A Survey of Cryptographic and Stegano-Cryptographic Models for Secure Electronic Voting System

Olaniyi, Olayemi Mikail[1],

Arulogun Oladiran Tayo[2],

Omidiora Elijah Olusayo[2],

Okediran Oladotun Olusola[2]

[1]Department of Computer Engineering
Federal University of Technology,
Minna, Niger-state, Nigeria.

[2]Department of Computer Science and Engineering
Ladoke Akintola University of Technology,
Ogbomoso, Nigeria.
* E-mail of the corresponding author: mikail.olaniyi@futminna.edu.ng

Abstract: The success rate of an electronic voting system in electronic decision making is dependent on security, authenticity and integrity of pre-electoral, electoral and post electoral phases of the electioneering process. Various Information Security and Privacy Technologies including steganography, cryptography, and combination of both as well as watermarking have been formulated in literatures to make e-democratic decision through e-voting systems to be fair and credible. In this paper, we present a survey of existing cryptographic and stegano-cryptographic schemes in securing e-voting systems. We established critical security requirements for secure e-voting systems for all phases of the electioneering processes, formulated an adaptable conceptual framework for secure e-voting systems for developing countries and proposed a multilayer, multi-domain and multimedia model for electronic voting system for the delivery of fair, transparent, better participatory and credible elections in future e-democratic dispensation in developing countries with significant digital divides.

Keywords: Authentication, E-Voting, Confidentiality, Cryptography, Security, Steganography, Image.

1. Introduction

The rapid application of Information and Communication Technology (ICT) in all facets of life has provided several potential benefits including improved efficiency, convenience with reduced costs and productivity. In literature, ICT has been used to provide different electronic solutions in governance (Rura *et al*., 2011; Roy and Karforma 2011a;Roy, Banik and

Karforma, 2011b); Learning (Queensland Government ,2013; Itmazi 2013); Shopping (Adeline *et al.*, 2006); Medicine (Gartner (2013) and in democratic decision making (Olaniyan, Mapayi, and Adejumo 2011;, Olaniyi *et al.*, 2011; Okediran *et al.*, 2011a, Olaniyi *et al.*, 2013).The success rate of these application areas depends on security, authenticity and integrity of the information transmission and storage during their respective e-service implementation (Roy *et al.*, 2011b).

The application of ICT in the proper execution of democratic rights has made Electronic Voting (E-Voting) systems one of the paramount pillars of e-governance. E-voting involved the use of computerized voting equipment in the process of voter's registration, ballot casting and counting, and ballot recording in a trustable manner (Cetinkaya & Koc, 2009; Olaniyi *et al.*,2011). Most electronic system of voting offers the following multiple advantages over the traditional paper-based voting: increased participation in democratic governance as more citizens have access to express their opinion, reduced costs as the materials required for printing and distributing ballots as well as the manpower required to govern poll sites are considerably reduced, flexible as it can be tailored to support multiple languages, 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, lower election fraud in endangered countries with young democracies (Sodiya, Onashoga and Adelani, 2011;Manish, Suresh , Hanumanthappa , and Evangelin , 2005; Okediran *et al.*, 2011a),

To fulfill these competitive advantages, researchers in electronic voting system have reached a consensus of a number of competing criteria that must be satisfied (Cranor and Cytron, 1996); NSF (2001); Okediran *et al.*, (2011a); Katiyar *et al.*, (2011), Lambrinoudakis , Gritzallis , Tsoumas , Karyda and Ikonomopulos (2003).These requirements in Okediran *et al.*, 2011a) are grouped into generic and system specific; in Lambrinoudakis *et al.*,(2003) as functional and non-functional requirements and in (Cranor and Cytron, 1996) as core pack properties

In order to establish a peaceful resolution of the struggle for political power and stability among the populace in democratic governance; all aspects of elections process must be directly observable by the candidates, the official observers and the electorate themselves (Olaniyi *et al.*, 2012). The direct observance of the electorate, transparency, integrity of the electoral process and security of lives must be fair and guaranteed. Therefore, for e-voting system to provide solution to challenges attributed to traditional voting method, a list of security requirements of e-voting must be observed. These requirements include: confidentiality, integrity, authentication and verifiability/non-repudiation (Ibrahim, Kamat , Salleh and Abdul Aziz (2003); Abo-Rizka and Ghounam (2007). Without these requirements, rigging, fraud and corruption in electoral process will occur.

The enforcement of security in electronic voting systems has been proposed with different Information Security and Privacy Technologies with data encryption schemes. In practice, these data encryption schemes like Data Encryption Standard (DES), and Advanced Encryption Standard (AES) have not only been adequate but are not very efficient in the encryption of large volume of digital data (Alok and Atul 2011); Tohari , Jainkun and Song 2009).This can be addressed by complementing data encryption with data hiding. Information hiding has been used to enhance security level of data encryption systems. The main driving force of information hiding is concern over copyright, such as audio, video and other works available in digital form, the ease with which unauthorised copies can be made and the need to identify violators and prosecute them (Chang and Lee 2006). Military communication systems make increasing use of information hiding. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Information hiding is an emerging research area which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography (Muhalim *et al.*, 2003).

In this paper, we made a survey of the existing cryptographic and stegano-cryptographic models for secure electronic voting systems, formulate a conceptual framework for secure e-voting and proposed a model for secure electronic voting system with the view of increasing participation, confidence and trustworthiness in electronic democracy. 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 (Olaniyi, Arulogun, and Omidiora 2012). In most cases, sending encrypted data over wireless channel may draw attention, while invisible communication will not. The combination of both sciences through stegano-cryptographic modeling technique for secure multilayer data communication is conjectured for stronger ballot protection and preservation of the electoral integrity from an adversary for near and remote secure e-voting scenarios. (Olaniyi *et al*., 2012)

The rest of the paper is organized into five sections. Section two describes the underlying mathematics of steganographic and cryptographic systems; Section three described research work conducted so far in the application of cryptographic models in E-voting systems; Section Four described research work conducted so far in the application of Stegano-cryptographic models in E-voting systems. We made a proposal for an adaptable framework for secure e-voting system and model for multilayer (Stegano-cryptographic), multi domain (Spatial and Frequency) and multimedia (Image and video) for secure e-voting systems in section Five and section six concludes and established our future direction.

