how the voting system would prevent voters from selling their vote prior to voting. Future research should look at issue of non-coercion in secure e-voting.

3 *Quantification of communication and network resource requirements*: Models for the quantification of communication and network resource requirements like bandwidth, throughput and packet size could also be developed to quantify the communication and network resources requirement for proper functioning of secure e-voting model.

4 *Exploration of audio cover and audio steganographic techniques*: Future steganographic investigation could also look at audio steganographic technique using audio cover for covert communication security in e-voting systems.

References

Abdulhamid, S.M., Adebayo, O.S., Ugiomoh, D.O. and AbdulMalik, M.D. (2013) 'The design and development of real time e-voting system in Nigeria with emphasis on security and result veracity', *International Journal of Computer Network and Information Security*, Vol. 5, No. 5, pp.9–18 [online] http://www.mecs-press.org/ijcnis/ijcnis-v5-n5/IJCNIS-V5-N5-2.pdf (accessed 7 August 2013).

Abo-Rizka, M. and Ghounam, H.R. (2007) 'A novel e-voting in Egypt', *International Journal of Computer Science and Network Security*, Vol. 7, No. 11, pp.226–234.

Adnaan Mohsin, A.B. and Wafaa Mustafa, A.B. (2010) 'Stego-based crypto technique for high security applications', *International Journal of Computer Theory and Engineering*, Vol. 2, No. 6, pp.835–841.

Antonio, A., Korakas, C., Manolopoulos, C., Panagiotaki, A., Sofotassios, D., Spirakis, P. and Stamatiou, Y.C. (2007) 'A trust-centered approach for building e-voting systems',

Proceedings of Electronic Government, 6th International Conference on Electronic Govermment, E-Gov 2007, Regensburg, Germany, pp.366–377.

Azeta, A.A., Azeta, V.I., Oluwaseun, O., Azeta, A.E. and Ayeni, G.A. (2013) 'Implementing an e-democracy system in Nigeria', *Proceedings of the 11th International Conference on Electronic Government and National Security*, Nigeria Computer Society (NCS), Osun State, Nigeria, pp.98–103.

Bloisi, D. and Locci, L. (2007) 'Image-based steganography and cryptography', *Proceedings of Second International Conference of Computer Vision Theory and Applications (VISAP)*, Barcelona, Spain, Vol. 1, pp.127–134.

Briony, O. (2003) 'The potential contribution of ICTs to the political process', *The Electronic Journal of e-Government*, Vol. 1, No. 1, pp.31–39.

Chang, C. and Lee, J. (2006) 'An anonymous voting mechanism based on the key exchange protocol', *Elsevier Computer and Security Journal*, Vol. 25, No. 4, pp.307–314.

Cheddad, A., Condell, J., Curran, K. and McKevitt, P. (2008) 'Security information content using new encryption method and steganography', *Proceeding of the Third IEEE International Conference on Digital Information Management (ICDI 2008*), University of East, London, UK, pp.563–568.

Gina, G.G., Roberto, G. and Gonzalo, I.D. (2010) 'Identity-based threshold cryptography and blind signatures for electronic voting', *WSEAS Transactions on Computers*, Vol. 9, No. 1, pp.62–71.

Ibrahim, S., Kamat, M., Salleh, M. and Abdul Aziz, S. (2003) *Secure Voting Using Blind Signature* [online] http://eprints.utm.my/3262/1/IEEE02-EVS_full_paper_ver14Nov.pdfR (accessed 17 November 2011).

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.

Li, C. and Hwang, M. (2012) 'Security enhancement of Chang-Lee anonymous e-voting scheme', *International Journal of Smart Home*, Vol. 6, No. 2, pp.45–52.

Light, J. and David, D. (2008) 'An efficient security algorithm in mobile computing for resource constrained mobile devices', *Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Vancouver, Canada.

Linu, P. and Anilkumar, M.N. (2012) 'Authentication for online voting using steganography and biometrics', *International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 1, No. 10, pp.26–32.

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, No. 1, pp.1–5.

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, No. 1, pp.1–12.

Longe, O.B., Roberts, A.B.C., Onifade, O.F.W., Kaka, O. and Isiaka, R.M. (2008) 'Framework for the development of a hybrid chaotic image scheme for multimedia data encryption', *Proceedings of 3rd International Conference on ICT Applications*, Obafemi Awolowo University, Ile-Ife, Osun State, Nigeria, Vol. III, pp.150–154.

