www.seetconf.futminna.edu.ng

www.futminna.edu.ng

Performance Evaluation of Enhanced Least Significant Bit Audio Steganographic Model for Secure Electronic Voting

Olaniyi Olayemi Mikail[1], Folorunso Taliha Abiodun[2], Abdullahi Ibrahim Mohammed[1], Nuhu Bello Kontagora[1], Abdulsalam Kayode Abdusalam[1]

[1](Computer Engineering Department, Federal University of Technology, Minna, Niger State, Nigeria)
[2](Mechatronics Engineering Department, Federal University of Technology, Minna, Niger State, Nigeria)
[*]mikail.olaniyi@futminna.eu.ng,.

ABSTRACT
This paper presents performance evaluation of an enhanced Least Significant Bit (LSB) audio steganographic model for secure electronic voting. The enhancement on the traditional LSB audio steganographic technique on the electronic vote was achieved through the hidden of secret information from fourth bit to sixth bit position. The sampled votes were digitally signed to ensure the integrity of the casted votes. The model was evaluated objectively using three quantitative metrics: Embedding capacity of the stego audio file, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of the cover and stego audio. The results of the quantitative evaluation of the model showed that the model was robust and imperceptible for the delivery of transparent and credible secure e-voting of high electoral integrity and confidentiality in developing countries of significant digital divide.

Keywords:Steganography, E-Voting, Audio, Editing, Embedding, Extraction, Confidentially, Integrity

1. INTRODUCTION

Democratic decision making in modern society have been transformed by the introduction of Information and Communication Technology (ICT). This introduction termed, electronic democracy(e-democracy), have added improved accessibility, accuracy, reduced cost and fast casting, counting and timely dissemination of electoral results to wider populace. The most important element of democracy is the voting procedure of the electorate. The introduction of ICT in this critical element of democracy is called electronic voting (e-voting)[22]. E-voting as a distributed social information system is a security-critical application of democracy with the usage of computerized infrastructures in ballot casting as reasonable alternative to traditional procedure of opinion expressing procedures [22, 26]. Electronic voting is seen as a tool for making the electoral process extra efficient and for increasing trust in its administration. Properly executed e-voting solutions can increase the security of the ballot, speed up the processing of results and make voting a stress-free exercise.

Every electronic voting system design must fulfill certain fundamental requirements which provide a platform for delivery of a reliable, impartial and confidential election. These requirements are: Non-repudiation, accessibility, transparency, auditability, confidentiality, integrity, authentication, and non-coercibility [15].In view to produce excellent and effective democratic processes, the aforementioned criteria must be taken into consideration. Other basic criteria are [13, 14,11]:

i. **Accuracy:**All valid votes must be recorded accurately and the result must be correct.
ii. **Democracy:** Democratic principles must be enshrined through single citizen single vote mechanism and those votes must count.
iii. **Ease of access:**The developed system must be easily and readily accessible to the electorate with minimal complexity.
iv. **Transparency:** This is the quality of the developed system to be free from ambiguity.
v. **Security:** This is the protection of castedvotes from spoofing and falsification for all phases of electioneering process.

vi. **Verifiability:** the casted votes must be check-balanced to ensure they meet up the basic requirements of the system.

Security in e-voting is the critical requirement amongst the aforementioned criteria whose purpose is to safeguard valued electronic data during casting, transmission, collation and audition [26]. Insecurity in voting can cause electorates to lose confidence in electoral activities. The root of credibility in democratic decision making in developing countries lies in proper provision of security requirements as well as other issues such as legislation, usability, convenience and universal accommodation of able and disable electorate in political decision making processes. The generic security issues of electronic voting systems include: authentication of near and remote voters, integrity, confidentiality and availability of electronic ballot in transit as well as verification of casted and counted votes. It is invariably impossible to develop a system that is perfect or fault free but if salient security requirements like authentication, integrity, confidentiality and verification of electorates of casted votes can be handled other features of availability and universal verifiability could be handled for the delivery of credible electronic voting exercise [13].

