Advances in Electrical and Telecommunication Engineering 1 (2018): 55-64
ISSN: 2636 - 7416

SCIENGTEX™
SCIENCE ENGINEERING TECHNOLOGY

**Advances in Electrical and Telecommunication Engineering (AETE)**

*AETE is a peer review journal of the Department of Electrical & Electronics Engineering, Ambrose Alli University, Nigeria*

# Bio-Crystographic Technique for Secure Electronic Voting System

[1]*Olaniyi, O. M., [2]Arulogun, O. T., [3]Kawonise, A. K., & [4]Ajimati, T.

*[1,4]Department of Computer Engineering, Federal University of Technology, Minna, Nigeria; [2]Department of Computer Science & Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria; [3]Department of Computer Science, Federal Polytechnic, Ede, Nigeria.*

*mikail.olaniyi@futminna.edu.ng

**ARTICLE INFO**

***Article history:***

Received 10 September 2018
Revised 30 November 2018
Accepted 7 December 2018
Published 20 December 2018

***Keywords:***

Confidentiality;
Crystography;
Electronic voting;
Gabor Filter;
Security;
Steganography.

## ABSTRACT

Democracy involves a system of governance where citizens are at liberty to actively participate in the nation's decision-making process by means of election. However, elections in most developing countries characteristically involve rigging in form of ballot snatching, falsification of votes and votes' manipulation during and after electoral processes. This can mar populace confidence in the entire electioneering process of democratic governance. This paper presents bio-crystographic technique for ensuring credibility during pre-electoral and post-electoral phases of an electioneering process. This integrated technique include: Gabor filter image enhancement scheme for biometric fingerprint trait for authenticating and validating valid voters and Lifting Wavelet Transform (LWT) based video Steganographic algorithm for ballot confidentiality, SHA 512/256 Hashing techniques for ballot integrity. Performance evaluation of these schemes resulted to an average Peak Signal to Noise Ratio (PSNR) of 66db. Also, the authentication scheme gives a False Acceptance Rate (FAR) of 0.0001% and a False Rejection Rate (FRR) of 0.1%. The results showed that the developed integrated schemes can effectively handle confidentiality, integrity and authentication issues in electronic voting systems in digitally divided electoral ecosystem.

## 1. Introduction

Democracy dates back to the classical Greek philosophers, when Aristotle argued that a large middle class may be conducive to it; hence, power or authority is not vested on the rich alone (Aminu *et al.,* 2016). This makes democracy differ from autocracy that is controlled by a selected group, giving room for transparency through a legitimate electoral process. Proper electoral process presents citizens with alternatives from which they can choose among a predefined list of delegates who are selected to settle issues of public concern. Furthermore, this can be described as a process to affirm democracy through formal decision-making process by which a populace appoints an individual to hold public offices (Abdulhamid *et al.*, 2013).

Electronic voting involves the adoption of electronic devices and interface for the purpose of appointing officials into power (Oke *et al.,* 2017). Over the years, electronic voting has been considered the best platform for electorates to express their vote with minimum effort and less time wastage (Okediran & Ganiyu, 2015). However, this system has been identified with technical vulnerabilities, few of which includes: voter's authentication in form of failed Smart Card Readers (SCR) (Osho *et al.*, 2015), Subscriber and Identification

**Please, cite this article as**: Olaniyi, O. M., Arulogun, O. T., Kawonise, A. K., & Ajimati, T. (2018). Bio-Crystographic Technique for Secure Electronic Voting System, *Advances in Electrical and Telecommunication Engineering, 1*(2): 55-64. Retrieved from: https://www.sciengtexopen.org/index.php/aete/article/view/21

Module (SIM) and voter's biometric fingerprint verification issues (Ibeh, 2015), result accuracy and post electoral auditing issues (Olaniyi *et al.,* 2016). As a result of these vulnerabilities in the electronic voting system, the development of different security measures becomes paramount.