2.0 Underlying Mathematics of Steganographic and Cryptographic Systems

Steganography technique is premised along transmission of confidential message on a channel, where some other kind of information is already being transmitted (Shamin and kattamanchi 2012). Usually a steganographic system consists of the secret message, 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 technique involves the replacement of unused data or useless data in the ***covert*** data, such as graphics, sound, text, and HTML with bits different invisible information. Media such as digital video, image, sound files and other related files contain perpetually redundant information that can be explored as “covers” to hide secret message**.** The general model of a steganographic system is shown in Figure 1.

The general process of embedding data using steganography is shown in Figure 2 and defined as (Chedad 2009) : Let *C* denote the cover carrier, i.e., image *A*, *M* the data to hide, M’ the extracted file, g_k the steganographic function and C′ the stego-image. Let *K* represent an optional key used to encrypt the message or to generate a pseudorandom noise which can be set to {Ø}, the null set, for simplicity. Also, Let *M* be the message to communicate, image *B*. E_m is an acronym for embedding and E_x is an acronym for Extraction. Therefore, a complete steganographic system would be:

$$E_m: C \oplus K \oplus M \rightarrow C' \qquad (1)$$

$$E_x(E_m(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M \qquad (2)$$

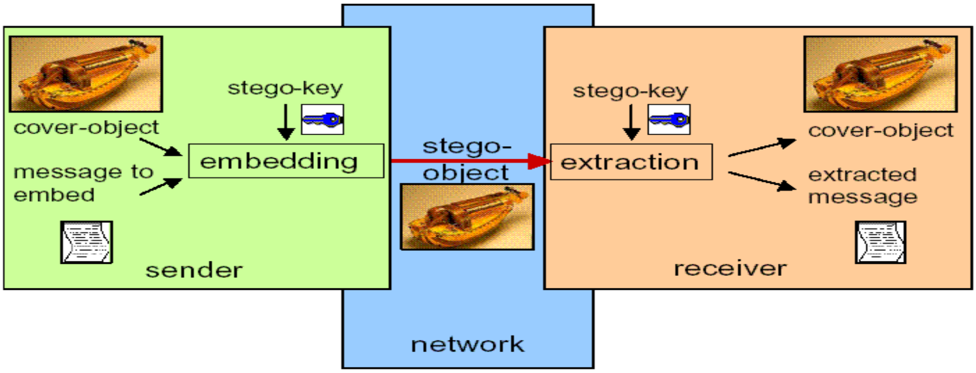


Figure 1: General framework of steganographic system (Navaneet 2012),

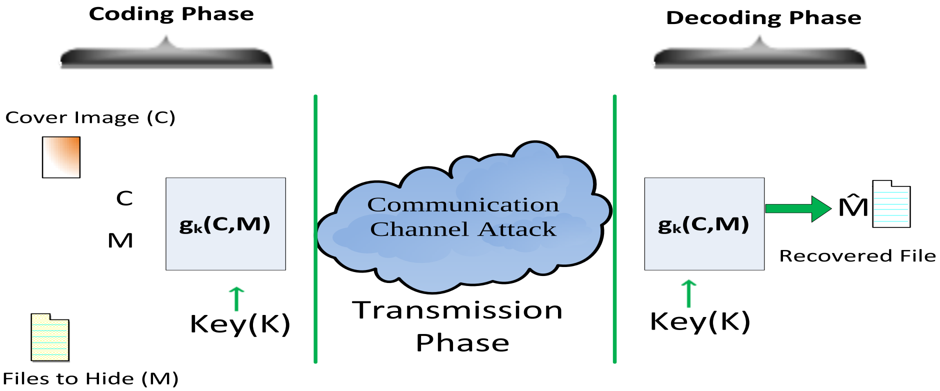


Figure 2: Communication-Theoretic View of steganographic embedding process (Chedad 2009)

In cryptography sensitive messages (called the plaintext) are encrypted into secret form, (called the cipher text) using the encryption key and transmitted across insecure networks in manner such that unintended antagonist cannot read the information except the intended recipient who decrypt the ciphertext using the decryption key (Schryen 2004). Cryptography encompasses many problems including authentication, encryption, key distribution, and decryption. The traditional solution to these problems is 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 $\mathcal{E}$ and *D* as well as common secret *K*, called Key, prior to remote transmission of sensitive information. The adversary may have the knowledge of $\mathcal{E}$ and *D* but does not know K. After the prior meeting, Party A encrypts message M by computing the cipher text $C=E_k(M)$ and sends C to B. Upon reception of an encrypted message *C*, Party *B* decrypts *C* by computing M $= D_k(C)$.The adversary who does not know *K* should not be able to determine message *M* from ciphertext C (PGP Corporation 2003; Hoffstein , Pipher and Silvermann 2008).The process of private key cryptography is illustrated in Figure 3 and Figure 4.

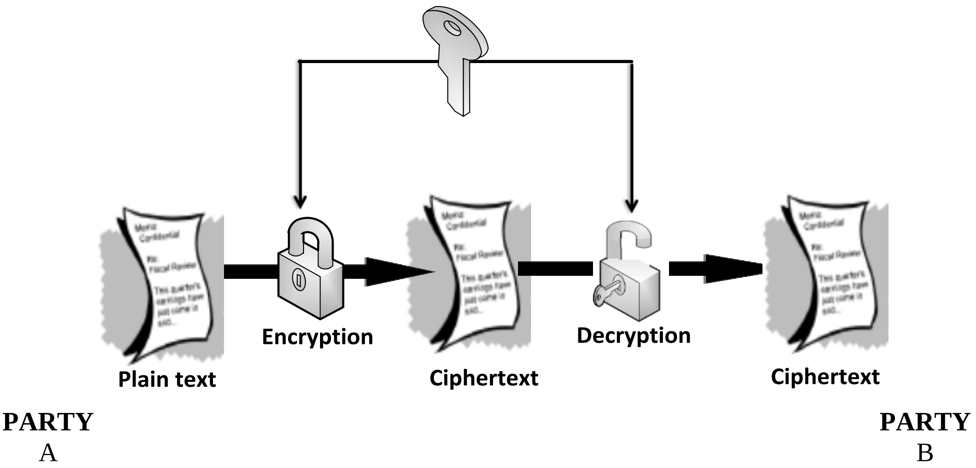


Figure 3: Conventional Cryptographic Process by Encryption (PGP Corporation (2003)

