Enhanced Stegano-Cryptographic Model for Secure Electronic Voting

Olaniyi, O.M.
Department of Computer Engineering, Federal University of Technology, Minna, Niger-state, Nigeria
E-mail: mikail.olaniyi@futminna.edu.ng

Arulogun O. T. Omidiora E.O Okediran O.O.
Department of Computer Science and Engineering
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
E-mail: otarulogun@lautech.edu.ng; eoomidiora@lautech.edu.ng ; oookediran@lautech.edu.ng

Abstract

The issue of security in Information and Communication Technology has been identified as the most critical barrier in the widespread adoption of electronic voting (e-voting). Earlier cryptographic models for secure e-voting are vulnerable to attacks and existing stegano-cryptographic models can be manipulated by an eavesdropper. These shortcomings of existing models of secure e-voting are threats to confidentiality, integrity and verifiability of electronic ballot which are critical to overall success of e-democratic decision making through e-voting.This paper develops an enhanced stegano-cryptographic model for secure electronic voting system in poll-site, web and mobile voting scenarios for better citizens' participation and credible e-democratic election. The electronic ballot was encrypted using Elliptic Curve Cryptography and Rivest-Sharma-Adleman cryptographic algorithm. The encrypted voter's ballot was scattered and hidden in the Least Significant Bit (LSB) of the cover media using information hiding attribute of modified LSB-Wavelet steganographic algorithm. The image quality of the model, stego object was quantitatively assessed using Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE) and Structural Similarity Index Metrics (SSIM).The results after quantitative performance evaluation shows that the developed stegano-cryptographic model has generic attribute of secured e-voting relevant for the delivery of credible e-democratic decision making. The large scale implementation of the model would be useful to deliver e-voting of high electoral integrity and political trustworthiness, where genuine e-elections are conducted for the populace by government authority.

Keywords: Electronic Voting, Cryptography, Steganography, Video, Image, Wavelet, Security

1. Introduction

Information and Communication Technology (ICT) as a converged technology of a wide range of services and applications through various types of physical infrastructure and software systems had had a great impact on every facets of modern life. Through ICT revolution, the manner around which man share information about developmental issues has radically been affected. Government, businesses, institutions and individuals have jumped into bandwagon of adopting ICT as part of their organizational processes (Jesus, 2003). The adoption of ICT in governance is aimed at the provision of better information and services to citizens with fewer resources through optimization of available resources and infrastructures. This aim could only be achieved through effective electronic participation (e-participation) between the populace and their governing authorities (Olaniyi *et al.*, 2012).

E-participation is a technology- mediated interaction among the citizens, formal political spheres and central governing spheres. The mission of e-participation is to endow citizen with privileges of ICT to respond in bottom-up decision processes and develop social as well as political responsibility over their choices (Dimitrios, 2011). Citizens' participation in electronic governance could be in the following context: Information provision, consultation, campaigning, deliberation, polling, electioneering and voting using different electronic methods. E-participation through electronic voting (e-voting) is the use of ICT in the context of public voting in elections, referenda or local plebiscites. E-voting as an important e-participatory governmental service has attracted attention as cost effective and electronic decision making alternative to traditional manual method of voting (Olaniyi *et al.,* 2013b). It is viewed as a critical constituent for improving citizen collaboration, enhance and strengthen the democratic processes in modern information societies. Electronic voting is believed to have the capacity to engage citizens in a wider spectrum, than what is currently available in a conventional electoral process through the empowerment of citizens with a means to express their timely opinion on civil affairs such as legislation, and representation. Electronic voting has the capacity to escalate usability and accessibility of the voting process through increase in election turnout while benefiting from transparency and openness in democracy (Dimitrios, 2011).

However, the adoption of e-voting whether in physical presence or at remotes site could be vehicle for electoral fraud, if appropriate information security measures is not in place to protect electoral information, monitor voting administrators from unauthorized access, usage, disclosure, modification and destruction of vital information in all phases of electioneering processes. E-voting systems are classified as a high impact social information system, whose loss of confidentiality, integrity, authenticity and availability could have adverse effect on the credibility of near and future democratic governance (Dimitrios and Dimitrios, 2011).

Consequently, the mitigation of these insecurity threats in e-voting systems has led researchers to formulate different information hiding and privacy models. These models are designed around the principle of cryptography, steganography and watermarking. Cryptography is the science of secret writing between the source and destination while steganography is the science of keeping the existence of hidden message secret. While the former attempted data scrambling for secure communication from an eavesdropper despite his awareness of data transmission; the latter hide the existence of data transmission from the awareness of an eavesdropper for secure data transmission (Olaniyi *et al.,* 2012). Watermarking is an information hiding technique for protection of the copyright of digital product from digital production and data safety maintenance. Its applications range from copyright image communication protection (Quan and Hong. 2008), Healthcare and Telemedicine (Gunjal and Mali, 2012), and in secure e-voting systems (Gunjal and Mali, 2008)

In Olaniyi *et al.,* (2013b), an attempt was made to rigorously survey existing cryptographic and stegano-cryptographic models in literatures for secure e-voting systems around their strengths and limitations. We established that the existing stegano-cryptographic models designed to provide fundamental security requirements of confidentiality, integrity, authentication and verifiability are formulated in piecemeal during pre-election phase, some proffer solution during election and post-election phase. Thus, existing stegano-cryptographic models for secure e-voting are vulnerable to attacks and can be manipulated by an eavesdropper.

In this paper, we present an enhanced stegano-cryptographic model for secure e-voting and perform further quantitative performance assessment of the impercibility and robustness of the model using Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE) and Structural Similarity Index Metrics (SSIM) image quality metrics as anticipated in Olaniyi *et al.,* 2014b and Olaniyi *et al.,* 2014c. The developed model is then compared with similar secure e-voting models in both spatial and frequency domains. An enhanced stegano-cryptographic model for secured electronic voting has been proposed for future e-democratic decision making with the view of increasing participation, confidence and trustworthiness, protects voter's against intimidation, provide sufficient evidence to convince the electorate to vote as a result of conducted, free, fair, credible and genuine e-elections.

The paper is organized into the following sections: Section two presents the concept of stegano-cryptographic modelling in secure e-voting system; Section three presents our enhanced stegano-cryptographic model for secure e-voting, section four discusses our voting procedure; Section five presents an implementation of voting model on mobile e-voting scenario; Sections six presented quantitative performance evaluation of our proposed model. Section seven compares our model with existing models while section eight concludes and recommend gaps for future research endeavor.

2. Concept of Stegano-Cryptographic Modeling in E-voting Systems

The notion of security in social information systems like e-voting is correlated to critical aspects of voters and ballot confidentiality, ballot integrity, voters' authenticity and voting service availability. An e-voting system is said to be unsecured, if an attacker can exploit vulnerability (a weakness) in any phase of electioneering process. To avert insecurity in e-voting systems, researchers have formulated various steganographic techniques, cryptographic techniques and combination of both to block threats through implementation of appropriate counter measures. While steganographic techniques ensure security by hiding voter's intent in an innocuous carrier for covert communication between the voter and voting authority; Cryptographic techniques scrambles voter's intent using an encryption algorithm for secure data communication between the voter and voting authority. 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 steganographic and cryptographic 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).