Electronic voting requires many security measures, which creates the borderline between e-voting and paper ballot voting. A secured electronic voting system is a system that ensures some degree of trust that enforces expected confidentiality, integrity, availability, verifiability and authenticity to the process of elections. A secure e-voting system is expected to fulfil requirements such as authentication, uniqueness, accuracy, anonymity, integrity, verifiability, auditability, reliability and secrecy. Existing security measures from literatures include: the application of different biometric traits, firewalls, cryptography, smart cards and steganography (Oke *et al.,* 2017). Several techniques for securing electronic voting systems exist (Abdulhamid *et al.*, 2013; Aminu *et al.,* 2016; Aranuwa & Oriola, 2012; Enokela & Osuagwu, 2011; Kumar & Singh, 2012, Oke *et al.,* 2017; Olaniyi, *et al.,* 2013; Osho *et al.,* 2016).

In this paper, confidentiality, integrity and authentication latency security issues in electronic voting systems using biometrics and crystographic techniques are addressed. Crystography involves the simultaneous application of information hiding techniques of steganography and cryptography for enhancing the security of communications over enterprise network (Gabriel *et al*, 2013; Mihir, 2012; Olaniyi *et al.*, 2017; Rura *et al.,* 2017). Cryptographic application in the context of this paper, involves securing electronic voting system using Lifting Wavelet Transform (LWT) based video Steganographic algorithm, SHA 512/256 cryptographic hashing techniques for ballot integrity. In addition, the schemes developed by Aminu *et al.* (2016), Osho *et al.* (2016) and Rura *et al.* (2017) for secure e-voting was improved upon by addressing pre-electoral authentication issues, electoral confidentiality issues and post electoral ballot auditing integrity issues through synergistic applications of Gabor filter image enhancement scheme on biometric fingerprint trait for authenticating and validating valid voters and the LWT based video Steganographic algorithm for ballot confidentiality, SHA 512/256 Hashing techniques for ballot integrity for secure electronic voting system in digitally divided democratic scenarios. The rest of this paper is organised into three sections. System hardware and software design considerations are presented in Section 2, Results and discussion are presented in Section 3, while Section 4 concludes and provides scope for future research.

## 2. Materials and Methods

The system architecture for the proposed techniques shown in Figure 1 comprised of two major components, which include: the Software and the hardware. The hardware component consists of the uni-modal fingerprint biometric and an Arduino development board. However, the software component consists of video steganographic algorithm and truncated SHA-512/256 hash function. The fingerprint biometric device validates authentication as it affects the electronic voting system. The microcontroller in Arduino Uno receives a 5V direct current through a USB connector from with which the fingerprint sensor is been powered. Whenever the fingerprint module is powered and a finger is placed on its sensor surface, it automatically detects the finger and sends a signal to the micro controller unit which decides either to grant a voter access to vote or not.

During voter authentication, the microcontroller compares the newly supplied fingerprint template with the ones stored in database. If it ascertains the existence of a match between the latter and the former, it automatically sends a string of data to the software application to launch an access page for the user where they can easily cast their vote. The proposed techniques are designed around kiosk type electronic voting system. Electorates are to visit any kiosk site for full participation in the electioneering process. The secure e-voting system is structured into three different phases with each phase handling it unique affairs as shown in Figure 2.

The functional diagram in Figure 2 was designed around hardware components and a program which runs on the microcontroller chip (ATMEGA 328P) embedded on Arduino board which serves as the brain of the system. The R305 fingerprint module sensor was selected to perform fingerprint enrolment, image processing, matching, searching, and template storage into database. The sensor can perform 1:1 matching or 1: N matching of sensor's real time image and equivalent minutiae stored in database. It employs the UART protocol to communicate with the host microcontroller. The default baud rate is usually 57600 bps though the module can support from 9600 to 115200 bps. The module makes use of an image buffer and two 512-byte character file buffers, which are volatile, and non-volatile flash memory for storing fingerprint templates and permanent settings. The module has four connecting pins; TX, RX, Ground and VCC (+5) as shown in Figure 3.

