ISSN 2320 2610
Volume 3, No.1, January – February 2014
International Journal of Multidisciplinary in Cryptology and Information Security
Available Online at http://warse.org/pdfs/2014/ijmcis01312014.pdf

Performance Evaluation of modified Stegano-Cryptographic model for Secured E-voting

Olaniyi, O.M[1], Arulogun O. T[2]., Omidiora E.O[2], Okediran O.O[2]
[1]Department of Computer Engineering
Federal University of Technology
P. M. B. 65, Minna, Niger-state, Nigeria
E-mail: mikail.olaniyi@futminna.edu.ng
[2]Department of Computer Science and Engineering
Ladoke Akintola University of Technology,
P. M. B. 4000, Ogbomoso, Oyo State, Nigeria
E-mail: otarulogun@lautech.edu.ng; eoomidiora@lautech.edu.ng; ookediran@lautech.edu.ng

ABSTRACT
In this paper, we present the performance evaluation of modified stegano-cryptographic model of secured electronic voting. This was achieved by the adoption of RSA and ECC cryptosystems for platform adaptable cryptography and an Improved LSB image spatial Algorithm and Wavelet video frequency for multi-domain and multimedia steganography. The model was evaluated by using StegSecret and StegDetect Steganalytic detectors for detecting and launching brute-force attack as well as dictionary attacks against stego objects and full reference objective assessment of spatial stego image using Structural Similarity Index Metric (SSIM).The result of the qualitative evaluations of the model show that the model is an imperceptible and robust e-voting model and therefore can serve as platform for the delivery of credible, fair and transparent future e-democratic decision making in developing countries with significant digital divides.

Key words: Biometric, Cryptography, Encryption, E-voting, Steganalysis, Steganography.

1. INTRODUCTION

Citizens' capability to express unhindered opinion of choice in trustworthy elections is the bedrock of democratic societies [20]. Election is a fundamental instrument of a democratic process that enables the electorate to determine fairly and freely who should lead them at every level of government periodically [19]. The democratic process rests on a fair, universally accessible voting system through which all citizens can easily and accurately cast a vote [5]. Voting is a method by which group of people express their opinion over who will lead them for a specific period of time via electoral processes [20]. The integrity of a nation's electoral process defines the integrity of a nation's democracy. Therefore, voting system must be fair, secured and universally accessible to all citizens [5]. The design of any voting system must satisfy a number of criteria. These requirements give an avenue for a free, fair, credible and confidential election. The system is to meet the following requirements:

i. ***Security***: Votes should not be manipulated during the whole process of voting.
ii. ***Convenience***: Voters should be able to cast votes quickly with minimal equipment or skills.
iii. ***Accuracy***: The outcome of the election is correct and includes all valid votes.
iv. ***Democracy***: All eligible voters must be able to vote, one person - one vote and no one can vote more than once [6].
v. ***Verifiability: Voti***ng systems should be verified so as to have confidence that they meet necessary criteria.
vi. ***Receipt-freeness:*** No evidence is given to the voter to disclose his vote [3].

Among these, security can be viewed as the most critical issue. The objective of security in e-voting systems is to protect valuable or sensitive electronic voting information while making it readily available. For an e-voting system to be secured, it must fulfill generic criteria such as authenticity, confidentiality, integrity and verifiability. Though, it might be difficult to come up with a system which is perfect in all senses, once it is possible to prove that a voter is genuine and any information about the voter's vote cannot be accessed by unauthorized parties, other requirements can be addressed easily [9].

In this paper, we present the design and qualitative performance evaluation of modified stegano-cryptographic model of secured electronic voting. Steganography is the science of hiding and transmitting data through innocuous carrier in an effort to conceal the existence of data from an eavesdropper while cryptography is the science of transmitting scrambled data in an effort to secure communications from an eavesdropper despite his awareness of the data transmission. In most cases, sending encrypted data over wireless channel may draw attention, while invisible communications will not draw attention [19]. The concurrent combination of both sciences for information security and privacy can be used for stronger mechanism of protecting and preserving the integrity of information from an adversary [17].

The rest of the paper is organized as follows. In section two, related works are discussed, the model design considerations is explained in section 3. Section 4 gives the model performance evaluation. Finally, we conclude in section 5.

2. RELATED WORK

There exists a number of related works in literature where the science of cryptography, steganography and combination of both are applied secure electronic voting systems for the delivery of credible electronic democratic governance.