The concept of stegano-cryptographic modeling technique in secure e-voting systems involved forming a hybrid technique of ensuring ballot confidentiality and integrity through simultaneous combination of covert data communication in steganography with data scrambling for secure communication in cryptography to ensure credible democratic governance. This hybrid relationship from Figure 1 co-exists as a result of mapping between the plaintext **P** and Message **M**, Cipher Text **E** and Stego Media **S** and Cryptographic Key **K** and the Stego Key **K**. The stegano-cryptographic model results as a hybrid model with the addition of a new element: the Stego key **K**, giving the unifying model the cryptographic functionality while preserving the desired steganographic attributes. The hybrid model embedding process yields Stego Media **S** exploiting not only Cover Media **C's** bits but also **K's** in Figure 1.Therefore by Figure 2, Alice (the voter) will have the privilege to embed the secret message M (that is, the plaintext) into the Cover media C (through steganographic process) while encrypting Message **M** by the Cryptographic key **K** (Through cryptographic process) simultaneously (Olaniyi *et al.,* 2012).

At the receiver side, Bob (the voting administrator) will be able to recover Secret Message **M** through Stego Media **S** and Stego **K**. In addition, Wendy (an eavesdropper) will neither detect that Secret Message M is embedded in Stego Media S nor be able to access the content of the secret message (Olaniyi *et al.,* 2012*)*. Figure 2 shows a classical example for an image based stegano-cryptographic model in e-voting systems. For instance in image steganographic application, the integrity of a voter and his vote is assured with the encryption of the message (vote) and then embedding of the encrypted message inside a 24-bit cover image. A secret key used for the stego-system encoder is then passed through the communication channel. At the voters administrator end, the secret key is used to extract the hidden message from the stego-image as shown in Figure 2.

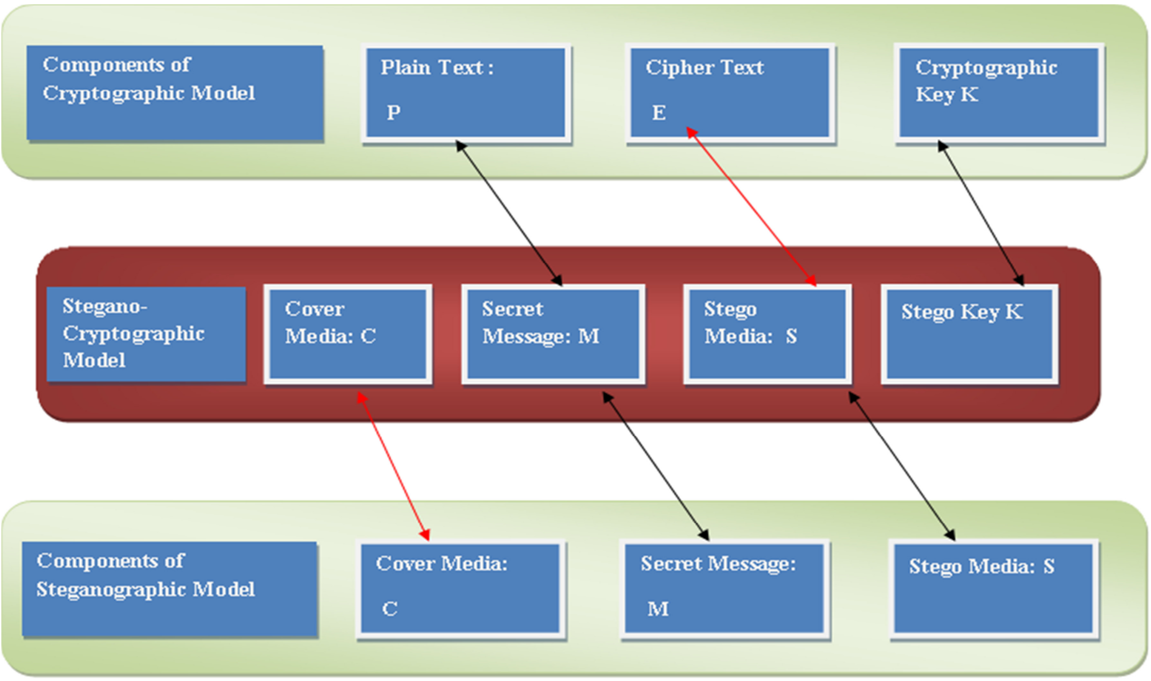


Figure 1: General Stegano-Cryptographic Model Mapping from Steganography and Cryptography (Adapted from (Bloisi and Luca , 2007))

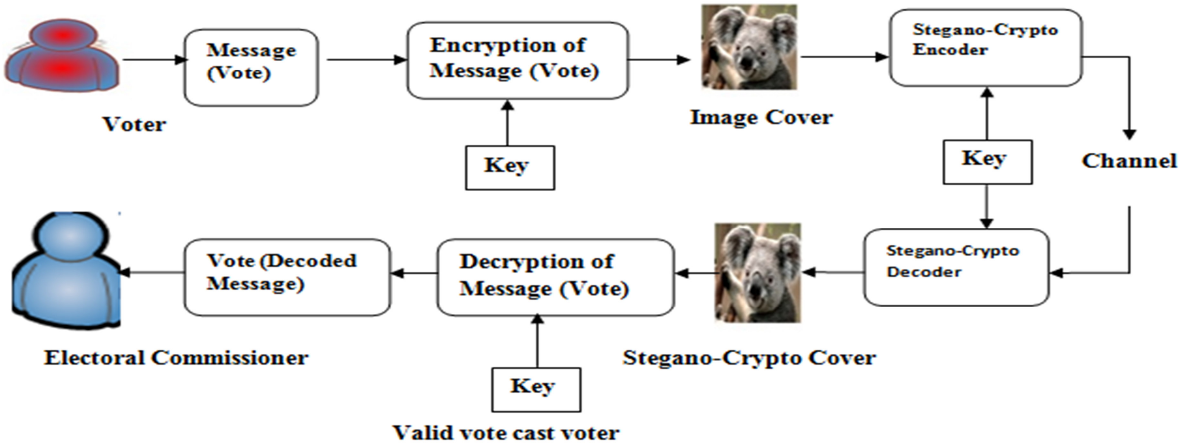


Figure 2: Application of Stegano-Cryptographic Modeling Technique in E-voting (Olaniyi *et al.,* 2012)

3. Proposed Enhanced Secure E-voting Model

The enhanced model for secure e-voting shown in figure 3 improves on katiyar *et al.,* (2011) unimedia stegano-cryptographic model by encrypting electronic ballot using Elliptic Curve Cryptography and Rivest-Sharma-Adleman cryptographic algorithm. The encrypted voter's ballot was scattered and hidden in the Least Significant Bit (LSB) of the cover media using information hiding attribute of modified LSB-Wavelet steganographic algorithm in both spatial and frequency domain for multilayer(steganography and cryptography) , multimedia(Image and Video) and multi-domain (spatial and frequency) secure e-voting modeling for future e-democratic governance.