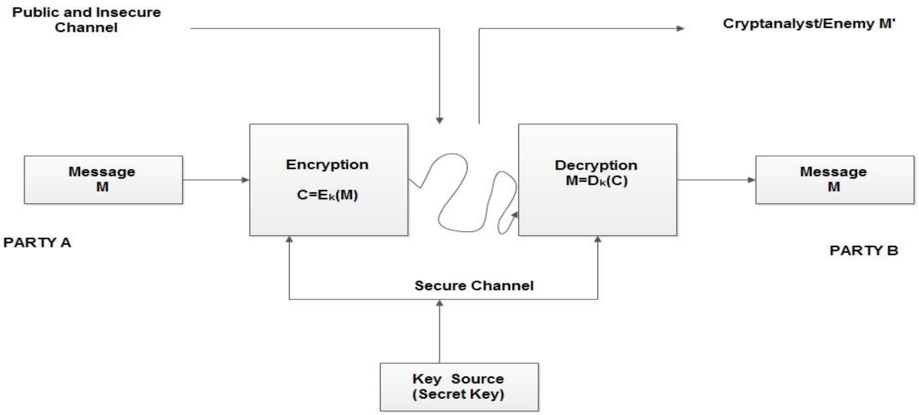


Figure 4: Secret key Cryptographic process by Encryption (Son, 2008))

In Figure 3 and Figure 4, the transformation of encrypted message transferred by party A to party B is entirely dependent on the strength of cryptographic algorithm and the secrecy of Key. The conventional private key cryptographic process is very fast but can be quite expensive due to the difficulty of key distribution (PGP Corporation 2003). The persistent problem of key distribution in private key encryption is solved by Public Key Cryptography (PKC) where a pair of keys is utilized for the cryptographic process. A separate key called public Key is used to encrypt data and the corresponding private key is used for decryption. Examples of Private-key cryptosystems are Data Encryption Standard (DES) and Advanced Encryption Standard (AES).The process of public key cryptography is illustrated in Figure 5 and Figure 6.

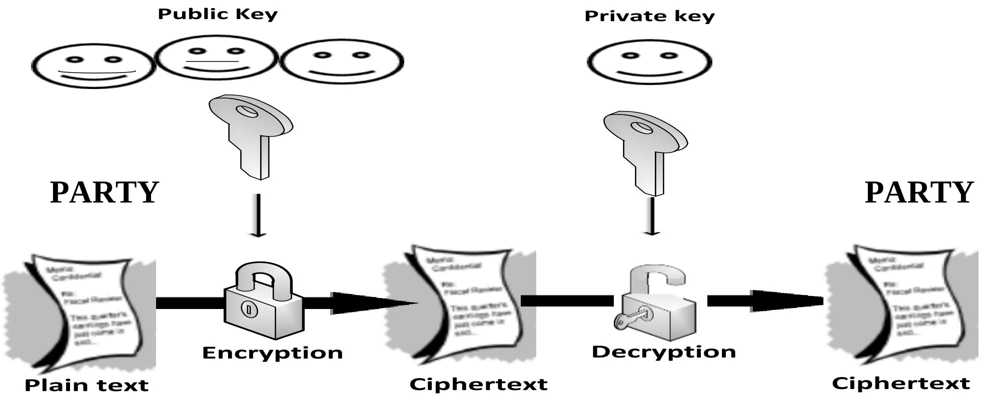


Figure 5: Public Key Cryptographic process (PGP Corporation (2003)

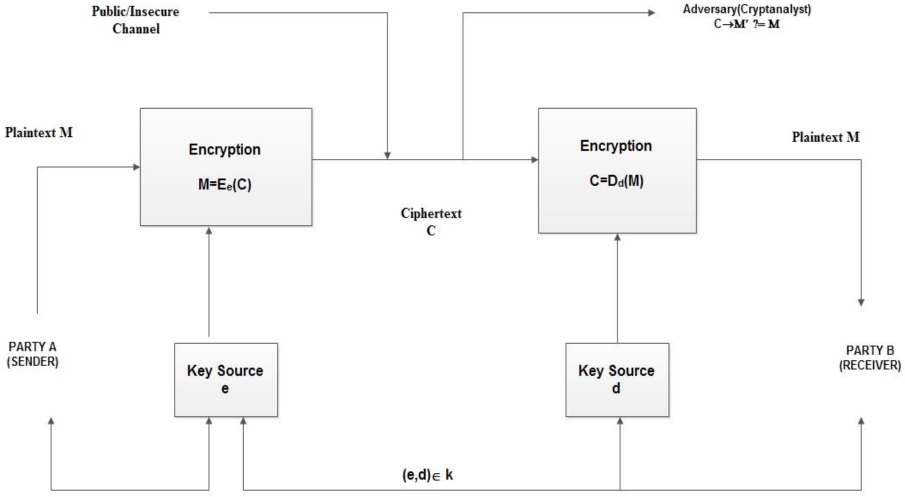


Figure 6: Public Key Cryptographic process (Son ,2008))