The requirement, design and implementation of a generic e-voting system were proposed in [22]. The security consideration of the model was based on RSA cryptosystem for end to end ballot security and firewalls in form of proxy server. The security consideration of the model was limited to large key size of RSA which requires large amount of computing time and large storage size on both mobile and electronic voting devices. Authors in [10] developed a security scheme that provides an extra layer of security against hacking called Stegacrypt. Stegacrypt is the hybridization of encryption and steganography. This is done by modifying the palettes of the carrier image and embedding one message bit of an encrypted file into each pixel in a Graphic Interchange Format (GIF) image. The problem of statistical weakness by using an insertion rate that is less than 4% of the least significant bit was overcome in this work as the visual quality of the carrier image is retained as compared to other steganography tools. The stability of the stegacrypt against attacks was tested by using stegalyzerSS, the result shows that stegacrypt is able to withstand various forms of attack on stego-image embedded by the software.

Also authors [9] combined both steganographic and cryptographic techniques to demystify authentication security requirements of an online e-voting system using both secret key and voters biometric fingerprint template as the cover. The proposed model is an improvement on [6] 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. In [13], authors combined both steganographic and cryptographic techniques to solve confidentiality and integrity security requirements of secure voting. However, the adopted steganographic technique has low robustness against statistical attack from statistical steganalyst. The manipulation of image cover by an adversary might destroy the hidden message from its destination [14].

Consequently, authors in [23] improved on [9] hashing speed limitation by replacing MD5 with SHA 256 and authenticating voters with biometric Iris. Authors in [25], 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. The proposed model Stego medium is unilateral and prone to statistical attack.

In [4], authors established an approach to provide secure mobile voting based on Biometrics in conjunction with elliptic curve cryptography and steganography especially for Authentication. The author describes Elliptic curve as a public key cryptography, and steganography as the technique of hiding confidential information within any media. The combination of these two algorithms gives an Elliptic Curve crypto-Stegano Scheme which is applied on a voter's Id as well as image and voice data. This is done in such a way that the Voter –Id and the captured image and voice data of the voter during the login phase is encrypted using the ECC algorithm with the use of WTLS protocol and hidden in an image using steganography. This provides an enhanced security over the insecure channel and the use of WTLS protocol makes the system much more secure. This proposed scheme provides enhanced security in the area of authentication only. The voting process itself is not being considered as this is also a very important process that requires enhanced security.

Authors in [11] proposed multimodal face and fingerprint biometric and multilayer techniques to the problem of authentication in online e-voting system. The strength of the model lies in the nexus combination of voter's facial image and fingerprint samples as well as MD5 hashing algorithm for higher degree of authentication in the security of e-system. However, the model lacks verifiability requirement of secured e-voting system and stego object medium is unilateral. In [27], authors' proposed secure online voting scheme with both facial biometric integrated with fingerprint authentication and video steganography for authentication requirement of secure remote e-voting. The model is mobile device platform unfriendly as the model is based on RSA with large key size which requires both large amount of computing time and consumes large storage size on mobile voting device.

In [8] the authors proposed a heuristic approach to introduce the concept of multi layer data security in the field of combined cryptography and steganography. The authors developed a system in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. This is done by employing symmetric block ciphers with linear algebraic equation for the cryptography and employing the least significant (LSB) technique for hiding the cipher text obtained from encryption in the cover image, which replaces the least significant bits of pixel selected to hide the information. An algorithm was proposed for securing text message in multiple protection layers. Some experiments were carried out to prove the efficiency of the proposed scheme using MSE and PSNR metrics.

Our model proposition for secured e-voting is premised along improving the platform limitation in [22] and [27] by limiting RSA cryptosystem to poll site and kiosk based e-voting scenario while ECC cryptosystem is adopted for mobile e-voting for speed and storage size design considerations and ballot integrity through cryptography. Further confidentiality, privacy and secrecy of e-ballot are accomplished by multi domain and multimedia improvement to [9], proposition using scattered LSB Image steganographic in spatial domain and Integer to integer wavelet video steganography technique in frequency domain. Concurrent combination of multi domain in our proposition gives a model with high Impercibility index and high robustness to attack from an adversary as shown in section three.