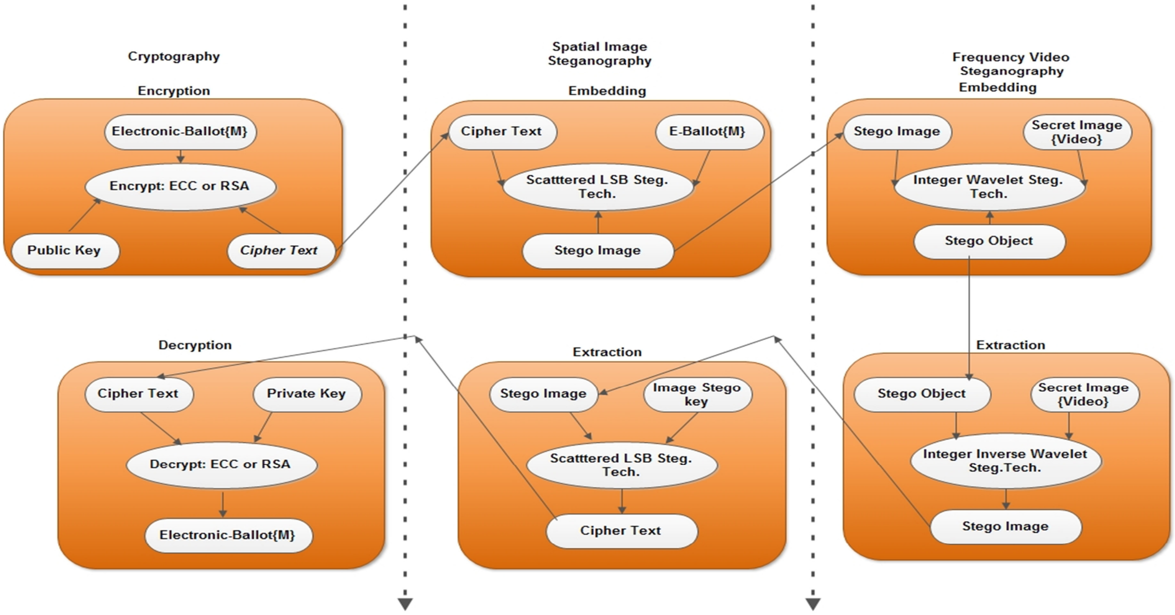


Figure 3: Enhanced Stegano-Cryptographic Model of Secured E-voting Olaniyi *et al.,* (2014c)

As shown in Figure 3, the approach of our image steganographic technique was the modified Least Significant Bit (LSB). The technique consists of two parts namely the embedding and the extraction part. The developed algorithm takes the LSB of the cover medium (*Spatial Image*) and swaps them with a sequence of bytes containing binary equivalent of voters confidential information *(*electronic ballot).

Although, the hiding capacity and impercibility of traditional LSB technique is low considering the statistical features of the stego image in comparison to the original image. The developed embedding algorithm employed modified LSB technique by scattering the bit equivalent of electronic ballot in random bits of the cover image in order to embed the confidential voter's intent. The bit of the cover image to be used for steganography is first extracted to allow for the hiding of the byte values of the text strings randomly in the byte values of the image. To fulfill this objective, the multiplicative congruential random number generation technique was used to generate sequence of random numbers used to match the specific bits in the cover image where the secret bit- electronic ballot are to be hidden.

The multiplicative congruential method is an arithmetic procedure to generate a finite sequence of uniformly distributed random numbers. Two integers P and Q are congruent, if their difference is an integral multiple of m. This is represented as (Prasada, 2010):

$$P \equiv Q \ (mod\ m) \qquad (1)$$

Given that:

i. (P- Q) is divisible by m.

ii. P and Q, when divided by m, leave identical remainders.

Let X_i be the ith uniformly distributed random number, then (i+1)th random number using multiple congruential method is given by relation:

$$\mathrm{X_{i+1}} = \mathrm{a.X_i} \ (\mathrm{mod\ m}) \qquad (2)$$

The following steps were used to implement the generation of random numbers using multiplicative congruential method:

```
1. Begin
2. Get $X_o$(Starting value ),a (Multiplier ),m(Modulus ),N(Total number of random number required )
3. Let $X_i$=Xo
4. For i= 1 to N Repeat step 5 to 6
5. Compute    $X_{i+1} = a.X_i \ (mod\ m)$            // Equation 2 above
6. Print $X_i$
7. End
```

The algorithm developed for generating the uniformly distributed random numbers based on these defined steps are (as presented in equation 2) :

Input: X_o(Starting value),a(Multiplier),m(Modulus),N(Total number of random number required)

```
Output: Sequence of random number,X
        X=Xo
          For i =1 to N Do

            Begin
                          T= a*X
                           Z= T/m
       L(i)= T(int(Z)*m)  //  Equation 2
       X=int(Z)
   Print X
    End
```

The following steps were used to implement the enhanced random LSB image steganographic method:

1. Begin
2. Read the cover image and ciphered message which is to be hidden in the cover image.
3. Calculate LSB of each pixels of cover image.
4. Generate pseudo random number using MCRG method to match the specific bits in the cover image
5. Replace LSB of cover image with each bit of secret message in step 2 using the sequence provided by MCRG generator.
6. Output stego image
8. End

Embedding Algorithm

These steps were transformed to embedding algorithm as:

```
Input: Cover image C, Ciphered message M,
Output: Stego image S
Let LSB($C_{ei}$) =$M_i$ ($M_i$ can be either 1 or 0).
  For i =1 to Length (M)   Do
  Get random pixel of cover elements such that $\{e_{1,}e_{2,} \dots . e_{1m}\}$ using MCRG
        $C_{ei}$=$M_{i}$← LSB ($M_i$) //  Replace $C_{ei}$ with the i^th message bit of M in computed
                                  random pixel of cover image
   End for
 S = $C_{ei}$
```

Extracting Algorithm

The general procedure of extracting encrypted as well as hidden vote is:

1. Begin
2. Read the stego image, S.
3. Calculate LSB of each pixels of stego image.
4. Retrieve cipher text bits
5. Pack the retrieved bit into character.
6. End

The extraction algorithm from above procedure thus is:

```
Input: Stego-image S
Output: Ciphered Message M
For i =1 to Length (M) Do
   $M_i = \ C_{ei}$LSB ($C_{ei}$)
End for
```

The integer wavelet transform (IWT) approach of frequency steganographic technique was used based on the merits reported in Chedad *et al.,* (2008): Hidden messages perceptually invisible, statistically undetectable and difficulty in payload extraction during transit. In order to prevent loss of payload hidden in the stego image in spatial domain, an invertible integer-to-integer wavelet transform (IIWT) is adopted for video frequency steganography. Figure 4a shows the embedding process of merging wavelets decomposition of the normalized 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 3:

$$f(x,y) = \alpha C(x,y) + \beta P(x,y) \qquad (3)$$

$$\propto + \beta = 1 \qquad (4)$$

Where f is modified IWT Coefficients, C is the original IWT and P is the approximation band IWT coefficients of the payload. The fusion parameters α and 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.