In Figure 5, it is computationally infeasible to decode the private key from public key. By default, any party can encrypt information with the public key but only party with private key can decrypt the message. The primary benefit of public-key cryptography is that it allows parties with no pre-existing security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Examples of Public-key cryptosystems are ElGamal, RSA, Diffie-Hellman, and the Digital Signature Algorithm (PGP Corporation (2003).Mathematically, a public-key cryptosystem(CS) may be defined as follows:

$$S = (M, C, K, M, C, e, d, E, D) \qquad (3)$$

Where M is the set of plaintexts, called the plaintext space.
C is the set of ciphertexts, called the ciphertext space.
K is the keys,called the key space.
M ϵ M is a piece of particular plaintext.
C ϵ C is a piece of particular ciphertext
e ≠ d and (e,d) ϵ K is the key.
E is the encryption function defined as:

$$Ee_k \;:\; M \rightarrowtail C \qquad (4)$$

Where M ϵ M maps to C ϵ C, using the public key e_k, such that:

$$C = Ee_k(M) \qquad (5)$$

D is the decryption function defined as:

$$Dd_k \;:\; C \rightarrowtail M \qquad (6)$$

Where C ϵ C maps to M ϵ M, using the private key d, such that:

$$M = Dd_k(C) \qquad (7)$$

Satisfying: $Ee_k Dd_k = 1 \;\; and \;\; Dd_k(C) = \;Dd_k(C) = \big(Ee_k(M)\big) = M$

(8)

The central task of public-key cryptography is to find the suitable one-way trapdoor one way function for both encryption and decryption for authorized users. However, the decryption should be computationally infeasible for an unauthorized user (Schryen 2004). The difference between steganography and cryptography is that the cryptography focuses on keeping the content of a message secret whereas steganography focus on keeping the existence of a message secret. Both are methods of protecting information from unwanted parties with the addition of the former added in most cases to supplement the latter. Message hiding reduces the chance of detecting it. However, if a message is encrypted before hiding it, in such case, if it is discovered then it must be cracked due the provision of another layer of protection-steganography. The combination of Steganography and Cryptography in an application area can achieve better security by concealing the existence of an encrypted message(Shamin and kattamanchi ,2012; Raphael and Sundaram 2012).

3.0 Literature Survey of Cryptographic Models of E-Voting System

In secure e-voting domain, after first cryptographic models for electronic elections were published several schemes have been proposed in literature to deal with the problem of insecurity in electronic voting (Chaum 1981; DeMillo, Lynch, and Merritt, 1982; Benaloh,, 1987). In Okediran, Omidiora, Olabiyisi, and Ganiyu 2011b), four generic cryptographic models (Mix-net, Homomorphic, Blind Signature and the Verifying Secret sharing) for secure electronic voting were compared amongst their core properties: universal verifiability, support for write-in ballot, efficient voting, efficient tallying and large scale election support. Although authors in Okediran *et al.*, (2011b), established that blind signature model is the most efficient cryptographic model for secure electronic voting due to its supports for core properties desirable for secure e-voting, there is tendency for democratic security feature to be defeated, because the voter has an opportunity to vote for more than once. There is need for a modified model based on the scheme to provide additional mechanisms to ensure, that every voter can cast one valid vote only. General framework of cryptographic model to secure electronic voting system is shown in Figure 7. Table 1 shows some related cryptographic models of e-voting systems to enforce security in democratic decision making along with their description, strength and limitations:

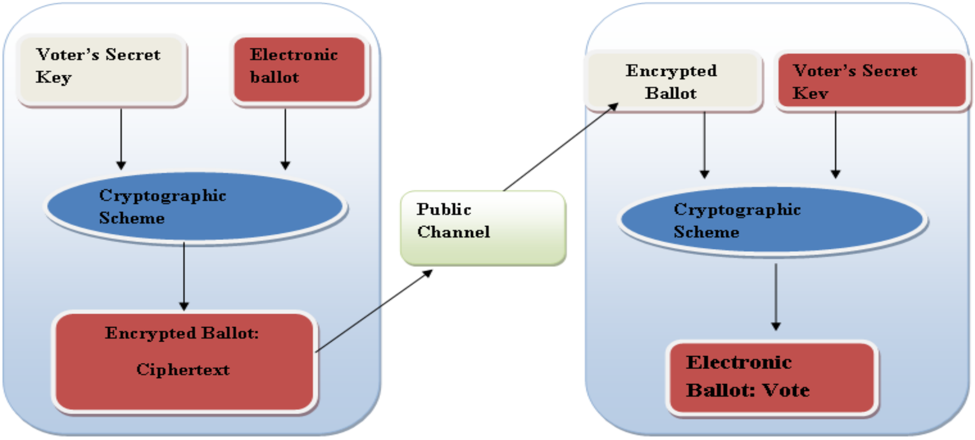


Table 1: Selected Cryptographic Models of Secure E-voting Systems

S/N	DESCRIPTION OF MODEL	CRYPTOGRAPHIC METHOD USED	STRENGTH OF THE MODEL	LIMITATION OF THE MODEL
1	In Okediran *et al.*, (2011a) , proposed the requirement, design and implementation of a generic e-voting system using a number of electronic devices including private computer network, web and mobile phone.	The security considerations of the model were based on RSA encryption algorithm for end to end message security and firewalls in form of proxy server.	The developed model provided ubiquitous voting service to electorate based on public key cryptography(PKC) which offers high flexibility through end to end key agreement protocols and biometric fingerprint authentication mechanism	The model is an authoritative cryptographic model based on RSA with large key size which requires both large amount of computing time and consumes large storage size on both mobile and electronic voting device.
2	In Sodiya *et al.*, 2011, authors designed an architecture for Secure E-voting to ensure privacy, receipt-freeness and non –coercion.	The combination of ECC and El-Gamal Cryptosystem to encrypt voters vote prior to transmission to voting authority for later decryption at	The model explore points from (x,y) coordinates of Elliptic Curve and probabilistic encryption to prevent problems of	The model is authoritative cryptographic model which can compromise the integrity of democratic elections as attention of

		tally phase.	anonymity ,coercion and bribery in E-voting System .	hackers/intruder are drawn to access and attack the vote being transmitted
3	In Purusthomata and Alwyn (2009), authors developed secure internet based e-voting system using Identity based Encryption system to satisfy privacy, anonymity, eligibility, fairness, verifiability and receipt freeness requirements of secure E-voting system.	Authors explore Identity based Encryption cryptosystem using the Unique ID of the voter (National Identity Number) as the public key for encryption. Using the system architecture private Key Generator, the system ensures that only owner has the private key for a typical ID.	The developed model provided effective enterprise key management system for e-voting system by data encryption, user authentication, data decryption, joint management of keys with partners and scaling for future growths	It has limitation as in Sodiya *et al*., 2011.
4	In 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.	Improved on YES/No e-voting protocol proposed by Pardos *et al., (*2007) using bitwise XOR operation for vote generation and blind signature for voter authentication	Strength lies in the denial of all voting authorities (Authentication, Certification and Publication) in knowing neither the ballot content nor any could link ballot to the corresponding voter.	It has limitation as in Sodiya *et al*., 2011 .
5	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.	Leveraged on small-key sized elliptic curve cryptographic algorithm for direct, faster encryption of vote in the mobile device and secure data transfer between the users and the administrator.	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.
6	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).	Authors introduced RSA public –key cryptosystem for Chang and Lee’s (2006) Registration Centre and the proxy server.	Developed a protocol to avert insider attack, Cheating by an administrator, detect and eliminate attack due to denial of Service Limited to Chang and Lee (2006) secure e-voting.	The model is an authoritative cryptographic model and thus limited to 2 above.