In this work, we present the performance evaluation of an Enhanced Least Significant Model ofSecure electronic voting as anticipated in [25]. Steganography is the science of keeping the existence of secret message in innocent media for covert communication in an unsecured channel. Since electronic voting involves secret and confidential decision making of an anonymous electorate [12]. Careful application of steganographic techniques in electronic voting could assists to deliver credible secure e-voting. In this contribution, we investigate performance of the model proposed in [25] objectively in view to guarantee a secure electronic voting. An enhanced LSB audio steganographic technique was used to develop a secure system that can significantly cater for security issues pervading different phases of electronic voting system in our contemporary world. Steganography is an information hiding technique for communication between source and destination from third party. This communication through invisibility of voter's choice by hiding it in unobjectionable carrier file is proposed in audio medium in this work.

The paper is organized into five sections: Section two provides the review of related works,, model designed consideration was presented in section three, performance evaluation of model was accomplished in section four. Section five concludes and provides opens issues for future research.

2. RELATED WORKS

There are several related works in literature that exploited the science of steganography for computer security especially in the field of electronic voting system design for credible and confidential electioneering process.

The design and development of a secure electronic voting system using a multifactor authentication and cryptographic hashing function were presented in [13]. In this work, significant attempt was made to improve the authentication of electorates before casting their votes as well as the integrity of the vote after being casted. After a unique id was generated, a unique short message service (SMS) code was automatically generated for instant authentication of voter. Only two of the security issues mentioned in [12] were tackled in [13] which are authentication and integrity. Hence the efficiency of the system cannot be guaranteed with only two security challenges addressed in [13]. Biometrics was added to the advantage of steganography in online voting system security in [20]. Complementary security systems are good

enough to guarantee secure voting process especially where password is added. The fingerprints of the voters were used as cover object for embedding voters' secret information. Personal Authentication Numbers (PAN) was used to authenticate voters for who they are. PSNR of the images range between 30-50db for scheme imperceptibility, but spatial domain steganography without any enhancement proposed is not secure enough to guarantee and effective secure e-votiing.

Authors in [4] designed a secure e-voting system based on homomorphic property and blind signature scheme. The proposed system in this work was implemented as embedded system on voting machine. This system employs RFID smart card to store all conditions that comply with the rule of the government to verify voters' eligibility. Central Tabulation Facility (CTF) was adopted to collect all secret ballots from local committee severs distributed across pole stations. The proposed system utilises homomorphic cryptosystem implemented using Paillier cryptosystem and blind signature based on RSA. The information stored in the RFID tags were used to track the activities of the voter and hence he/she cannot vote more than once. Security analysis was carried out using eligibility, secrecy, uniqueness, privacy and accuracy. The designed system was not in any way evaluated based on the specified issues it was built upon.

Since the major bone of contention in online voting system is information security, authors in [6] developed an online voting system powered by biometric security using steganography. The combination of science of cryptography with steganography in [6] added higher security. Fingerprint image was used as cover object for steganography while key generated was used to achieve cryptography. Cryptography helped to reduce to a great extent the risk of the system being hacked as hackers must find the secret key as well as the image. The merging of the secret key with image resulted into stego image which is similar to the cover image with no significant difference for detection by human eyes. The strength of the system lies in the cascading of different security platforms to make the system as a whole. However, the system is limited to large information overhead that must be processed and limited consideration for integrity of hidden vote on transit.

In [22] and [23] several steganographic techniques were analysed implanting them in various categories of steganography such as text, image, audio and file system. Also, [9] demonstrated the advantages of the techniques in [22] emphasising the fact that transform domain can ensure high embedding capacity with perceptual transparency than temporal domain. A survey was carried out on general principle of hiding in information security for audio carriers in [23]. In [1], a review was carried out on binary image steganography and watermarking analysing different techniques in each domain. Different factors in watermarking and steganography were considered such as visual quality, embedding capacity, security, robustness and computational complexity in [1] for image based processing in spatial and transform domains. The limitation of image steganography is such that it can only hide limited amount of information, therefore, making it attributed to low embedding capacity and perceptual transparency.