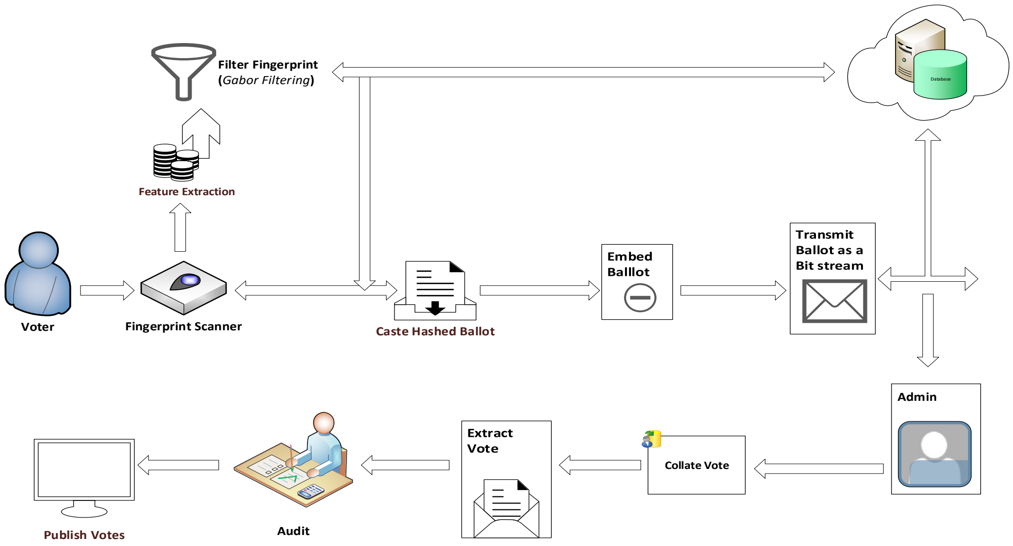


**Figure 1:** Architecture of secure electronic voting system

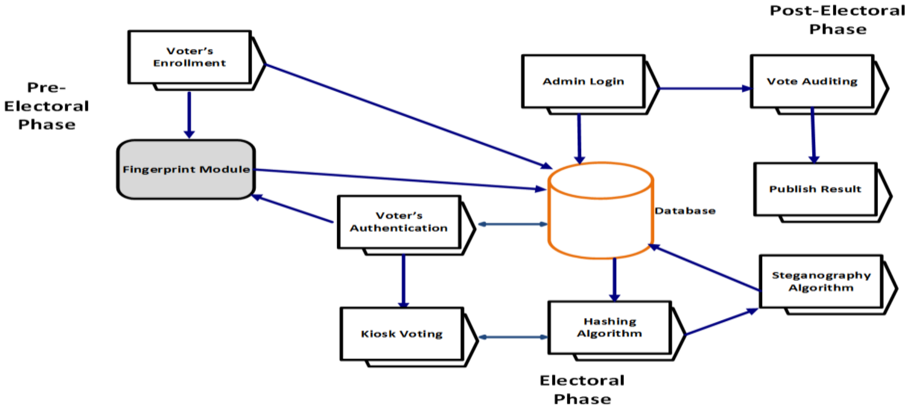


**Figure 2:** Secure electronic voting system functional diagram

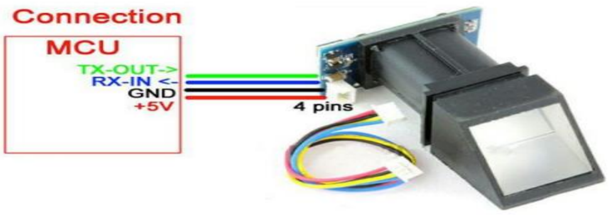


**Figure 3:** R305 Fingerprint Module

The R305 fingerprint module sensor power supply was from microcontroller chip (ATMEGA 328P) embedded on Arduino board through a Universal Serial Bus (USB) connector. The Arduino UNO board is rated 5V (DC), this voltage was regulated to meet the power requirement of the ATmega328P chip of 3.3V at maximum current of 50mA and that of the fingerprint sensor rated at 3.3V in (1). The Voltage Divider Rule