7	Gina *et al* , 2010 proposed identity based e-voting cryptographic e-voting protocol based on two bilinear pairing cryptographic 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 developed identity based e-voting cryptographic protocol neither require public key storage nor public key binding management and thus require less computing time to develop cryptographic operations compare to KC protocol.	It has limitation as in Sodiya *et al*., 2011.
8	In Gupta *et al*., (2011), authors proposed a blind signature based cryptographic scheme to provide voter's anonymity and ballot confidentiality in a secure e-voting system.	Used both blind signature to guarantee the voter's privacy and ballot confidentiality and digital signature to authenticate the voter.	The proposed scheme met confidentiality and authentication generic requirement of secure electronic voting system	Provide scope for fraud since a voter has tendency to vote for more than once, defeating democratic security requirement of e-voting.
9	In Patil (2010) was proposed a cryptographic protocol to guarantee voters privacy, authenticity, verifiability and integrity requirements of secure-voting system	Used blind signature, pseudo code and dynamic changing vote to guarantee the voter's privacy and ballot confidentiality as well as digital signature to authenticate the voter	Ensures one man one vote democratic process of governance through the combination of blind signature, pseudo coding and dynamic changing method of voting	The model is an authoritative cryptographic model and thus has limitation as in Sodiya *et al*., 2011.

4.0 Literature Survey of Stegano-Cryptographic Models of E-Voting Systems

The combination of the two principal information security and privacy technologies of cryptography and steganography to the problem of insecurity in an application area evolved stegano-cryptographic modeling technique in literature. In 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. Table 2 shows related stegano-cryptographic models of secure e-voting systems along with their description, strength and limitations:

Table 2: Selected Stegano-cryptographic models of secure e-voting systems

S/N	**DESCRIPTION OF MODEL**	**STEGANO-CRYPTO GRAPHIC METHOD USED**	**STRENGTH OF THE MODEL**	**LIMITATION OF THE MODEL**
1	Authors in Katiyar *et al*.,(2011), 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.	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	The strength of the model lies in stego image whose secret key has been encrypted prior to the hidden process on the fingerprint image cover	The speed of the encryption by hashing with SHA256 for time critical online voting for voter's all around the country and dependence on pseudo random function
2	Authors in Mallick and Kamilla (2011), combined both steganographic and cryptographic techniques to solve confidentiality and integrity security requirements of secure E-service like voting	Employed LSB spatial image domain steganographic technique pre-encrypted with symmetric block cipher with linear algebraic equation.	The model ensures confidentiality and integrity security requirements of an applied E-service area.	The adopted steganographic technique has low 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).
3.	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.	Improved on Katiyar *et al*., (2011), methodology by authentication voters with biometric iris recognition and hashing the secret key with MD5 algorithm prior to embedding both hashed key and voter's identification number to produce final stego image.	Improved the performance and security of similar implementation in Katiyar *et al*., (2011).	The model overdependence on random function.
4	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 uncoercibility, receipt-freeness and universal verifiability by experimentation with two different steganographic tools, F5 and Outguess on five different types of images.	Employed the principles of secret ballot theory, image steganography, visual cryptography and threshold decryption cryptosystems in Java	Proposed a model whose experimentation results show that slight changes exist between the original images and the stego images after secret message is embedded.	Stego medium is unilateral and prone to statistical attack.

5	In Raphael and Sundaram (2012) authors proposed a Stegano-crypto system for covert communication using Unicode symbols.	Encrypt plaintext into text file using Unicode symbols. The generated ciphertext is then compressed with crypto-key which is then hidden in an Image using VB.Net.	Develop a model for larger capacity of covert communication over an open channel	Stego medium is unilateral. Complication in the process of text decryption because the text file contains unicode symbols.
6	In Alok and Atul (2011), authors proposed a Crypto-Stegano scheme for mobile voting.	The scheme is based on face and voice biometric recognition for authentication and ECC Encryption for vote integrity and Image steganography for confidentiality.	The strength lies in the enhanced approach of ECC stego scheme to mobile voting platform.	Stego medium is unilateral.
7	In Swamminathan and Dinesh (2012), authors proposed a model for an online voting system with hybrid of image steganography and SHA 256 hash algorithm for cryptography.	Use LSB Technique of Steganography to embed User PIN, Secret key and voter biometric fingerprint template into cover image.	Reduces the risk of an intruder to locate both the secret key and voter's biometric template on the wireless medium.	Limited to the speed of the encryption by SHA 256 algorithm in does in Katiyar *et al*.,(2011), .
8 .	In Sulthana & Kanmani S (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.	Use RSA Algorithm for cryptography, Video steganography ,face and fingerprint biometrics	Increases voter identification and accuracy of voters for remote registration.	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 both mobile and electronic voting device.
9	Authors in Shamin and kattamanchi (2012) proposed Stegano-cryptographic model for secret data communication in E-service application area like voting	Employed DCT based frequency domain JPEG Image Steganographic Technique and Substitution Cipher for message encryption.	Ensures Confidentiality and Integrity security requirements in secure communication over an insecure channel.	Although the method adopted ensures exhibit difficult level of data detection on transit, DCT based frequency domain adopted steganographic are inflexible and generally do not survive data compressions.
10	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 model improved on methodology proposed in Prabha and Ramamoorthy (2012 and Katiyar *et al*.,(2011) using multimodal biometrics of face and fingerprint and MD5 hashing algorithm. The	The strength 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	Stego object medium is unilateral. Lack non-repudiation requirement of secured e-voting system.

		model authenticates voter's biometric face and fingerprint using principal component algorithms and Gabor filtering algorithms respectively.	security of e- system.	