3. MODEL ARCHITECTURAL DESIGN

Our model shown in Figure 1, combines multi-layer data security(steganography and cryptography), multi media (Image and video), and Multi-domain (Spatial and Frequency) to solve the problem of authentication, integrity, confidentiality, verifiability in our developed framework of secure electronic voting in pre electoral, electoral and post electoral phase of e-democratic decision making shown in Figure 2. The framework of our secure e-voting system is based on three-tier client-server architecture of Advancement Structured Information Standard (OASIS) paradigm [18]. In Figure 2, the electioneering process is model into three phases: The pre-election phase; the election phase and the post-election phase. This architecture provides greater application high flexibility and efficiency, since each tier runs on a separate machine to improve the system performance. The pre-election phase involves the registration of all entities that will enable the outcome of the election, such entities are: Voters information, administrators, Candidates and Parties information, which are all stored in the database.

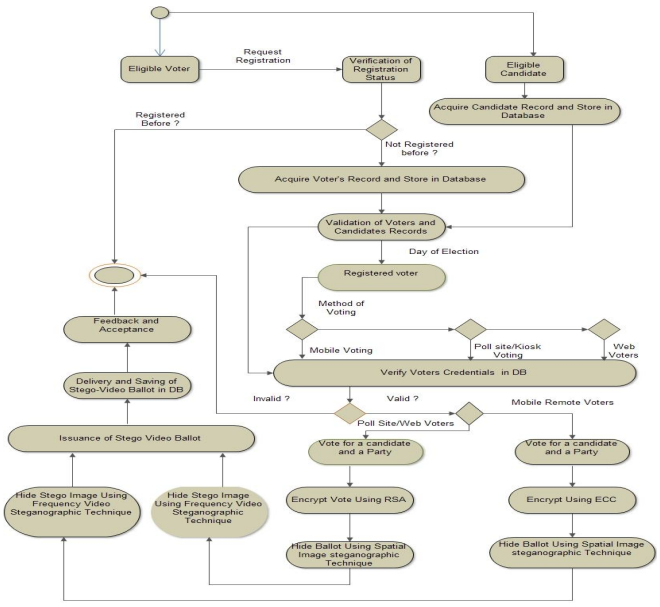

Figure 1: Modified Stegano-Cryptographic Model of Secure E-voting (Source:[21])

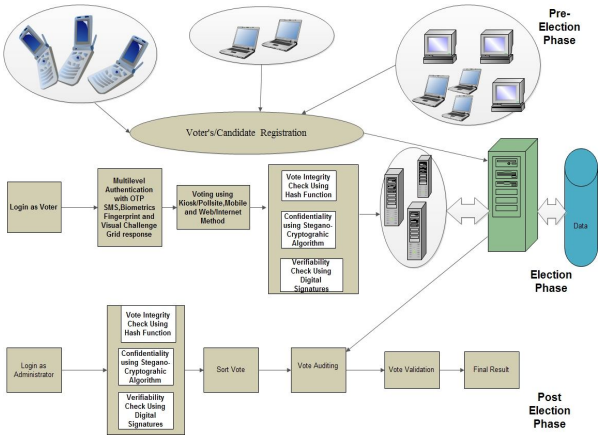

Figure 2: Framework of Secured E-Voting Model (Source: [21])

Our model in Figure 1 is designed around three voting scenarios: the remote mobile voting, web/internet voting and Kiosk/polls site voting. Remote web voting and Poll site voters cast vote from voting device through secured Uniform Resource Locator (URL) address of the secure e-voting system implemented based on the model. The e-voting system application runs remotely on the remote voter's device. The credential of remote web voter is verified through multifactor authentication 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 as shown in the framework in Figure 2. The ballot is encrypted using RSA cryptographic technique to obtain cipher text. The cipher text is hidden into system generated image using modified LSB spatial image steganographic technique to produce stego-image. Further confidentiality of the vote in the stego- image is achieved through further hiding of vote in a video cover using integer to integer wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator[21].

At the administrator end, the administrator recovers vote M by performing Integer Inverse wavelet transform on the stego object with the secret image to retrieved the cipher text from the stego image(S). Also using modified least significant bit extraction steganographic algorithm, the cipher text is extracted from the stego image using the stego key K (the stego key).The final cipher text is then decrypted using either RSA decryption algorithm to get the final message M (vote) without the knowledge of an adversary who will neither detect that M is embedded in S nor be able to access the content of the secret message. This is an improvement over similar presentation in [22]. The concurrent combination of spatial and frequency steganographic technique in our model leads to the development of a model with high imperceptibility index,

high robustness to attacks and high payload capacity in multimedia cover.