A steganographic system for data hiding in video/audio was proposed in [5]. The system successfully hides information in different data format but the limitation is such that only small information of few bytes can be hidden in the cover files. Lempe-Ziv-Welch (LZW) universal lossless data compression technique was used for hiding information coupled with AES encryption and decryption algorithms. Hiding encrypted data in audio wave file was done by [17] building on a secret key steganographic system. The proposed system was

developed for message encryption using Data Encryption Standard (DES) and was evaluated using Signal to Noise Ratio (SNR). Authors in [16] developed apeak-shaped-based steganographic technique for mp3 audio using LSB steganography based on the MDCT by applying PSB algorithm. The Peak Shaped Model algorithm that is used for JPEG images was modified to be suited for MP3audio file in other to implement a good steganographic technique. Proposed work was actualized based on statistical properties of MP3 samples, which were compressed by Modified Discrete Cosine Transform. These coefficients were chosen with regards to the statistical relevance of individual coefficients within the distribution. The embedding capacity after performance evaluation was 12.5% and PSNR is 58.21db.The shortfall of [16] was in the low resistance to statistical attack through steganalysis.

Audio in Image Steganography based on Wavelet Transform was proposed in [7]. The work proposed an audio-image steganography, hiding an audio file inside a cover image using LSB technique and wavelet transform. The audio file was first compressed, embedded in the cover image, extracted and then reconstructed. Wavelet was achieved by carrying out some compaction ratio. Compaction was carried out in two level Haar, Daubechies and Coif wavelets. Increase in the audio file causes a corresponding decrease in the PSNR. The speech has high MSE property which cannot ensure enough safety and the size of embedded speech can significantly destroy the image if too large.

Secure Scheme in Audio Steganography (SSAS) was proposed in [10]. The authors designed a system to increase the security by addressing secret message before embedding using mathematical model and map for subsequent extraction of the secret message. The work proposed a new technique for audio steganography using a two phase approach. The stego math selection phase embedding and extracting phase. Stego embed for embedding and P_Map for extraction. A secure stego object was obtained as the output by subjugating or abridging the probability of attach on the secret message or exchanging it. The integrity of the secret message was not put into consideration. The fourth position LSB algorithm was used for embedding with is not safe enough but rather can be improved upon to guarantee a secure information protection

In [2] authors worked towards improving robustness of security through the use of concept of Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) on audio steganographic method. Image was embedded inside a cover audio and the stego audio obtained was compared with simple Least Significant Bit insertion method for data hiding in audio. The cover audio was first converted to streams of bits; the image is also converted to bit streams and then embedded inside the cover audio. DWT was applied on the audio file for taking the higher frequency and generate a random key. 8×8 blocks for each 16bits data was taken and the last 3bits data was used to store image in the cover audio. Inverse of the algorithm was also designed for extraction of the image from the stego audio. Generation was described in detail for embedding and extracting of the image which gave a reasonably good result PSNR of more than 30decibel.

This work made a significant improvement over [2], [4], [7], [10] and [16] through the proposed enhanced LSB audio steganographic technique. Taking advantage of the advantage of Human Auditory System (HAS), we developed a technique to improve information secrecy without noticeable difference to human hearing. Our developed model provided solution for voter's

authentication as well as protection of casted votes from eavesdroppers, hackers and imposters while transmitting electronic ballot over insecure networks. This work improves on similar models in literature with the insertion into sixth bit of the LSB of the cover audio, thereby making the designed model a vehicle for the delivery of credible future e-election in societies where digital democratic dispensation is practiced.

3. MODEL ARCHITECTURAL DESIGN

The designed model shown in Fig. 1 embodies two exceptional security requirements of voting system which are: integrity and confidentiality of vote using object oriented design (OOD) metaphor in Unified Markup Language Activity diagram. Two security layers are implemented in aspects of digital signature for the vote integrity and enhanced LSB audio steganographic technique for the confidentiality of the casted votes. The proposed e-voting model was structured around pre-electoral, electoral, and post electoral phases of e-democratic decision making in Fig. 2. The architectural design in Fig. 2 was adapted to tackle three security issues where RFID cards were used for voter's authentication and verification, digital signature were appended to the votes for integrity control and enhanced LSB audio steganography caters for the system confidentiality. The whole electioneering processes were layered into three phases of electoral processes; pre-election phase, election phase and the post-election phase of the voting exercise.. Voter's registration was carried out at the front end which is the pre-election phase. The candidates, parties and electorates information are documented for use in the subsequent phases. This information includes: name, phone no, sex, marital status, age, occupation and so on. This information helps to verify the eligibility of participants in the exercise and hence for system audit.