(VDR) theorem was applied through a linear voltage regulator to reduce the input voltage of 5V to meet up with 3.3V rating required by R305 sensor as follows:

$$V_{out} = \frac{R_2}{R_1 + R_2} \times V_{in} \quad (1)$$

where $V_{\text{in}}$ = 5V, $R_1$ = 1kΩ and $R_2$ = 1.95kΩ; hence,

$$V_{out} = \frac{1950}{1000 + 1950} \times 5 \;= 3.3V$$

## *2.1 Crystographic Algorithms*

Digital communication is growing rapidly daily and the internet is the most popular medium for digital communication. However, data transmission through the internet is faced with many challenges such as data confidentiality and integrity. Hence, the act of secret communication through crystography or simultaneous application of information hiding techniques of steganography and cryptography for preserving the security of data communications over unsecured channel. These algorithms are defined as follows:

***Steganographic definitions:*** Steganography is a digital camouflaging security technique for the purpose of hiding information from an adversary. It can also be described as the art and science of disguising the existence of a message (Olaniyi *et al.*, 2013, Rura *et al.,* 2017). The proposed scheme is based on video steganography based on Lifting Wavelet Transform (LWT). When implementing LWT on a video object, the video is first transformed into its sub-images. The sub-image is divided into four sub bands each of which represent a region in the given image. The sub bands are: Lower resolution approximation component (LL), horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub band is obtained after low-pass filtering of both the rows and columns and has the maximum information content.

Generally, Since the high frequency sub-bands (HH) only deals with the edges and textures of an image at which the human eye is not obviously sensitive to changes in such sub-bands the LWT algorithm is applied at the high frequency sub-band (HH) and since most of the image visual elements are concentrated at the lower frequency sub-bands (LL) and hence, applying LWT at the lower frequency sub-bands will significantly degrade the image quality thereby lowering the PSNR value.

***Cryptographic definitions:*** The proposed cryptographic scheme was designed around truncated SHA-512/256 hashing algorithm, implemented on the digital ballot file. The hashing function was applied on the ballot before vote casting; hence, the hashed ballot is been embedded into a cover video for transmission. At the vote auditing phase, the extracted ballot (Hashed) is compared with the un-hashed ballot to affirm its integrity. If there exist any variation between the extracted ballot and the un-hashed ballot then it will be concluded that the integrity of the vote in question has been compromised and the vote is declared invalid. The procedure for SHA-512/256 hashing algorithm is presented Figure 4.

The truncated SHA-512/256 hash algorithm was implemented with C#, using visual studio as a coding environment. The algorithm was implemented as follows:

Step 1: Compression function, SHA 512 is an iterated hash function that pads and processes the input message using t 1024-bit message block $m_j$. The hash value of 512-bit hash value is computed using the compression function f;

$$h_0 = IV \quad (2)$$

$$h_{j+1} = f(h_j, m_j) \quad for\; 0 \le j < t \quad (3)$$

Hash output is the final 512-bit chaining value $h_t$.

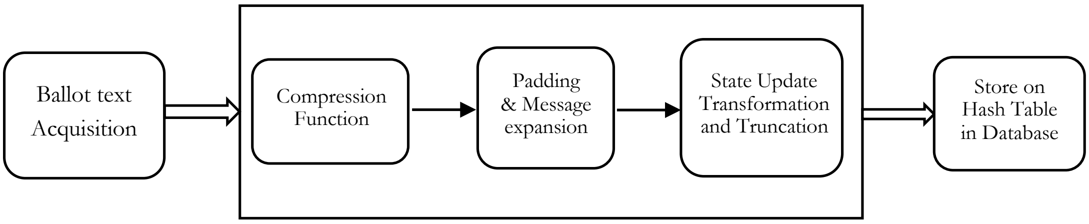

Ballot text Acquisition
Compression Function
Padding & Message expansion
State Update Transformation and Truncation
Store on Hash Table in Database

**Figure 4:** Flow process diagram of the truncated SHA 512/256 hash function

Step 2: Padding and message expansion, the message expansion of SHA-512 separates each 1024-bit message block into 64-bit words $M_i$ , $i = 0, \ldots \ldots, 15,$ and then increases these into 80 lengthened message words $W_i$ as:

$$W_i = \begin{cases} M_i \\ \sigma_1\,(W_{i-2}) + W_{i-7} + \sigma_0\,(W_{i-15}) + W_{i-16} \end{cases}, 0 \leq i < 16,\ 16 \leq i\ < 80 \tag{4}$$