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
            Step1: Get a video of extension as input of time two seconds
            Step2: 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 step2.
            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.
```

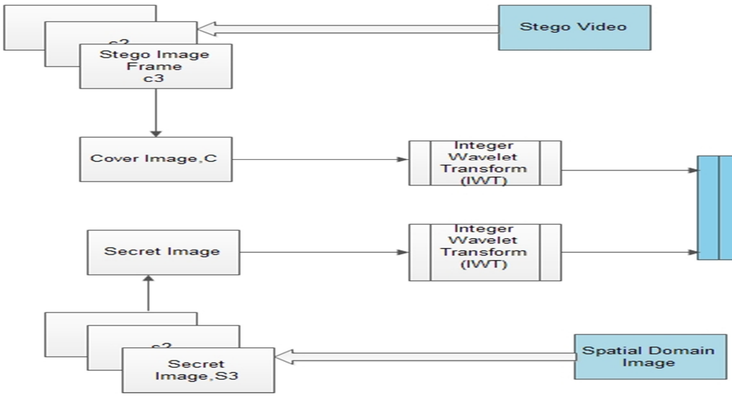
Consequently, Figure 4b shows the retrieval technique for getting the secret image from the stego video (stego image frame). The stego image is normalized and Inverse Integer Wavelet transform (IIWT) is taken. The data extraction process involves subtracting the IWT coefficient of the original cover image, C(x,y), from IWT coefficient of the stego image frame, S, f(x,y) in equation 3 as equation 5.

$$P = f(x,y) - C(x,y) \qquad (5)$$

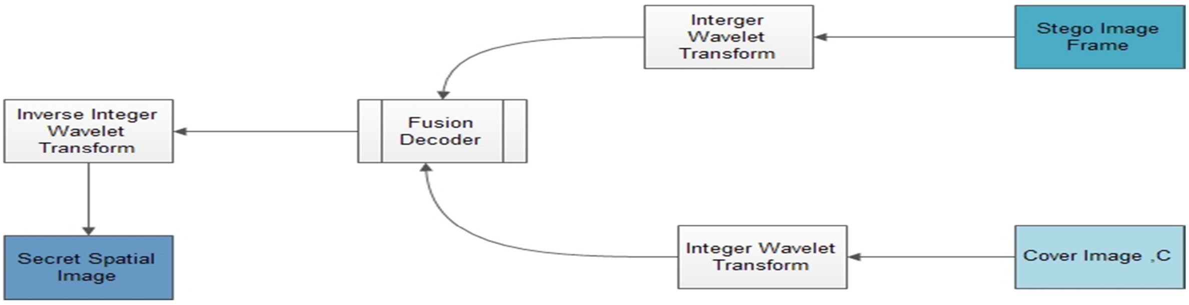
The first step of IIWT on these coefficients is applied by second IIWT in order to retrieve the coefficient of the secret image P as shown in Figure 3.3b.

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 IIWT for the original cover image and the stego image.
            Step 3: Subtract IIWT 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
            Step5: The secret spatial image P is obtained.
```



a: Stego Image Fusion encoding process


Interger Wavelet Transform
Stego Image Frame
Inverse Integer Wavelet Transform
Fusion Decoder
Secret Spatial Image
Integer Wavelet Transform
Cover Image ,C

b: Stego Image Fusion decoding process

Figure 4: Stego object fusion encoding and decoding process (Olaniyi, *et al.,* 2014c)

4. Voting Procedure

In manual paper based voting, the procedure for an election involves, registration, accreditation of voters, voting, collation of ballots, counting and announcement of election results. Similarly, in secure e-voting systems similar procedure is observe with implementation of different information system security techniques and protocols unique to individual proposition. The following steps are the procedure involved in our proposed enhanced stegano-cryptographic based secure e-voting system.

4.1 Registration Phase

The registration stage is the planning stage for preparation towards possible constraints in the entire phase of electoral process. The right of the voters to vote was ensured only eligible voters can accurately cast a vote after successful voter's registration. Each voter would be identified through multifactor authentication: what the voter has (One time pin password), what the voters is (biometric fingerprint) and what the voter accurately respond to (Visual Challenge response to Grid questions) in kiosk, poll sites and remote e-voting scenarios.

4.2 Authentication and Validation phase

Since the model considers e-voting from the lens of kiosk/ poll-site, web and mobile voting scenarios, registered voters would be required to input their unique credentials based on the platform of voting. For kiosk/poll site evoting scenarios, voters would be authenticated through enrolled credentials of one time pin password, biometric fingerprint and accurate response to visual challenge to real time grid questions. The remote e-voting procedure would be authenticated and validated through one time pin password and accurate response to visual challenge to real time grid questions for proper level of trust between the voter and the system. The voter would be privileged to vote immediately their credentials are authenticated and validated as who they claim they are.

4.3 Voting Phase

This embraces the selection of voter's candidate by the voter as well as the process of sending the electronic ballot to the server. Our enhanced model for secure e-voting presented in section three for electronic ballot scrambling and embedding in image and video cover both in spatial and frequency domain are used protect the voter's intent as stego object from an eavesdropper or an attacker for kiosk, poll sites and remote e-voting scenarios. This process is shown in UML activity diagram of enhanced stegano-cryptographic model for secured e-voting of Figure 3 in Figure 5.