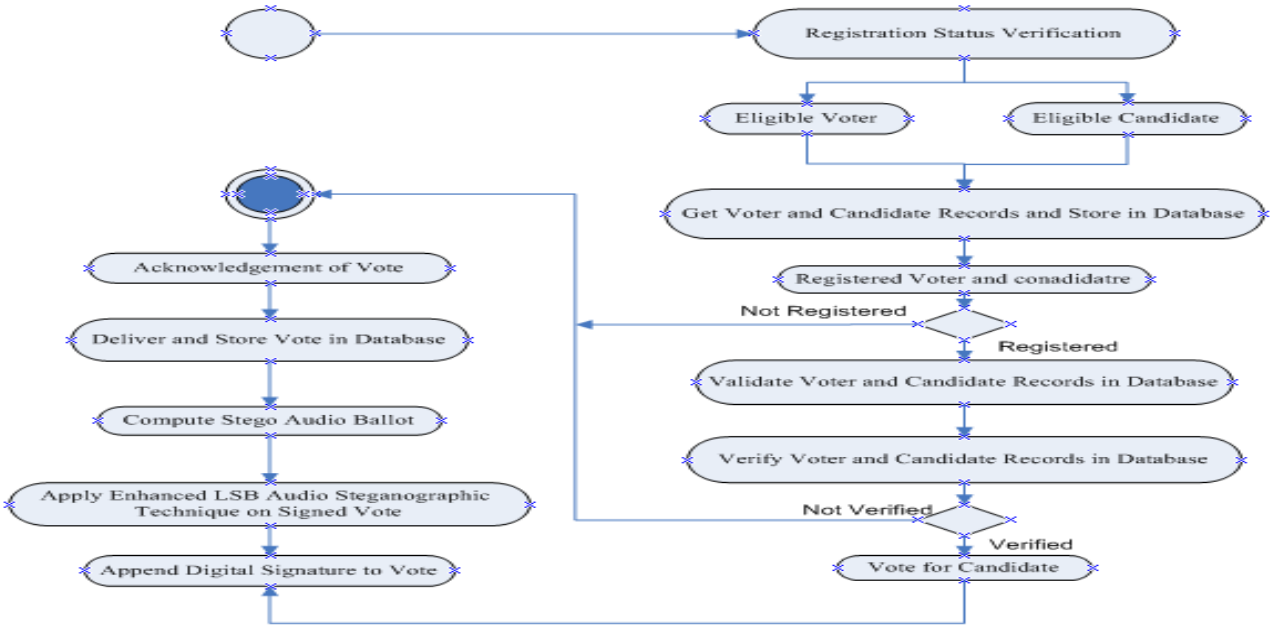

Fig. 1: Enhanced LSB Audio Steganographic Model of Secure E-voting System

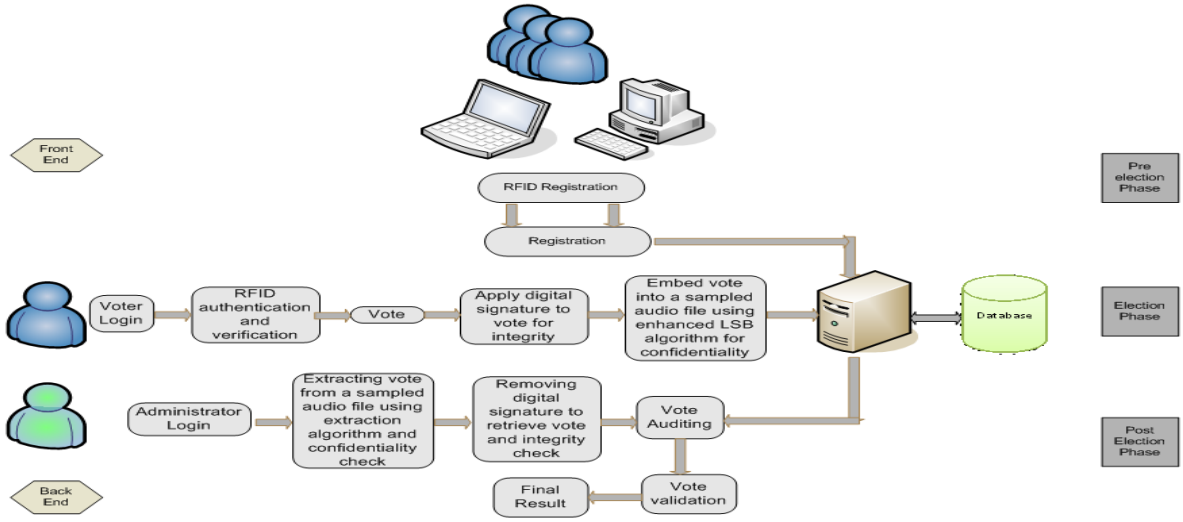

Fig. 2: Secured Electronic Voting System Architectural diagram (adapted from [26])

From Fig. 2, the model was designed around a kiosk type voting system where voters are made to move to a particular voting site for the first two phases of the electioneering process. In the registration phase, each voter is assigned a unique RFID tag which stored the voter's details in the database for further validation and verification in the election phase. This RFID tag was designed for voter's identification during voting, which is further check-balanced with the ID digit stored in the database. The casted vote (V) is sampled and digital signature is appended on it using vote MD5 hashing technique. The resultant digital object is then embedded with embedding algorithm (Em) in a digitized cover audio file using enhanced LSB audio steganographic technique of information security. Stego audio file is the end object which possesses no suspicious difference from the cover audio and the vote can be extracted by the administrator using the reverse mechanism.

In the post-election phase in Figure 2, the administrator retrieves the casted vote (V) from the stego audio (A) file using the extraction algorithm (Ex). This technique helps to protect the confidentiality of the votes from any suspicious knowledge of any adversary, imposter or hacker. This system ensures high perceptual transparency, payload capacity and reasonably robust against attack.

Our proposition is an improvement over [6], [8] and [10] from with respect to the use of RFID for voter's authentication and convenience. The electorate is only required to move his/her RFID card to the tag reader for automatic verification of ID. This has created an authentication and verification mechanism for electorates without any inconvenience. After casting vote, it is then hashed automatically application of MD5 hashing algorithm for integrity control over the casted votes. The digitally signed vote is then hidden in the sixth bit position of the sampled audio for an enhanced LSB audio technique to improved technique over the existing methods adopted by most systems designers as shown in both schemes for embedding and extraction illustrates as follows:

The following algorithm describes the embedding and extracting processes of information security on the electronic ballot:

Embedding algorithm