Step 3: The state update transformation (Dobraunig *et al.,* 2015),starts from the value $h_j$ ,

$$h_j\ = (A_{-1}, \ldots, A_{-4}, E_{-1}, \ldots, E_{-4}) \tag{5}$$

The previous 512-bit chaining and updates it by applying the step functions 80 times. In each step $i = 0, \ldots, 79$, $W_i$ (one 64-bit expanded message word) is used to compute the two state variables $E_i$ and $A_i$ as demonstrated in (5).

$$E_i = A_{i-4} + E_{i-4} + \textstyle\sum_1(E_{i-1}) + IF \sum_1(E_{i-1}, E_{i-2}, E_{i-3}) + K_i + W_i,$$
$$A_i = E_i - A_{i-4} + \textstyle\sum_0(A_{i-1}) + MAJ \sum_1(A_{i-1}, A_{i-2}, A_{i-3}). \tag{6}$$

Following the last step of the state update transformation, the previous chaining value $h_j$ is included to the output of the state update. The output of the feed-forward sum is the chaining value $h_{j+1}$ for the subsequent message block $m_{j+1}$ (or the final hash value $h_t$):

$$h_{j+1}\ = (A_{79} + A_{-1}, \ldots, A_{76} + A_{-4}, E_{79} + E_{-1}, \ldots, E_{76} + E_{-4}). \tag{7}$$

The truncated variant of SHA-512 differs only in its initial values and the final truncation to 256 bit, while the rest of the algorithmic description does not change. The message digest of SHA-512/256 is obtained by neglecting the output words $E_{79} + E_{-1}$, $E_{78} + E_{-2}$, $E_{77} + E_{-3}$, and $E_{76} + E_{-4}$ of the last compression function call. The truncated SHA 512/256 have same security strength as SHA-512, the only exception is in the resulting output which uses Equation 15 to set the initialisation vector

$$IV_{512t} = SHA512(T) \tag{8}$$

### *2.2 Finger Print Image Enhancement Using Gabor Filter*

A major approach in automatic fingerprint matching is to automatically and reliably extract minutiae from a collected fingerprint template. Nevertheless, the performance of a minutiae extraction algorithm place high value on the quality of the fingerprint image, it is necessary to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. The Gabor filtering technique is proposed. A Gabor filter, named after Denis Gabor applies its impulse response as the multiplication of a harmonic function with a Gaussian function. As per *convolution theorem*, the convolution of Fourier Transformation (FT) of harmonic function and FT of Gaussian function is nothing but FT of a Gabor filter's impulse response:

$$[\mathrm{FT}(Gabor) = FT(Harmonic)\ FT(Gaussian)\,] \tag{9}$$

The filter consists of a real and an imaginary component, which represent the orthogonal directions. The two components are used individually or in a complex form. The application of Gabor filter strikes through factors like face recognition, texture classification, facial expression classification and fingerprint image compression and optimization. The synergy of Gabor filter with a fingerprint authentication system will greatly minimise the problems of fingerprint image errors by optimizing low image quality and effect of noise on feature extracted from enrolled image. When using fingerprint biometrics for user authentication, a finger code is first created before the resultant

### *2.3 Techniques Performance Evaluation Measures*

In order to evaluate the confidentiality and integrity of the proposed techniques, a steganalytic measure using Invisible secret software was employed to analyse and detect the ballot text in the stego video. Also, the mean square error (MSE), peak signal to noise ratio (PSNR) and structural similarity index measures (SSIM) are metrics used for evaluating stego image frame quality and vital characteristic features were also evaluated. These measures are defined as follows:

***Computation of embedding capacity of stego video:*** This is utilised to allude to the most extreme sum of data that can be covered up inside a cover video without subsequently harming the nature of the video medium. It is ascertained by assessing the proportion of the measure of secrete message to that of the cover video in question as defined by (10).

$$EC = \frac{Size\ of\ secrete\ message}{Size\ of\ cover\ message}, \tag{10}$$

where EC is the embedding capacity.