An attempt to achieve multimedia improvement on limitation of [8] was accomplished in remote mobile voting. Remote mobile voter casts vote using his credential verified through multifactor authentication using both two-way one-time short message service (SMS) code and accurate response to visual challenge response from the grid. The mobile voter is validated by accurate comparison of remotely entered one-time SMS code; accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish remote voters are who they claim they are shown in the framework in Figure 2. The mobile ballot is thus encrypted using elliptic curve cryptographic (ECC) technique to obtain cipher text for speed and memory constraints reasons of mobile device. The cipher text is hidden into system generated image using modified LSB spatial image steganographic technique to produce stego-image. Further confidentiality of the vote in the stego-image is achieved through further hiding of vote in a video cover using integer to integer wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator[21].

4. MODEL PERFORMANCE EVALUATION

This involves assessment of the model to determine its level of performance and to know if the model meets up to expected security requirements of e-voting. This can be achieved by steganalytic investigation and Objective image quality assessment. Steganalysis aims at discovering or detecting of information hidden in images. With steganalysis, the security level of security our model can be assessed as the steganalytic detector tries to launch various attacks such as chi-square attacks, dictionary attacks, etc. on the model. Image Quality Assessment (IQA) on the other hand is the process of determining the degree to which the stego object satisfy the naturalness and usefulness of the cover image as well as a platform for benchmarking the model [8]. IQA plays a fundamental role in the design and evaluation of imaging and image processing systems [30].

4.1 Steganalytic Investigations

Steganalysis refers to the body of techniques devised to detect hidden contents in digital media [26]. Steganalysis is an allusion to cryptanalysis which refers to the body of techniques devised to break codes and ciphers [28]. The requirement of steganalysis is to determine accurately whether a secret message is hidden in the testing medium. This may include judging the type of the steganography, estimating the rough length of the message and extracting the hidden message [12]. In e-voting domain, the process of evaluating the level of confidentiality of electronic ballot is called Steganalysis, which is the evaluation of steganography algorithms and methods. With steganalysis, the level of security of various steganography algorithms could be determined as it tries to launch various attacks such as chi-square attacks, dictionary attacks, and RS attacks on the algorithms. Steganalytic investigations will often have to be backed up with scanning for hidden information using detectors such as: StegDetect, StegalyzerSS, StegSecret, Ben 4D.

StegSecret is an open source steganalytic program developed to detect steganographic content in different digital media. It detects EOF, LSB, DCTs and other techniques. Stegdetect was written by Niels Provos in 2001. Stegdetect is also another reliable detector in detecting JPEG images that have content embedded with JSteg, JPHide and OutGuess [17]. Stegdetect also contains a utility using brute-force attack that launches dictionary attacks against JSteg and JPHide. This utility is called Stegbreak. Xsteg is the Graphical User Interface(GUI) to Stegdetect.

For the evaluation our model, the final spatial stego-Image was scanned for possible detection by Stegdetect with sensitivity level of 1.00,5.00 and 9.00 as shown in Figure 3.The higher the index level of sensitivity of the suite, the higher the level of detection of the stego Image. For each jpeg image found in the secure electronic voting system folder, *"C:\users\Engr Olaniyi\desktop\Olaniyi"*, Stegdetect displays the output from possible steganographic systems found in each image or ***"negative"*** if no steganographic content could not be detected. Stegdetect detector expresses the level of confidence of the detection with one to three stars. From Figure 3, the developed model stego image named, *"C:\users\Engr Olaniyi\Olaniyi\Web\StegoImage.jpg"* was ***negatively detected*** by Stegdetect indicating that the stegdetect could not detect the content (encrypted electronic ballot -vote) embedded in the stego Image and therefore could not launch the brute force attack against the stego-image. Therefore, the developed modified Stegano-cryptographic technique for e-voting system is truly secured since the stego-Image is perfectly imperceptible and robust to attack.