Input: A wave (.wav file) source audio and a payload file (vote in text form)

Output: A stego wave audio

Begin

1. Read the header information from the source audio file and generate compresses output audio file.
2. Generate 128-bit message digest(MD5 hash fuction)
3. Generate 32 digit hexadecimal text value of the vote(payload)
4. Repeat the following steps until 32-bit payload size(in bytes) are embedded:
    a. Read a sample amplitude value from the source audio file
    b. Apply the enhanced LSB algorithm on the sixth bit position to the LSB for payload embedding
    c. Write the sample value as the output audio, the stego wave audio.
    d. stop

End

Extraction algorithm

Input: A stego wave audio

Output: The extracted payload and the message digest

Begin

1. Read sample amplitude of the stego wave audio file as input.
2. Apply the inverse of the enhanced LSB algorithm on the sixth bit position to the LSB for payload extraction
3. Extract the payload
4. Extract the message digest of the payload
5. Generate 128-bit message digest (MD5-hash function) of the extracted payload.
6. Compare the two message digests to verify the authenticity of the extracted payload.
7. Save vote
8. Increment vote count by 1

End

4 MODEL PERFORMANCE EVALUATION

This entails the assessment of the developed model to determine whether it meets up with the set goal and performance as expected of an electronic voting system [15]. This can be carried out in two broad categories of subjective and objective evaluations. Subjective evaluation describes the process of subjecting the stego audio to steganalytic test and listening hears of electoral officials, voters and observers were allowed to test the system in view to detect the slightest change in the audio files both stego and cover audio. Steganalysis tried to detect any hidden content in a digital file suspected to be carrying hidden information. This technique also exploits the disadvantages of Human Auditory System (HAS) thereby taking advantage of the disadvantage of human hears. At certain frequency, sound are not audible to human hears and this is therefore being capitalized upon. Subjective evaluation model have been carried out in [25]. In this paper, the developed model was evaluated objectively through embedding capacity, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). This evaluation was carried out with regards to the three basic properties of information security: robustness, imperceptibility and payload capacity.