3.0 Proposed Stegano-Cryptographic Model for Secure E-Voting Systems

From the above mentioned literature survey, it is clear that cryptographic and stegano-cryptographic models have been implemented in e-voting systems to provide fundamental security requirements of confidentiality, integrity, authentication and verifiability/non-repudiation to avert various degrees of rigging, fraud and corruption in the process of democratic decision making. Most attempt to provide these security requirements are in piecemeal during pre-election phase, some proffer solution during election and post election phase. This has established the gap of developing a concurrent, multi-layer (stegano-cryptographic) and multimedia (Image/video) e-voting model for driving future free, fair and credible e-democratic transition in developing country like Nigeria in all phase of electioneering process.

In this research, we propose multi-layer (steganography and cryptography) data security, multi media (Image and video), and Multi -domain (Spatial and Frequency) model to 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 system is based on three-tier client-server architecture of Advancement Structured Information Standard (OASIS) paradigm (OASIS, (2003). 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 8: The Pre-election phase; the Election phase and the Post- election phase.

This architecture provides greater application high flexibility and efficiency, since each tier runs on a separate machine to improve the system performance. The pre-election phase involves the registration of all entities that will enable the outcome of the election, such entities are: Voters information, administrators, Candidates and Parties information, which are all stored in the database. Our proposed Stegano-cryptographic model for secure e-voting system shown in Figure 9 permits eligible electorate (E.g. Greater than or equal 18 years

Nigerian Constitution) registers with an electoral agent at designated registration center. The model assumes that 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.

Three methods of voting are allowed from figure 9: the remote mobile voting, web/internet voting and Kiosk/polls site voting. The mobile terminal voters vote using his credential which is verified using both two-way one-time short message service (SMS) code and accurate response to visual challenge response from the grid. The National Orientation Agency and the Mass Media would have made adequate awareness for these authentication techniques prior to the day of election. 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 system generated picture using modified scattered Least Significant Bit (LSB) spatial image steganographic technique to produce stego-image. For further confidentiality of the vote, the stego- image is further hidden into a video cover using 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).

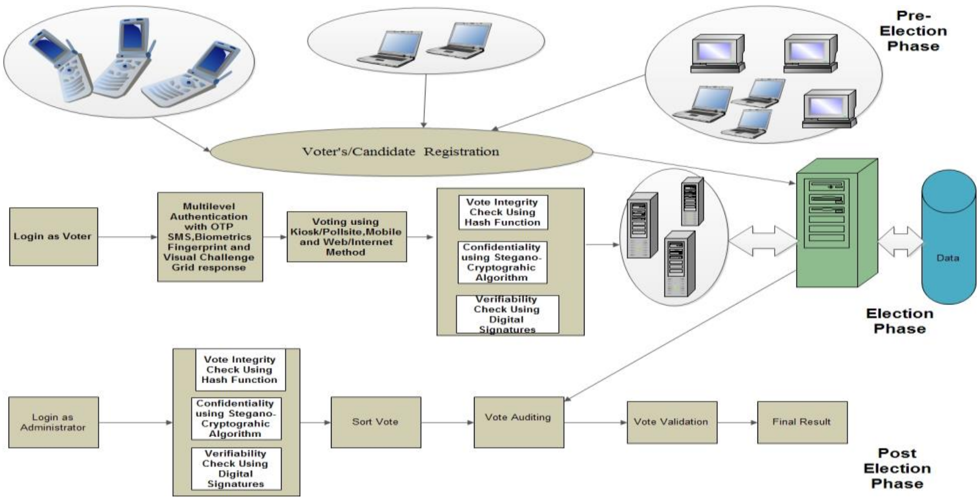
A remote web voter casts vote remotely with the voting device (PC/Mobile device) through the Uniform Resource Locator (URL) address of the secure e-voting system. The voting application runs remotely on the remote voter’s device. The credential of remote web voter is verified using both two-way one-time short message service (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 to produce stego-image. For further confidentiality of the vote, the stego-image is further hidden into a video cover using wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator. A multimedia proposition to similar presentation as does in Katiyar *et al*., (2011).

Consequently, the poll site/Kiosk voters cast their 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. 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 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 from figure 8, the stego video is decrypted using Integer inverse wavelet steganographic technique to extract the hidden ballot in a spatial image. The spatial image is further processed using modified LSB image steganographic algorithm to extract the hidden ballot scattered over the jpeg image for all method of voting (Poll site, Web and Mobile). 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. An improvement to similar presentation as does in Okediran et *al*., (2011a). The concurrent combination 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 (image and video) as shown in Table 3. An improvement to similar stegano-cryptographic model presented in Katiyar *et al*.(2011).

Table 3: Comparison of performance metrics of steganographic techniques

	Spatial Domain	**Transform Domain**	**Spatial/Transform**
Imperceptibility	High	High	**High**
Robustness	Low	High	**High**
Payload Capacity	High	Low	**High**


Pre-
Election
Phase
Voter's/Candidate Registration
Login as Voter
Multilevel Authentication with OTP SMS,Biometrics Fingerprint and Visual Challenge Grid response
Voting using Kiosk/Pollsite,Mobile and Web/Internet Method
Vote Integrity Check Using Hash Function
Confidentiality using Stegano-Cryptograhic Algorithm
Verifiability Check Using Digital Signatures
Data
Election
Phase
Login as Administrator
Vote Integrity Check Using Hash Function
Confidentiality using Stegano-Cryptograhic Algorithm
Verifiability Check Using Digital Signatures
Sort Vote
Vote Auditing
Vote Validation
Final Result
Post
Election
Phase