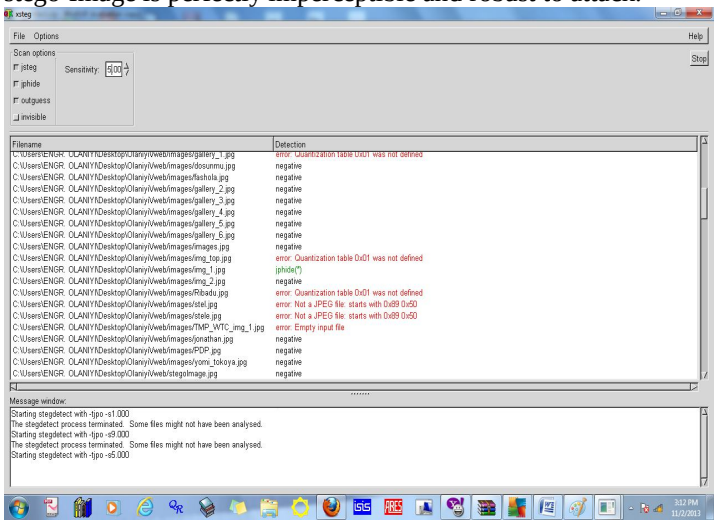

Figure 3: Steganalytic investigation using Stegdetect detector

Similar result was obtained when the stego image in the same folder was scanned with StegSecret steganalysis detector shown in Figure 4. The evaluation of our model after scanning with Stegsecret steganalytic tool depicts that the tool could not launch visual attacks and statistical Attack such as Chi Square and RS Attack for sequential LSB detection and estimation of pseudo LSB size respectively on the stego Image. Therefore the developed modified Stegano-cryptographic e-voting is perfectly imperceptible**.**

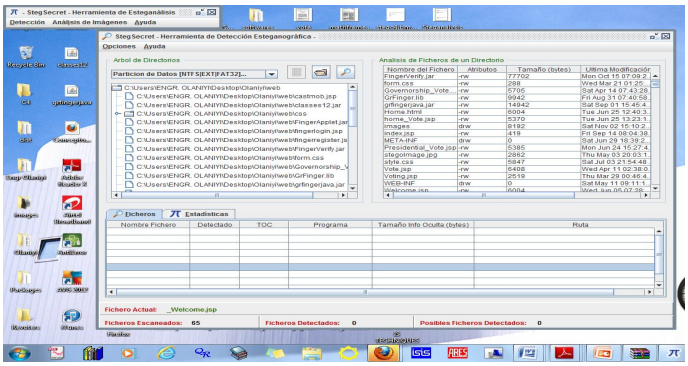

Figure 4: Steganalytic investigation using StegSecret steganalytic tool

4.2 Image Quality Assessment (IQA)

Image quality assessment (IQA) in this context is the process of determining the degree to which the stego object satisfies the naturalness and usefulness of the cover image as well as a platform for benchmarking our model. IQA can be accomplished using subjective method and objective method model. Subjective method entails getting a group of observers to analyzed the perceived image quality image and compute mean opinion score (MOS) and differential mean opinion score. This method is complicated and time consuming [8].The objective analysis involves the mathematical computation of the image quality based on reference image. The reference can be classified into Full Reference (FR), No reference (NR) and Reduced Reference (RR).Most objective IQA embraces full reference method of involving both the test Image and original image using Mean Square Error (MSE) similarity metric and Structural similarity index metrics (SSIM) [8].

In evaluating the performance stegano-cryptographic models in literature, for instance in [8], is accomplished through the computation of Peak Signal to Noise Ratio (PSNR) from Mean square error (MSE) similarity metric due to their simplicity in calculation, have clear physical meanings, mathematically convenient and ease of implementation [30]. The PSNR is the measure of the distortion of the stego image in comparison with the cover image. Higher PSNR means less distortion between the two images [1].

However, the computations of PSNR for stegano-cryptographic models lack two critical features: a) The ability to assess image similarity across distortion types and b) They are not very well matched to perceived visual quality [15],[29]. They are acceptable image assessment measures when the images in question differ by simply increasing distortion of a certain type. A new approach to assess image quality independent of the type or size as well as pixel size of the testing image is called Structural Similarity index metric (SSIM). Experiments conducted in literature shows that SSIM Index can be used as a better and effective alternate IQA. SSIM estimates the visual impact of shifts in image luminance, changes in photograph contrast, as well as any other remaining errors, collectively identified as structural changes [30][7]. For two images x and y of common size N*N, SSIM is given as:

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

(1)

Where: μ_x is the average of x, μ_y is the average of y, σ_y^2 is the variance of y, σ_{xy} is the covariance of x and y, $C_1 = (k_1 L)^2$ and $C_2 = (k_2 L)^2$ are two variables to stabilize the division with weak denominator. L is the dynamic range of the pixel-values and $k_1 = 0.01$ and k_2 = 0.03 by default.