4.1 Objective Evaluation

This is the process of evaluating the perceptual transparency of the stego audio and embedding capacity. This describes the techniques used for detection of the level of efficiency and effectiveness of the algorithms used to develop the system.

4.1.1 Embedding Capacity

This refers to the maximum amount of information that can possibly be hidden inside a cover audio without consequently damaging or scathing the quality of the audio file. It is calculated by evaluating the ratio of the amount of secret message to that of the cover audio object.

$$EC = \frac{Size\ of\ secret\ message}{Size\ of\ cover\ object} \qquad (1)$$

4.1.2 Mean Square Error (MSE)

This is an error metrics used to represent the cumulative square error between the original audio signal and the

compressed audio (stego audio). The lower the value of the calculated MSE, the lower the error rate between the samples which shows little distortion was introduced. It is calculated by the following formula.

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M*N} \quad (2)$$

Where M and N are the rows and columns of the audio samples respectively. I_1 is the stego audio while I_2 is the cover audio.

4.1.3 Peak Signal to Noise Ratio (PSNR)

This is used to estimate the amount of similarities that exist between the cover audio and the stego audio. It is a function of Mean Square Error (MSE). It is a ratio of quality measurement between the two files calculated in decibels. The higher the PSNR of the comparison, the better the analysis demonstrating low distortion of the stego audio generated from cover audio

$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \quad (3)$$

Where R is the minimum fluctuation in the stego audio which is usually 255 in integer data type

4.2Results of Objective Performance Evaluation

The outcomes of the tested developed system are described in Tables 1 and 2. Table 1 shows the audio samples evaluation with the various sizes, bit rates and embedding capacity. Table 2 on the order hand shows the results obtained from stego audio analysis after evaluating their Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). These analyses on MATLAB software tool obtained are tabulated as follows:

Table 1: Embedding Capacity of Audio Files

Audio File	Audio Size(KB)	Bit Rate(kbps)	Embedding Capacity (%)
Bom	768	88	0.23
Corn	415	176	0.43
One	78.1	128	2.27
Samp	434	705	0.41
Pledge	348	176	0.51

Table 2: MSE and PSNR of the Sampled Audio Files

Audio File	Audio Size (KB)	Bit Rate (kbps)	Vote Size (kb)	MSE (db)	PSNR (db)
Bom	768	88	1.77	0.2	104.6268
Corn	415	176	1.77	0.5	121.0942
One	78.1	128	1.77	0.9	139.8472
Samp	434	705	1.77	0.7	115.6010
Pledge	348	176	1.77	0.1	101.3640

After comparison of stego audio samples, the average embedding capacity obtained was 0.77%. This is the maximum amount of data size that can be hidden in a cover audio without raising any suspicion. Figure 3 also demonstrated various values obtained from MATLAB analysis of both the stego audio and the cover audio for both bom and Corn audio media. An average value of PSNR value of 116.5066decibel was obtained after analysis of proposed model with Bom, Corn, One, Samp and Pledge audio covers. The proposed was model for secure e-voting

was 50% better than [16] and 42.9% better than [10] using expression in (4).