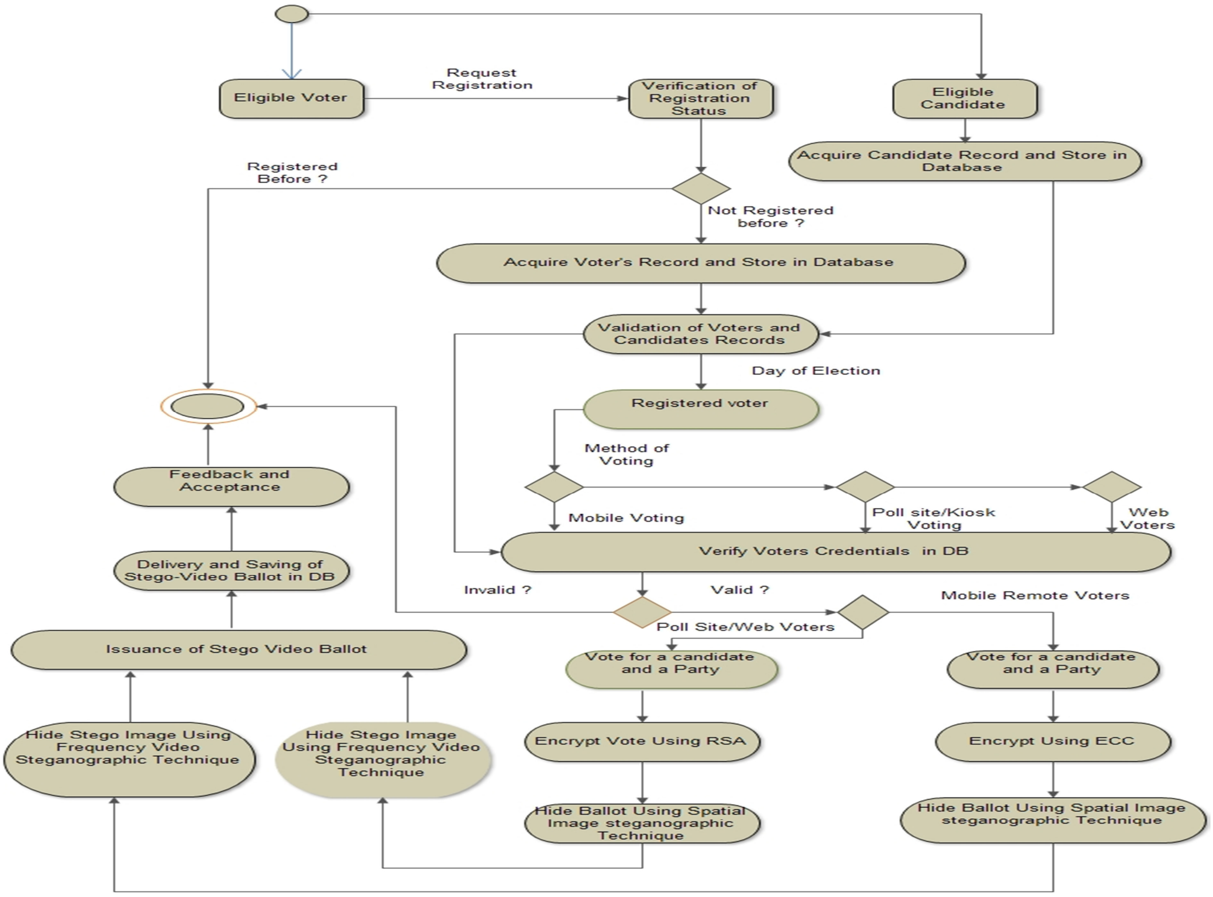

Eligible Voter
Request Registration
Verification of Registration Status
Eligible Candidate
Acquire Candidate Record and Store in Database
Registered Before ?
Not Registered before ?
Acquire Voter's Record and Store in Database
Validation of Voters and Candidates Records
Day of Election
Registered voter
Method of Voting
Feedback and Acceptance
Mobile Voting
Poll site/Kiosk Voting
Web Voters
Verify Voters Credentials in DB
Delivery and Saving of Stego-Video Ballot 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 5: UML activity diagram of enhanced stegano-cryptographic model for secured e-voting in Figure 3 (Olaniyi, *et al.,* 2014c)

4.4 Tallying

In this stage, each collected electronic ballot technically referred to as stego object, is first extracted using the wavelet steganographic algorithm to yield a stego image. The stego image is further processed with LSB steganographic algorithm to yield an encrypted cipher text containing the hidden electronic voter bit for extraction using either RSA or ECC depending on the platform of voting. The extracted votes are then collated by an administrator for publication to the electorate.

4.5 Publishing and Ballot verification

In classical paper based voting, the announcement of the result of the election succeeds the tallying process. In secure e-voting system based on our enhanced model, the integrity of extracted vote while in transit is ensured by validating an altered vote during transit at the post-election phase by encoding the vote with a private key. The process involves comparing the result of each electronic ballot by comparing the encrypted vote added the ballot to the hashed vote. The encrypted vote is decrypted and then hashed using SHA256 hashing algorithm. If the hashed result matches with the hashed function sent during voting phase, the system (the server) would automatically update the user's vote by one, else, the vote would be regarded as to have been hacked while in transit, hence, vote would not be counted for the user(Olaniyi, *et al.,* 2013a). This ballot integrity procedure is shown in Figure 6. Also, voters can also secretly verify whether their vote is among the collated vote for final declaration of result. In this manner, the fundamental security requirements of authentication, integrity, confidentiality and verifiability has been achieved as neither the voters nor the election administrator has access to identify the collected electronic ballots.

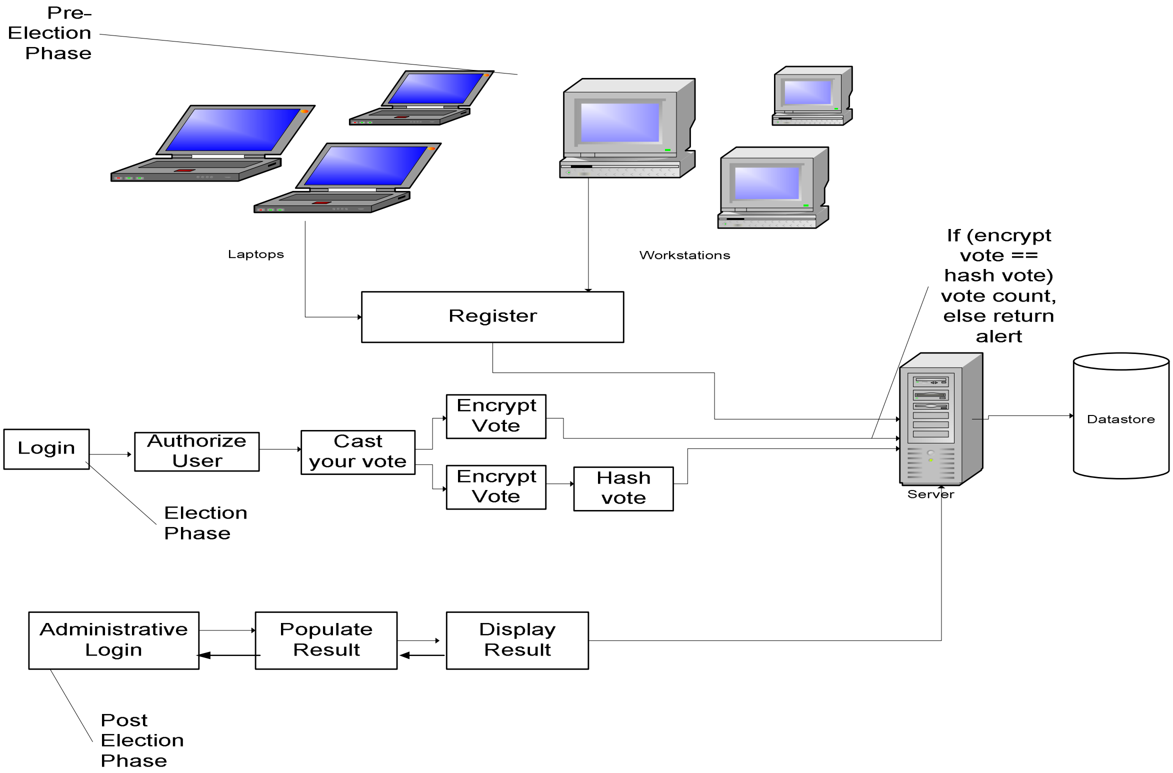


Figure 6: Vote Integrity check of extracted electronic ballot (Olaniyi, *et al*., 2013a)