**Computation of MSE and PSNR Metrics:** These measures are utilized to assess the measure of similarity that exist between the cover video and it respective stego video document. PSNR is a capacity of the MSE, a proportion of value estimation between the two media computed in decibels. The higher the PSNR of the correlation, the better the examination exhibiting low contortion of the stego record created from cover video. MSE and PSNR are defined as presented in (11) and (12) respectively.

$$MSE = \frac{\sum M,N[\mathrm{I}_1(m,n)-I_2(m,n)]^2}{M*N} \tag{11}$$

$$P\mathrm{SNR} = 10\ \log_{10}\frac{\boldsymbol{R^2}}{\boldsymbol{MSE}} \tag{12}$$

Where *M* and *N* are the rows and columns of the video frames respectively and *R* is the minimum fluctuation in the stego medium, which is usually 255 in integer data type.

These two performance metrics are inversely proportional to each other. The value of PSNR increases when two images are close to each other whereas the value of MSE decreases when the two frames are similar to each other. Using PSNR, images of values above 30db are said to be of high quality.

***Structural Similarity Index Measure*:** The SSIM index is a technique for measuring the similarity between two media. The original image is used as a reference while the other is used for comparing. SSIM estimates the visual impact of shift in Image frame luminance, changes in photograph contrast which are collectively identified as structural changes in image frame (Olaniyi *et al.*, 2014). For two image frames $x$ and $y$ of common size $N * M$, the SSIM is given by the equation:

$$SSIM(x,y) = \frac{[(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)]}{[(\mu_x^2+\mu_v^2+C_1)(\sigma_x^2+\sigma_y^2+C_1)]}, \tag{13}$$

where $\mu_x$ is the average of $x$, $\mu_y$ is the average of $y$, $\sigma_y^2$ is the variance of $y$, $\sigma_{xy}$ is the covariance of $x$ and $y$, $C_1 = (k_1L)^2$ and $C_2 = (k_2L)^2$ are two variables to stabilise 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 (13) approaches 1, the greater the degree of fidelity of the compressed image is close to the original image (Abdulsalam *et al*, 2017). The dynamic range of (13) is given as follows:

$$SSIM = [-1, +1] \tag{14}$$

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 (Olaniyi *et al.,* 2014).

***Fingerprint evaluation:*** The fingerprint biometric system was evaluated using standard metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR) with threshold range of 0.3 to 1.

## 3. Results and Discussion

The developed prototype of the hardware component is presented in Figure 5 while Table 1 and Table 2 show the results of different user trials on the authentication module of Figure 5 with different threshold set values to ascertain efficiency of the authentication module. The results of FRR in Table 1 gives the degree to which the system wrongly accepts invalid users while the results of FAR in Table 2 shows the degree to which the authentication system wrongly rejects a legitimate user.

Figure 6 shows the original and the stego frames. The cover frame (Figure 6a) is the specific frame selected from the original video for embedding the secrete message while the stega frame (Figure 6b) is the new frame generated as a result of applying the LWT based video steganography algorithm. As observed (Figure 6), it is very impossible to perceive any possible difference between the cover frame and stega frame when analysed visually. Hence, the difference between the stega and cover image is imperceptible and thus maintain the confidentiality of the casted ballot. Figure 7 shows the histogram equalisation of original and the stega frames.

**Table 1:** False reject rate for fingerprint data collected

| **Threshold**<br>**(%)** | **Matching**<br>**Attempts** (*N*) | **False Rejects**<br>(*n*R) | **FRR**<br>(*n*R/*N*) | **%FRR**<br>(*n*R/*N*) x 100 | **True Acceptance Rate**<br>(*1-FRR*) x 100% |
|---|---|---|---|---|---|
| 0.335 | 50 | 2 | 0.04 | 4.0 | 96.0 |
| 0.443 | 50 | 1 | 0.02 | 2.0 | 98.0 |
| 0.656 | 50 | 2 | 0.04 | 4.0 | 96.0 |
| 0.868 | 50 | 3 | 0.06 | 6.0 | 94.0 |
| 1.000 | 50 | 5 | 0.10 | 10 | 90.0 |