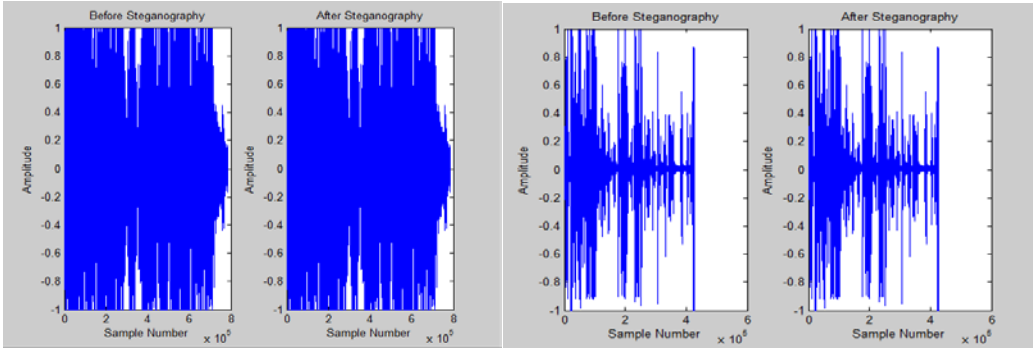

Figure 3: The Wave Plot of both Bom and Corn Audio before and after Steganography

$$\%\ Comparison = \frac{PSNR\ of\ new\ model - PSNR\ of\ existing\ model}{PSNR\ of\ new\ model} \quad (4)$$

Table 4.3: Comparative Analysis of PSNR Value of Existing Models

S/N	Compared Works	PSNR Values (db)	% improvement
1	**The proposed Model**	**116.5066**	
2	Peak-Shaped-Based Steganographic Technique for MP3 Audio (Raffaele, *et.al.*, 2013)	58.2100	50.0372
3	Audio in Image Steganography based on Wavelet Transform (Kaul, *et.al.*, 2013).	59.6548	48.7971
4	New Secure Scheme in Audio Steganography (SSAS) (Mohammed, *et.al.*, 2013).	66.4275	42.9839
5	Hiding Image in Audio using DWT and LSB (Gupta *et.al.*, 2013)	37.0733	68.1792
6	Message Guided Adaptive Random Audio Steganography using LSB Modification (Taruna *et.al.*, 2014)	86.0462	26.1448

5. CONCLUSION AND RECOMMENDATIONS FOR FUTURE WORK

This work has successfully presented the architectural design and performance evaluation of an enhanced LSB audio Steganographic model for a secure electronic voting.The model provided countermeasures over ballot integritybreach and spoofing of the ballot confidentially on transits, verification and validation of voters at kiosk site using RFID card uniquely assigned to voters. The model was quantitatively evaluated using embedding capacity, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) quality metrics. The proposed model for secure e-voting was 50% better than [16] and 42.9% better than [10] similar models in literature. The proposed secure e-voting model if applied in conducting future electoral process in developing countries could assists in delivery of credible e-election in societies where digital divide is significant. We hereby recommend the wide scale test-running and subsequent adoption of the developed model for the electoral authority in developing countries like Independent National Electoral Commission (INEC) in Nigeria for future comprehensive secure electronic voting. The following open issues can be addressed in future research endeavour:

a) **Voting Service Availability:** Future design could address voting service availability issue towards Denial of Service(DoS) and Distributed Denial of Service (DDoS) attacks.

b) **Frequency domain for higher security measures:** Improvement can be made on the

security technique through the use of enhanced frequency domain for higher imperceptibility, robustness and payload capacity of hidden information.

c) Audio linguistic steganography can also be combined with other security technologies to increase both generic and non-generic of secure e-voting.

d) Integration of speech processing for visually impaired is also recommended.

REFERENCES

[1] Chhajed G. J., Deshmukh K. V. and Kulkarni T. S. (2011). Review on Binary Image Steganography and Watermarking. International Journal on Computer Science and Engineering. 3(11). 3645-3651.

[2] Gupta N. and Sharma N. (2013). Hiding Image in Audio using DWT and LSB. International Journal of Computer Applications (0975 – 8887). 81(2).

[3] Hernandez-castro J. C., Tapiador J. E., Palomar E. and Romero-gonzalez A. (2010). Blind Steganalysis of Mp3stego. Journal of Information Science and Engineering 26, 1787-1799.

[4] Hussien H. and Hussien A. (2013). Design of a Secured E-voting System. Electronic and Communication Department. AAST Cairo, Egypt. 5.

[5] Jyotheeswari J. and Reddy V. L. (2013). A Novel Steganographic System for Data Hiding in Video/Audio. International Journal of Computer Applications. 82(11). 31-36.

[6] Katiyar S., Meka K. R. (2011). Online Voting System Powered By Biometric Security Using Steganography. Second International Conference on Emerging Applications of Information Technology, IEEE.