As equation 1 approaches 1, the greater the degree of fidelity of the compressed image is close to the original image. The dynamic range of equation 1 from [2] is:

$$SSIM = [-1, +1] \qquad (2)$$

The best value 1 is achieved if and only if the two images are similar and -1 if the two images are highly structurally un-similar [2].

4.2.1 IQA using SSIM Computations

The quality of the stego image from the developed stegano-cryptographic model based on experimental findings of 4.1 was evaluated and benchmarked by comparing the structural similarity information between the distorted image – the stego image and its reference image cover image for index levels of 1 to 4. Figure 5a - Figure 5j depict the cover image(in color); Spatial Stego Image(in color), cover image(in Grayscale); Inverted Spatial stego, Spatial stego Image at SSIM Index at level 1 to 4 respectively. Table 1 shows the computed structural similarity Index metric (SSIM) between the cover image and stego image at index level 0 to 4 using the ImageJ Image Processing software program, a Java based Image processing program for editing, analysing and processing color and grayscale Images.


Figure 5a: Cover Image
Figure 5b: Stego Image


Figure 5c: Cover Image (Grayscale)
Figure 5d: Stego Image (Inverted Grayscale format)


Figure 5e: SSIM Index level 1 of Stego Image
Figure 5f: SSIM Index level 2 of Stego Image

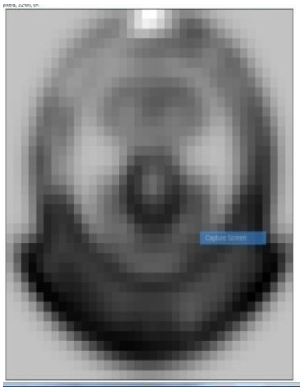
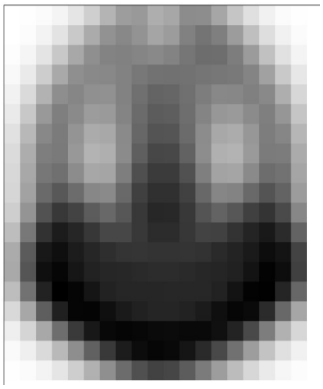

Figure 5e: SSIM Index level 3 of Stego Image
Figure 5f: SSIM Index leve1 4 of Stego Image

Table 1: Parameters of SSIM used in benchmarking the developed secured e-model

Level	SSIM Value
0	0.4284
1	-0.0891
2	-0.2335
3	-0.3646
4	-0.4765

Considering Figure 5a and Figure 5b, the cover image and spatial stego image are visually similar with human objective assessment but from equation 2 above, the negative value of SSIM index value from index 1 to 4 from Table 1 affirms that the stego image is completely un-similar to the cover image structurally, thus, the developed stegano-cryptographic model for secure e-voting is secured.

With the result of the evaluation in section 4.1 and 4.2, we can therefore conclude that the model is imperceptible and robust to attack from an adversary. Therefore, the developed-voting model can serve as a platform for the delivery of credible, fair and transparent future e-democratic decision making in developing countries with significant digital divides.

5. CONCLUSION

This paper has presented the architectural design and qualitative performance evaluation of a modified stegano-cryptographic model of secured electronic voting for delivery of transparent and credible of e-democracy of high integrity and political trustworthiness. The strength of the model lies in its double data layer, media and domain against any "Man-in-the-Middle" attack or any other form of eavesdropping of electronic ballot while on transit. This is to ensure that the issue of trust in the electoral process is resolved and thus ensure the electorates put their confidence in the electoral process. The secured electronic voting model if implemented in future e-democratic decision making in developing countries will help increase the level of citizens' participation in the elections and ensure a better, faster, easier and more efficient means of voters' registration ,voting and auditing compare to existing manual method of voting.

REFERENCES

[1] A.B AdnaanMohsin and A. Wafaa Mustafa. B(2010),"Stego Based Crypto Technique for High Security Applications", International Journal of Computer Theory and Engineering,Vol.2,No 6,pp 835-841.

[2] A. Aibinu, A.R, Najeeb, M. J., Salami, and A. A. Shafie, (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

[3] A. Antonio, C, Korakas, C, Manolopoulos A, Panagiotaki, D, Sofotassios, P. Spirakis and Y.C Stamatiou (2007), "A Trust-Centered Approach for Building E-voting Systems", In Proceedings of Electronic Government,6th International Conference on Electronic Govermment , EGOV 2007, Regensburg, Germany, pp 366-377.