**Table 2:** False acceptance rate on fingerprint data collected

| **Threshold**<br>**(%)** | **Matching Attempts**<br>(*N*) | **False Acceptance**<br>(*n*R) | **FAR**<br>(*nA*/*N*) | **% FAR**<br>(*nA*/*N*) x 100 |
|---|---|---|---|---|
| 0.335 | 50 | 0 | 0.00 | 0.00 |
| 0.443 | 50 | 2 | 0.04 | 4.00 |
| 0.656 | 50 | 3 | 0.06 | 6.00 |
| 0.868 | 50 | 4 | 0.08 | 8.00 |
| 1.000 | 50 | 5 | 0.10 | 10.0 |

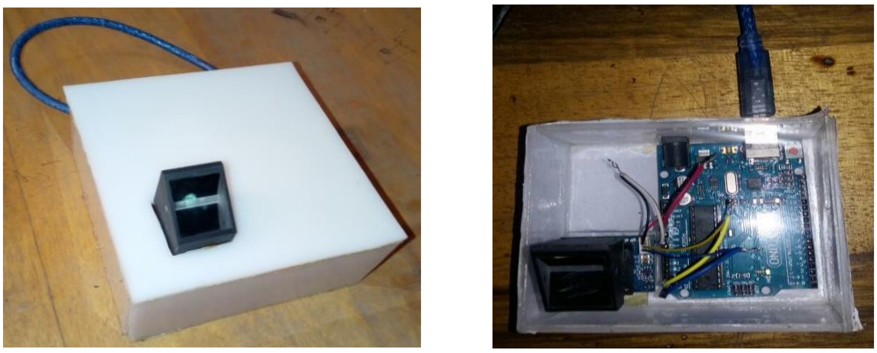
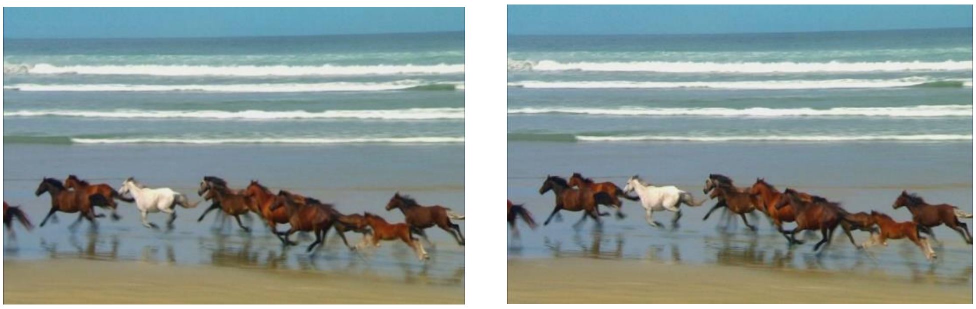
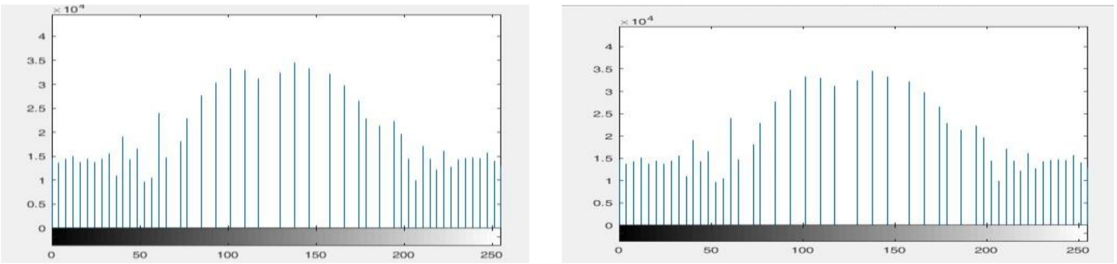


**Figure 5:** Cross-sectional views of developed prototype system authentication skeletal module



(a) (b)

**Figure 6:** Frames (a) Cover Frame (b) Stega Frame



(a) (b)