[7] Kaul N. and Bajaj N. (2013). Audio in Image Steganography based on Wavelet Transform. International Journal of Computer Applications (0975 – 8887) 79(3).

[8] Kohno T. Stubblefield A. (2004). Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy. IEEE Computer Society Press.

[9] Kulkarni S. A., Patil S. B. Patil B. S. (2013). A Optimized and Secure Audio Steganography for Hiding Secret Information - Review. Journal of Electronics and Communication Engineering. 12-16.

[10] Mohammed S. A., Ibrahim S., Ghazali S. and Ahmad A. (2013). New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences. 7(6): 250-256.

[11] Okediran O. O., Omidiora E. O., Olabiyi S. O., Ganiyu R. A. and Sijuade A. A. (2011b). Towards Remote Electronic Voting Systems. Computer Engineering and Intelligent Systems. 2(4). 2011. 72-82.

[12] Olaniyi O. M., Arulogun O. T. and Omidiora E. A. (2012a). Towards an Improved Stegano-Cryptographic Model for Secured Electronic Voting. African Journal for Computer and Information Communication Technology. 5(6). 10-16.

[13] Olaniyi O. M., Arulogun O. T. and Omidiora E. A. (2013b). Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions. International Journal of Computer and Information Technology. 2(6). 1122-1130.

[14] Olaniyi O. M., Arulogun O. T., Omidiora E. A. and Okediran O. O. (2014a). Performance Assessment Of An Imperceptible And Robust Secured E-Voting Model. International Journal of Scientific & Technology Research. 3(6). 127-132.

[15] Olaniyi O. M., Arulogun O. T., Omidiora E. O. and Okediran O. O. (2014c). Performance Evaluation of modified Stegano-Cryptographic model for Secured E-voting. International Journal of Multidisciplinary in

Cryptology and Information Security. http://warse.org/pdfs/2014/ijmcis01312014.pdf. 3(1). 1-8.

[16] Raffaele P, Fabio G. and Roberto C. (2013). Peak-Shaped-Based Steganographic Technique for MP3 Audio. Journal of Information Security, 4, 12-18.

[17] Sabir F. A. (2014). Hiding Encrypted Data in Audio Wave File. International Journal of Computer Applications. 91(4). 6-9.

[18] Sakthisudhan K., Prabhu P. and Thangaraj P. (2012). Secure Audio Steganography for Hiding Secret information. International Conference on Recent Trends in Computational Methods, Communication and Controls.

[19] Saurabh A. and Ambhaikar A. (2012). Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security. International Journal of Science and Research. 1(2).

[20] Tambe S. A., Joshi N. P. and Topannavar P. S. (2014). Steganography & Biometric Security Based Online Voting System. International Journal of Engineering Research and General Science. Volume 2, Issue 3. 8.

[21] Taruna and Jain R. (2014). Message Guided Adaptive Random Audio Steganography using LSB Modification. International Journal of Computer Applications. 86(7). 4-9.

[22] Gallegos-Garcia,G., Gomez-Cardenas,R and Dunchen-Sanchez, G(2010).Electronic Voting Using Visual Cryptography. Proceedings of fourth IEEE International Conference on Digital Society,IEEE Computer Society,31-36.

[23] Tatar U. and Mataracioğlu U. (2007). Analysis and Implementation of Distinct Steganographic Methods. Tübitak Uekae, Department of Information Systems Security 06700, Kavaklıdere, Ankara, Turkey.

[24] Verma S. S., Gupta R. M. and Shrivastava G. (2013). A Survey on Recent Steganography Technique Using Audio Carrier. International Journal of Advanced Research in Computer Science and Software Engineering. 3(11).

[25]Olaniyi, O.M,Folorunso, T. A.,Abdullahi I. M., and AbdulSalam, K..A(2015), "Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique .IOSR Journal of Computer Engineering, *In press.*

[26]Olaniyi, O.M, O.T Arulogun, E.O. Omidiora, & Okediran O.O (2015)," Enhanced Stegano-Cryptographic Model for Secure Electronic Voting", Journal Of Information Engineering and Applications ,5(4):1-15