5. System Implementation

The model was simulated using JAVA Programming Language and Oracle 10g Database Management System (DBMS). Selected qualified voters were asked to enroll data for remote mobile e-voting scenario through interaction with the sample secure e-voting system Graphical User Interface (GUI) presented in Figure 7. The detailed system implementation of the enhanced model for both kiosk and poll- site e-voting scenarios have been presented in Olaniyi *et al.* (2014c). The system (GUI) of the mobile voting system based on the developed model required the voters to enroll their unique physiological biometric fingerprint, their personal data during registration phase prior to voting using their mobile devices.

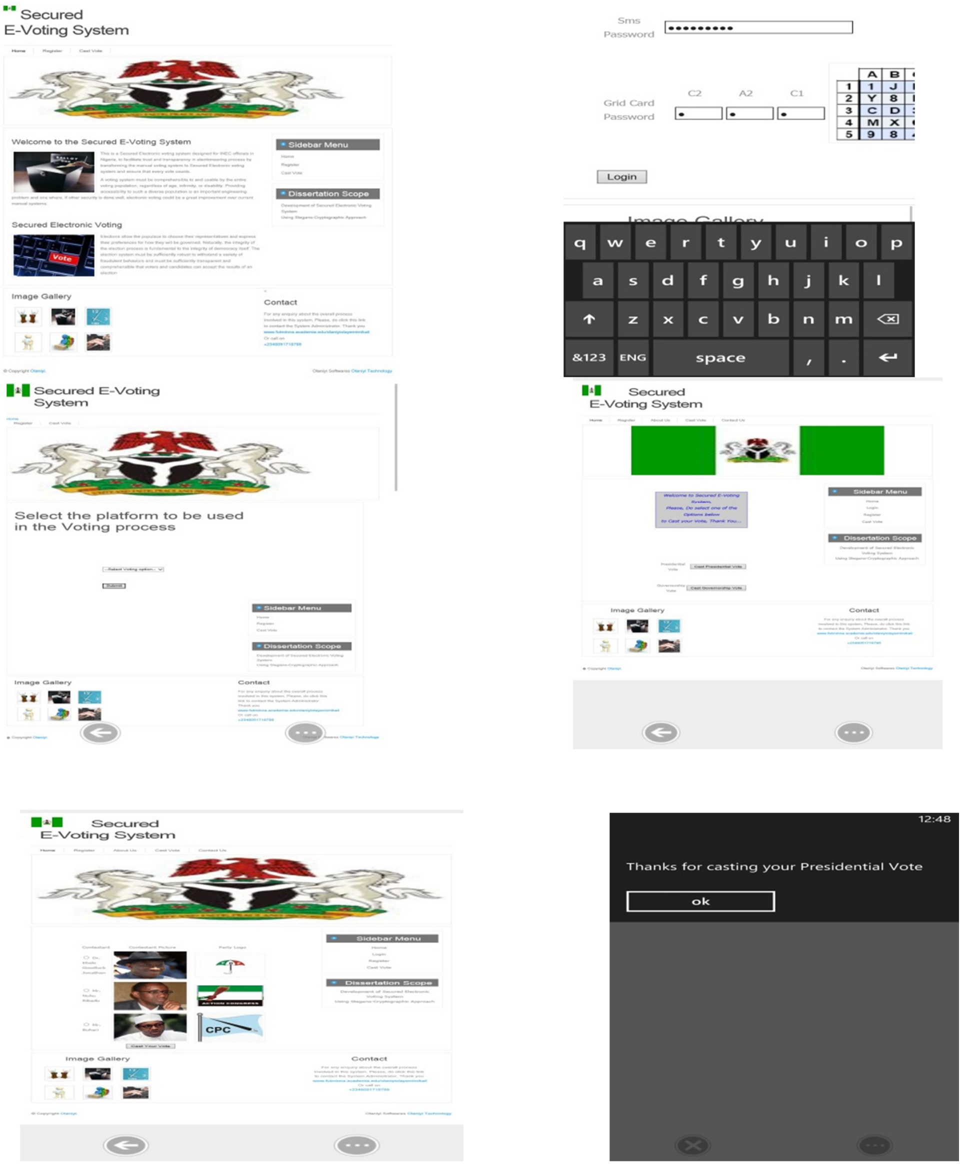

Secured E-Voting System
Welcome to the Secured E-Voting System
Secured Electronic Voting
Sidebar Menu
Dissertation Scope
Image Gallery
Contact
Sms Password
Grid Card Password
C2
A2
C1
Login
Select the platform to be used in the Voting process
Thanks for casting your Presidential Vote
ok
12:48

Figure 7: The Mobile Client end of the enhanced stegano-cryptographic based Secure Voting System

6. Model Performance Evaluation

The performance measure of steganographic systems are measured along three key parameters: imperceptibility, robustness and payload capacity and the stability of the stego media against detection using steganalytic detectors (Nagham *et al.,* 2012; Olaniyi *et al.,* 2014b ; Olaniyi *et al*., 2014c). These three key parameters are defined as:

a) Imperceptibility**:** The ability to avoid detection i.e. where the human visual fail to notice it. Impercibility parameter is the primary requirement of a steganographic technique. Truly secure steganographic technique should be imperceptible neither by human eye nor by statistical attacks (Nagham *et al.*, 2012).

b) Robustness: This is the ability of steganographic technique to survive the attempts to remove the hidden information through attempts like cropping, rotation (in cover medium like image), data compression and filtering.

c) Payload Capacity: Payload refers to information that can be hidden in cover media during steganographic process. Payload capacity therefore refers to the maximum amount of information that can be hidden and retrieved successfully.

Performance evaluation of our enhanced model was accomplished both quantitatively and qualitatively. Quantitatively through computation of SSIM stego image quality metrics value for different stego image pixel dimensions using ImageJ, Image processing environment. Qualitatively using five-point likert psychometric analysis, descriptively analysed in Statistical Package for Social Sciences (SPSS) through assessment of users perceptive of secure e-voting system based on the developed stegano-cryptographic e-voting technique. In Olaniyi *et al.,* 2014a; Olaniyi *et al.,* 2014b and Olaniyi *et al.,* 2014c preliminary quantitative and qualitative performance evaluation of our model have been carried out respectively.