Mallick, P.K. and Kamilla (2011) 'Crypto steganography using linear equation', *International Journal of Computer and Communication Technology*, Vol. 2, No. 8, pp.106–112.

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, No. 5, pp.370–377.

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 [online] http://martinolivier.com/open/stegoverview.pdf (accessed 4 June 2012).

Nagham, H., Abid, Y., Ahmad, R. and Osamah, M. (2012) 'Image steganography techniques: an overview', *International Journal of Computer Science and Security*, Vol. 6, No. 3, pp.168–187.

OASIS (2006) *OASIS Standard: Election Markup Language (EML) Process and Data Requirements*, February, Version 4.0a, Organization for the Advancement of Structured Information Standards [online] https://www.oasis-open.org/standards (accessed May 2012).

Okediran, O.O., Omidiora, E.O., Olabiyisi, S.O., Ganiyu, R.A. and Alo, O.O. (2011) 'A framework for a multifaceted electronic voting system', *International Journal of Applied Sciences*, Vol. 1, No. 4, pp.135–142.

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.

Olaniyi, O.M., Arulogun, O.T. and Omidiora, E.O. (2012) 'Towards an improved stegano-cryptographic model for secure electronic voting', *African Journal of Computing and ICT*s, Vol. 5, No. 6, pp.7–16.

Olaniyi, O.M., Arulogun, O.T., Omidiora, E.O. and Adeoye, O. (2013a) 'Design of secure electronic voting system using multifactor authentication and cryptographic hash functions', *International Journal of Computer and Information Technology (IJCIT)*, Vol. 2, No. 6, pp.1122–1130.

Olaniyi, O.M., Arulogun, O.T., Omidiora, E.O. and Okediran, O.O. (2013b) 'A survey of cryptographic and stegano-cryptographic models for secure electronic voting system', *Covenant Journal of Informatics and Communication Technology (CJICT*), Vol. 1, No. 2, pp.54–78.

Orji, N. and Uzodi, N. (2012) *Post-Election Violence in Nigeria: Experiences with the 2011 Elections*, Policy and Legal Advocacy Centre (PLAC) [online] http://www.placng.org/new/publications/pev.pdf (accessed 4 December 2013).

Prabha, S.M. and Ramamoorthy, S. (2012) 'A novel data hiding technique based bio-secure online voting system', *Proceedings of International Conference on Computing and Control Engineering (ICCCE 2012)*, pp.1–4 [online] http://www.iccce.co.in/Papers/ICCCECS143.pdf (accessed 4 October 2012).

Reddy, M.H. and Raja, K.B. (2012) 'High capacity and security steganography using discrete wavelet transform', *International Journal of Computer Science and Security*, Vol. 3, No. 6, pp.462–472.

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, 25–28 September, Langwi, Malaysia.

Si, H. and Li, C. (2005) *Maintaining Information Security in E-Government through Steganology* [online] http://www.igi-global.com/chapter/encyclopedia-digital-government/11652.pdf (accessed 5 October 2012).

Sodiya, A., Onashoga, S. and Adelani, D.I. (2011) 'Secure e-voting architecture', *Proceedings of Eighth International Conference on Information Technology: New Generations*, IEEE Computer Society, pp.342–347.

Sujata, M. and Banshidhar, M. (2010) 'A secure multi authority electronic voting protocol based on blind signature', *Proceedings of International Conference on Advances in Computer Engineering*, pp.271–273.

Sulthana, S.S. and Kanmani, S. (2011) 'Evidence based access control over web services using multi security', *International Journal of Computer Applications*, Vol. 17, No. 3, pp.1–7.

Tohari, A., Jainkun, H. and Song, H. (2009) 'An efficient mobile voting system security scheme based on elliptic curve cryptography', *Proceedings of Third International Conference on Network and System Security*, IEEE Computer Society, pp.474–479.

Wang, X., Feng, D., Lai, X. and Yu, H. (2004) *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*, Cryptologye Print Archive, Report 2004/199 [online] http://eprint.iacr.org/2004/199.pdf (accessed 5 October 2012).