[4] Alok K and Atul K (2011),"A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with
Elliptic Curve Crypto-Stegano Scheme" , International Journal of Technology And Engineering System (IJTES), Vol 2. No1, pp 8-11.

[5] J. Bannet, D. W. Price, A Rudys. J. and Singer , D. S. Wallach (2004), "Hack-a-Vote: Security Issues with Electronic Voting Systems", IEEE Security and Privacy Journal, pp 32- 37.

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

[7]] R Dosellmann and X. D. Yang (2008)," A Formal assessment of SSIM", Technical Report of Department of Computer Science, University of Regina, Rega, Canada, pp1-15

[8] S.A Gandi and C.V. Kulkarni (2013), "MSE Vs SSIM" ,International Journal of Scientific and engineering Research(IJSER),Vol4, No7, pp930-933 .

[9] S. Katiyar, K R Meka, F A Barbuiya, and S Nandi (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

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

[11] P . Linu and M.N. Anilkumar (2012),"Authentication for Online Voting Using Steganography and Biometrics", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET),Vol. 1 No. 10,pp 26-32

[12] B. Li , J. He, J. Huang and Y. Q. Shi (2011)," A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No 2 ,pp142-172

[13] Mallick P K and Kamilla (2011), " Crypto Steganography Using linear Equation, International Journal of Computer and Communication Technology, Volume 2 Issue 8,pp106-112.

[14] T.J. Morkel, H.P Eloff and M.S. Olivier (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

[15] A. Mittal, , R. Soundararajan and A. C. Bovik (2013),"Making a Completely Blind Image Quality Analyzer", IEEE Signal Processing Letters,Vol.22 No.3,pp 209-212.

[16] H Nagham, Y, Abid, R Ahmad and Osamah M (2012),"Image Steganography Techniques: An Overview", International Journal of Computer Science and Security, Vol. 6 No 3,pp 168-187.

[17]P. Niels, and H. Peter, (2011), "Detecting Steganographic Content on the Internet" Retrieved at http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf on 8th February, 2012

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

[19] N.O Obakhedo(2011), "Curbing Electoral violence in Nigeria:The Imperative of Polital Education",African Research Review:International Multidisciplinary Journal,Ethiopia,Vol.5.No.5,pp 99-110,Retrieved online at http://www.ajol.info/index.php/afrrev/article/viewFile/72297/61230 on 9th January 2014.

[20] O. M. Olaniyi, O. T. Arulogun, and E.O. Omidiora (2012),"Towards an Improved Stegano-Cryptographic Model for Secure Electronic Voting", African Journal of Computing and ICTs, Vol. 5, No.6 pp 10-16.

[21] O. M. Olaniyi, O.T Arulogun, E.O. Omidiora, Okediran O.O (2013)," 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.

[22] O. O. Okediran, E. O. Omidiora, S. O., Olabiyisi , Ganiyu R. A,. Alo O. O. (2011), "A Framework for a Multifaceted Electronic Voting System", International Journal of Applied Science and Technology Vol. 1(4) , pp 135 – 142.

[23] S. M. Prabha 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

[24] Radcliff, D. (2012), "Computer World" Retrieved at http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00.html on 6th March, 2012.

[25] L, Rura, Isaac B, and M. K Haldar (2011), "Secure Electronic Voting System Based on Image Steganography", Proceedings of IEEE Conference on Open Systems (ICOS2011), IEEE, September 25-28,2011,Langwi, Malaysia.

[26]A. Rocha and S. Goldenstein,(2008), Steganography and Steganalysis in digital multimedia:Hype or Hallelujah,RITA,Vol.15.No. 1, pp83-110 Retrieved online at http://www.ic.unicamp.br/~siome/papers/Rocha-Rita08.pdf on January 15th 2013.

[27] S. S Sulthana and S. Kanmani (2011), "Evidence based access control over web services using multi security" , International Journal of Computer Applications ,Vol.17(3),pp1-7

[28] B. Schneier. (1995), "Applied Cryptography", John Wiley & Sons, New York.

[29]Wang, Z., Bovik A. C. Rao, P., (2004), "Image Quality Assessment: From error visibility to structural similarity", IEEE Transaction on Image Processing, Vol13. No.(4), pp 600–612.

[30] O.R.Vincent and O.K. Adepoju (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.