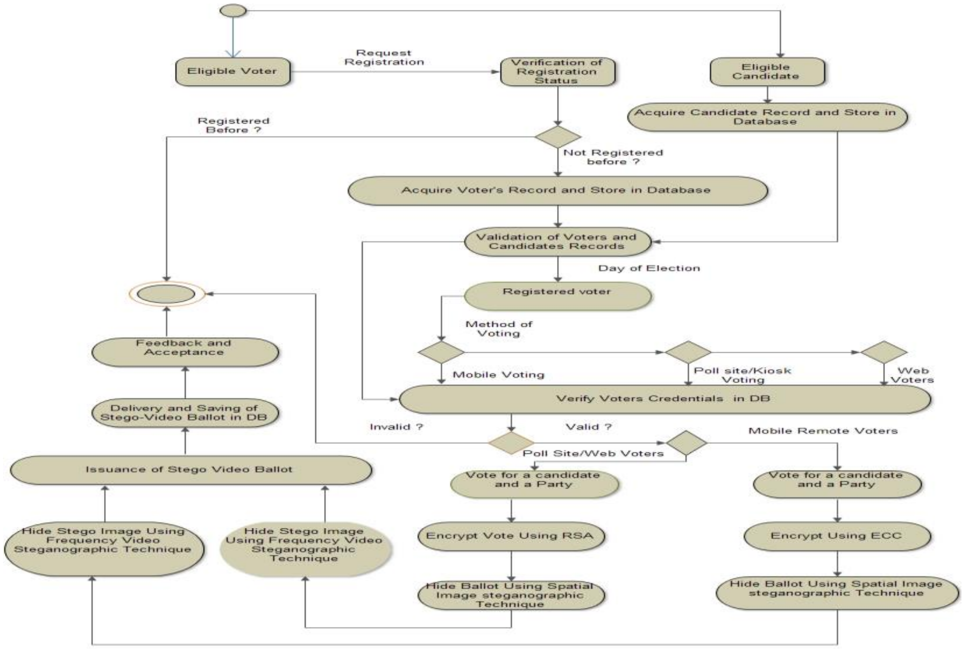

Eligible Voter
Request Registration
Verification of Registration Status
Eligible Candidate
Acquire Candidate Record and Store in Database
Registered Before ?
Not Registered before ?
Acquire Voter's Record and Store in Database
Validation of Voters and Candidates Records
Day of Election
Registered voter
Method of Voting
Feedback and Acceptance
Mobile Voting
Poll site/Kiosk Voting
Web Voters
Delivery and Saving of Stego-Video Ballot in DB
Verify Voters Credentials in DB
Invalid ?
Valid ?
Mobile Remote Voters
Poll Site/Web Voters
Issuance of Stego Video Ballot
Vote for a candidate and a Party
Vote for a candidate and a Party
Hide Stego Image Using Frequency Video Steganographic Technique
Hide Stego Image Using Frequency Video Steganographic Technique
Encrypt Vote Using RSA
Encrypt Using ECC
Hide Ballot Using Spatial Image steganographic Technique
Hide Ballot Using Spatial Image steganographic Technique

Figure 9: Stegano-Cryptographic Model of Secure E-voting System

5.0 Conclusion and Future Work

This paper has provided a comprehensive survey of the existing cryptographic and stegano-cryptographic models for secure electronic voting systems, formulated a platform adaptable framework upon which our proposed multilayer and multimedia model for secure e-voting system can be deployed. The design and development secure e-voting systems for electronic democratic decision making must meet a list of concurrently observed security requirements. Without these requirements; rigging, fraud and corruption in electoral process will ultimately mar the integrity of the electioneering process. Various attempts in literature had proposed and developed secure e-voting systems using cryptographic models, steganographic models and combination of both to these generic security requirements in piece-meal. This has established the gap of developing a concurrent, multi-layer (stegano-cryptographic) and multimedia (Image/video) e-voting model for driving future free, fair and credible e-democratic transition in developing country like Nigeria. The successful implementation and evaluation of the proposed model on the formulated framework would lead to the development of secure e-voting system with high degree of authentication, integrity, confidentiality and auditabillity for the delivery of transparent, free, fair and credible electronic democratic decision making in the developing countries where significant digital divides exist.

In future, the proposed model for secure e-voting system would be implemented on the formulated framework using an appropriate software process models for the development of modified secure e-voting model with the capacity to guarantee and validate voter's for who they are, guarantees the integrity of elections, ensures privacy of the voters, guarantees the confidentiality of the vote and provide mechanism for fraud detection after the electioneering process in developing country like Nigeria where issue of digital divide is significant.

References:

Abo-Rizka M & Ghounam H.R (2007), "A Novel E-voting in Egypt", International Journal of Computer Science and Network Security ,7(11),226-234.

Adeline C.P, Ali K & Hishamnddin (2006),"E-Commerce: A study on Online Shopping in Malaysia", Journal of Social Science,3 (3),231-242

Alok K & Atul K (2011), "A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme", International Journal of Technology and Engineering System (IJTES), 2(1), 8-11.

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

Bloisi, D & Locci, L (2007), "Image Based Steganography and Cryptography", Proceedings of Second International Conference of Computer Visio Theory and Applications (VISAP), 127-134.

Cetinkaya , O & Koc, M,L(2009),"Practical Aspects of DynaVote E-voting Protocol",Electronic Journal of E-Government,7(4),327-338.

Chaum D.(1981),"Untraceable Electronic Mail Return Addresses and Digital Pseudonyms", Communications of the ACM, 24(2) , 84-86.

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

Chedad A. (2009), "Steganoflage: A

new Image Steganography Algorithm", PhD Thesis, University of Ulster, UK.

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

DeMillo, R. A., Lynch, N. & Merritt A. M(1982), "Cryptographic Protocols" ,Proceedings of 14th Annual ACM Symposium on Theory of Computing, 383-400.

Gartner (2013)," E-health for a Healthier Europe", Retrieved online at www.calliope-network.eu/Linkclick.aspx

Gina G. G, Roberto G and Gonzalo I. D. (2010),"Identity based Threshold Cryptography and Blind signatures for Electronic Voting", WSEAS Transactions on Computers, 9 (1), 62-71

Gupta N, Kumar P & Chokar S (2011), "A Secure Blind Signature Application in E-voting", Proceedings of the 5th National Conference, Computing for National Development, pp1-4.