In this section, further quantitative performance evaluation of the confidentiality requirements of secure e-voting model was evaluated based on assessment of stego image quality. The assessment the quality of the developed model stego Image was accomplished through computation of Root Mean Square Error (RMSE), Signal to Noise Ratio (SNR), Peak to Signal Noise Ratio (PSNR) and full referenced multi-indexed Structural Similarity Index metrics (SSIM) between the distorted image – the stego image and its reference image cover image for index levels of 0 to 3 using SNR and SSIM plugin in ImageJ Image processing environment. ImageJ program is a Java based Image processing application for editing, analysing and processing color and gray scale Images. Our findings of the assessment of the stego Image quality (shown in Figure 8) using RMSE, SNR,PSNR and full referenced, multi-index Structural Similarity Index metrics (SSIM) between the distorted image (stego image) and its reference image cover image is shown in Table 1. Considering SNR and PSNR similarity metrics in Table 1, increase in security of multilayer and multi-domain e-voting model is inversely proportional to image size, with both values of PSNR and SNR increasing with decrease in pixel value of image. This signifies the e-voting model is secured from theoretical perspective: high PSNR value indicates high image quality.

BELLS UNIVERSITY OF TECHNOLOGY
CHORDS OF KNOWLEDGE
BELLS UNIVERSITY OF TECHNOLOGY
CHORDS OF KNOWLEDGE

A: Cover Image (8-bit, Grayscale)

B: Stego Image(8bit Grayscale)

Figure 8: Cover and Stego Image in Grayscale.

Table 1: Comparison of various quality measurements on stego image and cover image

Cover Image	Stego Image	SNR[dB]	PSNR[dB]	RMSE [dB]	SSIM(at level 0)	SSIM(at level 1)	SSIM(at level 2)	SSIM(at level 3)
Bellslogo.jpg 512*512	Bellslogo.jpg 512*512	50.118	56.015	89.136	0.7706	0.5700	0.7214	0.7698
Bells logo.jpg 256*256	Bellslogo.jpg 256*256	51.909	57.840	83.109	0.8179	0.7191	0.7504	0.8011
Bells logo.jpg 128*128	Bellslogo.jpg 128*128	55.569	61.566	72.030	0.8989	0.8075	0.8457	0.9056
Bellslogo.jpg 64*64	Bellslogo.jpg 64*64	63.963	70.097	50.025	0.9459	0.8847	0.9185	0.9569

Also, considering the limitations of PSNR, SNR and MSE image quality metrics: Inability to assess effectively image similarity across distortion types and inability to matched perceived visual quality (Vincent and Adepoju 2013; Mittal, *et al*., 2013; Wang *et al*., 2004), necessitated the computation of full reference Structural Similarity Index metrics (SSIM) at index level of 0 to 3 of the stego image in Table 1. According to Aibinu *et al.,* (2008), For two images x and y of common size N*N, SSIM is given as:

$$SSIM(x,y) = ((2\mu_x\, \mu_y \;+\; C_1)(\,2\sigma_{xy} + C_2\,))/((\mu_x^2 \;+\; \mu_v^2 \;+ C_1\,)(\,\sigma_x^2 + \sigma_y^2 \;+ C_1\,)) \qquad (6)$$

$$SSIM = [-1,+1] \qquad (7)$$

The best value 1 is achieved if and only if the two images are similar and -1 if the two images are highly un-similar (Aibinu *et al.,* 2008). From equation 7, the increase in index value from 0 to 3 made computed SSIM value to 1 (from 0. 0.8989 to 0.9056 in Bellslogo.jpg of 128*128) indicating greater fidelity of stego image closeness to the original cover image, hence the developed e-voting model is imperceptibly secured.

7. Comparative Assessment with other Similar models of e-voting systems

The developed enhanced stegano-cryptographic model for secure e-voting was compared with other existing methods in literatures, in spatial domain like Rura *et al.,* 2011,Katiyar *et al.,* 2011, and Prabha and Ramamoorthy (2012),Kamau *et al.,*2013 and in transform domain like Shamin and kattamanchi (2012). From the comparative study, it can be concluded that the developed e-voting model is better in terms of high impercibility of stego image, high robustness to survive attempts to remove the hidden data, moderate PSNR values and qualitative SSIM values compare to existing stegano-cryptographic e-voting model in literature.

Table 2 and Table 3 show the comparison of the developed modified stegano-cryptographic model for e-voting with other existing e-voting model in different domains. Table 4 shows the numerical comparison of PSNR metric values with existing e-voting models. The developed model is 37.58% and 16.14% better than Shamin and kattamanchi (2012) and Kamau *et al*., (2013) in frequency and spatial domain respectively.

Table 2: Comparison of the developed e-voting model with other spatial domain method

S/N	**Paramater of Comparison**	**Rura *et al.,* 2011,Katiyar *et al.,* 2011, Prabha and Ramamoorthy (2012) and Kamau *et al*., (2013)**	**The developed e-voting model**
1	**Attack on Image**	Because all are e-voting model based on spatial domain techniques.,data are easily easily tractable from raw pixel intensities and falter for most types of image attacks.	Since the model embraces further transform domain layer on the spatial stego image using wavelet techniques, extraction from wavelet coefficients is far more complex and robust with chosen jpeg image.
2	**Image compression factor**	All e-voting models embraces only uncompressed image	The model works on both uncompressed and compressed image.
3	**Performance evaluation factor**	Rura et al evaluated only with histogram level;Katiyar et al and Prabha and Ramamoorthy (2012) evaluated only with the speed of hash function which cannot effectively established the security of the scheme for e-voting.	Model was evaluated qualitatively with RMSE, SNR,P SNR and SSIM standard image quality metrics with high level of imperceptibility index rate and quantitatively with pyschometric analysis with high rate of user's perceptive rating.
4	**Test of the hidden data security**	Secuirty of the idden data not tested.	Security of tested hidden data using steganalysis was very high.

Table 3: Comparison of the developed e-voting model with other DCT domain method

S/N	**Paramater of Comparison**	**Shamin and kattamanchi(2012)**	**The developed e-voting model**
1	**Method of transformations**	The model embraces transform domain techniques by modifying DCT coefficients.	The developed evoting model embraces the modification of both scattered LSB spatial image and wavelet frequency coefficients.
2	**Image compression factor**	The model works only on uncompressed image	The model works on both uncompressed and compressed image.
3	**Security of hidden data**	Security of the hidden data tested with PSNR metric	Security of tested hidden data using steganalysis and SNR,PSNR and SSIM Image quality metrics

Table 4: Numerical Comparison of the PSNR Metric values of the developed e-voting model with other Exiting E-voting Models/Technique

S/N	Similar E-voting Model/Technique	PSNR Computations(dB)	Percentage of Comparison (%)
1	Kamau, Kimani and Nwangi (2013)	58.78	***16.14***
2	Gunjal and Mali (2012)	54.32	***22.50***
3	Shamin and kattamanchi (2012)	43.75	***37.58***
4	Mallick and kamilla (2011)	42.77	***38.98***
5	The developed Model	**70.09**	

8. Conclusion and Recommendations

The design of e-voting systems for electronic democratic decision making must embody a list of generic security requirements of authentication, confidentiality, integrity and non-repudiation. Without these requirements, rigging, fraud and corruption in electoral process will ultimately mar the integrity of the electoral 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 had established 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 this paper, an enhanced stegano-cryptographic e-voting model has been developed for an architectural framework of secure e-voting in poll site, web and remote mobile voting scenarios. This was achieved using Software Engineering, Information Hiding techniques and Information Systems Design approaches by careful combination of evolutionary spiral and unified process software process models.