Hoffstein J, Pipher J &Sivermann J (2008),"An Introduction to Mathematical Cryptography", Springer, USA

Ibrahim S, Kamat M, Salleh M, & Abdul Aziz S (2003),"Secure voting using blind signature available at URLhttp://eprints.utm.my/3262/1/IEEE02-EVS_full_paper_ver14Nov.pdf Retrieved on November17th 2011

Linu P & Anilkumar M.N (2012),"Authentication for Online Voting Using Steganography and Biometrics", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 1(10),26-32.

Light J and David .D(2008), "An efficient security algorithm in mobile computing for resource Constrained mobile devices," Proceedings of the 4thACM symposium on QoS and security for wireless And mobile networks, Vancouver, Canada.

Li C and Hwang M (2012),"Security Enhancement of Chang-Lee Anonymous E-Voting Scheme", International Journal of Smart Home, 6 (2), 45-52.

Mallick P K and Kamilla (2011), "Crypto Steganography Using linear Equation, International Journal of Computer and Communication Technology, 2(8), 106-112.

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 November 17th 2011.

Morkel T, Eloff J.H.P & Olivier M.S(2010),"An Overview of Image Steganography", Department of Computer Science, University of Pretoria, South Africa, Retrieved online at http://martinolivier.com/open/stegoverview.pdf on 4th June 2012 on November 15th 2011

Muhalim M A, Subariah I, Mazleena S and Mohd R k(2003), "Information Hiding Using Steganography", Faculty of Computer System and Information System, Department of Computer Science. Retrieved online at http://martinolivier.com/open/stegoverview.pdf on 4th June 2012.

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

Navaneet S. S. (2012),"A model for Performance Enhancement of Steganography through Dynamic Key Cryptography", International Journal of Advanced Networking and Applications:,3(6),1395-1401.

OASIS, (2003)," Election Markup Language (EML) 4.0a", Organization for the Advancement of Structured Information Standards, July 2003.

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 (Journal of IEEE Nigeria Computer Section), 4(2), 9 – 16.

Olaniyi, O.M, Adewumi D.O, Oluwatosin E.A, Arulogun, O. T & Bashorun M. A (2011), "Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance ", African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section), 4(3), 23 – 32.

Olaniyi, O.M, Arulogun, O. T and Omidiora E.O (2012), "Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting ", African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section),5(6), 10 –16.

Olaniyi, O.M, O.T Arulogun, E.O. Omidiora,& Adeoye O (2013),"Design of Secure

Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions" ,International Journal of Computer and Information Technology (IJCIT),2 (6),pp 1122-1130.

Okediran O. O, Omidiora E.O, Olabiyisi S.O, and Ganiyu R A (2011b)," A Comparative Study of Generic Cryptographic models for Secure Electronic Voting", British Journals of Science 1(2), 135-142.

Okediran O. O, Omidiora E.O, Olabiyisi S.O, Ganiyu R A and Alo OO(2011a)," A framework for a Multifaceted Electronic Voting System", International Journal of Applied Sciences,1(4), pp 135-142.

Patil V.M (2010),"Secure Electronic Voting System by Using Blind Signature and Cryptography for voter's privacy and Authentication", Journal of Signal and Image Processing,1(1),pp 1-6.

Pardos A.B.C, Eucins A.H,White S.H,Del Rey A.M & Sanchez G.R(2007),"A Simple Protocol for Yes-No Electronic Voting", International Journal of Computer Science and Network Security,(IJCSNS),7(7),72-76.

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),1-4,Retrieved online at http://www.iccce.co.in/Papers/ICCCECS143.pdf

Purusthomata B.R and Alwyn R P (2009),"Design and Implementation of Secure Internet Based Voting System with User Anonymity using Identity Based Encryption System", Proceedings of IEEE International Conference on Services Computing, IEEE Computer Society, pp 474-481

PGP Corporation (2003),"An Introduction to Cryptography", PGP Corporation, USA

Queensland Governnment (2013)," E-learning for Smart classrooms" Retrieved online at http://gld.gov.au/smartclassrooms/documents/strategy/pdf/scbyte-elearning.pdf n November 17th 2011

Raphael A. J. & Sundaram V., "Cryptography and Steganography – A Survey", International Journal Computer Technology Application, 2 (3), 626-630.

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,Langwi, Malaysia.

Roy A & Karforma S (2011), "Risk and Remedies of E-governance Systems", Oriental Journal of Computer Systems and Technology, 4(2), 329-339.

Roy A , Banik S & Karforma S (2011),"Object oriented modeling of RSA digital signature in E-governance", International Journal of Computer Engineering and Information Technology(IJCEIT),26(1),24-33.

Roy A & Karforma S (2012)," A survey of digital Signatures and Its Applications", Journal of Computing and Information Technology, 3(1),45-69.

Ruther J and Southerton(2000),"E-shopping: delivering the goods? ", Consumer Policy Review, 10(4), 139-144.

Shamin A.L and kattamanchi H(2012)," Secure Data transmission Using Steganography and Encryption Technique", International Journal of Cryptography and Information Security,2(3),161-172.

Song S., J. Zhang, X. Liao, J. Du & Q. Wen(2011), "A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advances in Control Engineering and Information Science, Elsevier Inc, 15,2767 – 2772.

Sodiya A, Onashoga S and D I Adelani (2011), "Secure E-Voting Architecture" ,Proceedings of Eighth International Conference on Information Technology: New Generations, IEEE Computer Society,342-347.

Schryen G, (2004),"Security Aspects of Internet Voting", Proceeding of 37th Annual Hawaii International Conference on System Sciences (HICSS '04), 5, 50-61.

Son Y (2008)," Cryptanalytic Attacks on RSA", Springer, USA.

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, 271-273.

Sulthana S. S & Kanmani S (2011),Evidence based access control over web services using Multi security ,International Journal of Computer Applications ,17(3),pp1-7

Swamminathan B and Dinesh C. D (2012),"Highly secure Online voting system with Multi-security using Biometric and Steganography", International Journal of Advanced Scientific Research and Technology, 2(2), 195-203.

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,474-479.

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