A secured e-voting system was modeled and developed on the Stegano-Cryptographic e-voting model for pre-electoral, electoral and post electoral processes where voter's registration, ballot casting and vote audition were accomplished on mobile platforms. The performance of developed e-voting model was quantitatively evaluated on the secure e-voting system application for fundamental security requirements of e-voting. The developed model is 37.58% and 16.14% better than Shamin and kattamanchi (2012) and Kamau *et al.*, (2013) in frequency and Spatial domain respectively. The result of the evaluation shows that the developed e-voting model has an appreciable attribute 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.

The enhanced secure e-voting model was developed to address these fundamental security issues to e-voting in developing countries with peculiar and massive access to high end infrastructural ICT facilities. Therefore, it is recommended that government organizations like Independent National Electoral Commission (INEC) in Nigeria should embrace the findings of this research to facilitate credible, transparent, free and fair e-democracy in future elections.

Future research in the field of security in electronic voting should look at the following open issues: 1) Security of e-voting system 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. 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 system. 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. With the achievement of above recommendations, government and its election authority could increase public participation, political trust and confidence while solving security problems in e-democratic decision making in future elections.

References

Aibinu A., Najeeb A.R, Salami, M. J., and Shafie, A. A. (2008), "Optimal Model Order selection for Transient Error Autoregressive Moving Average (TERA) MRI Reconstruction Method ",World Academy of Science,Engineering and Technology(WASET) Journal,Vol.42, pp 161-165 Retrieved from *http://irep.iium.edu.my/5452/1/Optimal_Model_Order_Selection_for_Transient_Error.pd*f

Bloisi, D. and Locci, L. (2007), 'Image Based Steganography and Cryptography': In

Proceedings of Second International Conference of Computer Vision Theory and Applications (VISAP), Barcelona, Spain, Vol. 1,pp 127-134.

Cheddad, A., Condell, J.,Curran, K. and McKevitt, P. (2008),'Security Information Content Using New Encryption method and Steganography': In Proceeding of the Third IEEE International Conference on Digital Information Management (ICDI 2008), University of East London ,UK, pp. 563-568.

Dimitrios, Z.(2011)," Methodologies and Technologies for Designing Secure E-voting Information Systems", PhD Thesis, University of Aegean,Greece.

Dimitrios, Z. and Dimitrios, L. (2011)," Securing e-Government and e-Voting with an Open cloud", Government Information Quarterly, Vol.28, pp239-251.

Gunjal, B.L. and Mali, S. N. (2008), "Applications of Digital Watermarking in Industries", Computer Society of India (CSI) Communications, Vol.36 No.6, pp 5-7

Gunjal, B.L. and Mali, S. N. (2012), "Secure E-Voting System with Biometric and Wavelet based Watermarking Technique in YCgCb Color space", Proceedings of IET International Conference on Information Science and Control Engineering (ICISCE 2012), pp1-6

Kamau, G.M., Kimani, S. and Nwangi, W. (2013), "A General Purpose Image-Based Electors Smart Card Using an Enhanced Least Significant Bit Steganographic Method for Information Hiding: A case study of the Kenyan Electoral Process", International Journal of Computer Science Issues (IJCSI), Vol. 10 No.1, pp. 339-347.

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.

Mallick, P.K. and Kamilla, N.K. (2011), "Crypto Steganography Using Linear Equation, International Journal of Computer and Communication Technology, Vol. 2 (8), pp106-112.

Mittal, A., Soundararajan, R.and Bovik, A. C. (2013),"Making a Completely Blind Image Quality Analyzer", IEEE Signal Processing Letters, Vol. (22)3,209-212.

Nagham H, Abid Y, Ahmad R, and Osamah M. (2012),"Image Steganography Techniques: An Overview", International Journal of Computer Science and Security, Vol. 6 (3),pp 168-187

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 ICTs, Vol. 4(3), pp 23 – 32.

Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & 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, O.T Arulogun, E.O. Omidiora, & 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.

Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O (2014a), "Performance assessment of an imperceptible and Robust Secured E-Voting Model ", International Journal of Scientific and Technological (IJSTR), Vol. 3 No.6, pp.127-132.

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

Olaniyi O.M., O.T Arulogun, E.O. Omidiora, & Okediran O.O (2014c),"Implementing generic security Requirements in e-voting using modified Stegano-cryptographic Approach", International Journal of Information and Computer Security (IJICS), Inderscience Publishers, *In press*

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(ICCCE2012),1- 4, Retrieved online at http://www.iccce.co.in/Papers/ICCCECS143.pdf

Prasada, R.G (2012), "Random Number Generation and its better Technique", MEng Disseration, Thapar University, Patiala, India.

Quan, L and Hong L (2008)," Application of Digital Watermark and Mobile Agent in Copyright Protection System", Proceedings of IEEE International Conference of Computer Science and Information Technology , Singapore, pp1-4.

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),Malaysia, pp 80-85.

Shamin A.L and kattamanchi H (2012)," Secure Data transmission Using Steganography and Encryption Technique", International Journal of Cryptography and Information Security, Vol.2 No 3,161-172.

Jesus M (2003)," The Importance of ICT for developing Countries", Interdisciplinary Science Reviews", Vol. 28 No.1 pp 10-14.

Wang, Z , E. P. Simoncelli, and. Bovik, A. C, (2003), "Multi-scale Structural Similarity for Image Quality

Assessment," In Proceedings of IEEE Conf. Signals, Systems and Computers, vol. 2, pp. 1398–1402.

Vncent O.R and Adepoju O. K.. (2013)," On Image quality assessment Using Structural Similarity Index", Proceedings of the 11th International Conference on Electronic Government and National Security, Nigeria Computer Society(NCS),pp 104-109.

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 B. Tech in 2005 and M.Sc. in 2011 in Computer Engineering and Electronic and Computer Engineering respectively. He had his PhD in Computer Science (Computer and Information Security) from the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria in 2015. He has published in reputable journals and learned conferences. His areas of research includes: Information and Computer Security, Intelligent Systems, Embedded Systems and Telemedicine.

Oladiran T Arulogun is an Associate Professor 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 B.Sc. Computer Engineering in 1991. He obtained his M.Sc. and Ph.D 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 B.Tech. Computer Engineering, M.Tech. and Ph.D in 2002, 2008 and 2011 respectively. He has published in reputable journals. His research interests include: Computational optimization, e-commerce, biometrics- based algorithms and their applications to e-voting systems