**Figure 7:** Histogram equalisation for (a) Cover Frame (b) Stega Frame

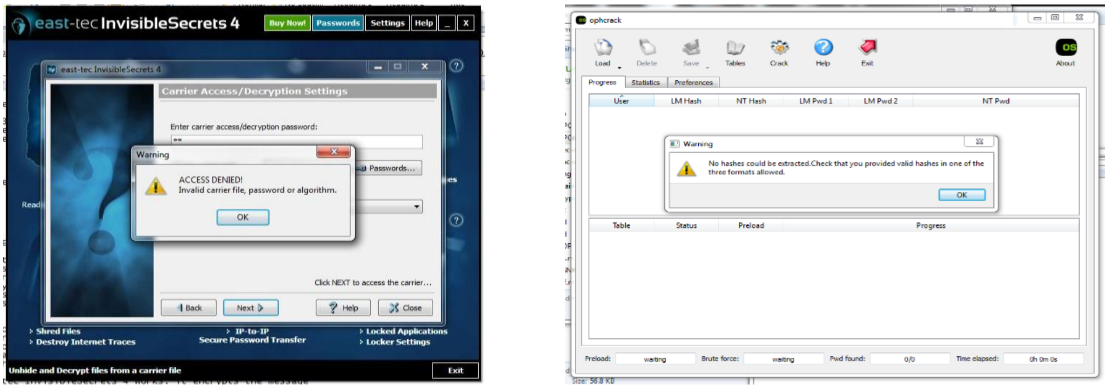
The cover frame is the specific frame selected from the original video for embedding the secrete message while the stega frame is the new frame generated as a result of applying the steganography algorithm. Through visual analysis, it was impossible to perceive any possible difference between the cover frame and stega frame. Hence, the difference between the stega and cover image is imperceptible and thus maintain the confidentiality casted ballot.

It is observed from the quantitative results of the video metrics analysis shown in Table 3 that an increase in the number of video frame has only little or no change in visual quality. However, rescaling the matrix size shows a sudden increase in the PSNR value. This simply implies that increase in the frame dimension will simultaneous result to an increase in the embedding capacity. Also, this will ameliorate any possible distortion of the secrete message. The PSNR value of results (presented in Table 3) shows that all PSNR values are greater than 60db, which depicts a high quality when using the human visual system (HVS). The structural similarity index as shown in Table 3 proves that the image similarity index is highly negligible and at an acceptable level.

**Table 3:** Result of video metrics analysis

| S/N | Frame size | Number of Frames | Vote Size (byte) | PSNR | SSIM |
|---|---|---|---|---|---|
| 1 | 512 x 512 | 20 | 25 | 69.4159 | 1 |
| 2 | 512 x 512 | 50 | 25 | 68.6425 | 1 |
| 3 | 720 x 1280 | 50 | 25 | 73.0320 | 1 |
| 4 | 720 x 1280 | 20 | 25 | 73.0320 | 1 |
| 5 | 720 x 1280 | 100 | 25 | 73.0320 | 1 |

There exists numerous software developed for the detection and identification of suspected payload transmitted over the internet. The major goal is to detect a suspected carrier and determine any possible payload. Invisible secret was used to investigate stego video as shown in Figure 8a to ascertain the performance of the transform based video Steganographic algorithm. Also, Hopcrack software package was employed in checking the integrity of the hashed ballot using truncated 512/256 hashing algorithm. The result of the hash attack result is as shown in Figure 8b. As can be observed from Figure 8(a), the invisible secret stega analysis software could not decrypt or sense the presence of a payload in the stega-file neither was the password cracking tool in Figure 8(b) able to detect the hashed vote as would have been possible with most hashed files and passwords. Hence, the aim of ballot hiding has been successfully achieved.



Carrier Access/Decryption Settings

Enter carrier access/decryption password:

Warning

ACCESS DENIED!
Invalid carrier file, password or algorithm.

Click NEXT to access the carrier...

Unhide and Decrypt files from a carrier file

(a)

Warning

No hashes could be extracted.Check that you provided valid hashes in one of the three formats allowed.

Preload: waiting Brute force: waiting Pwd found: 0/0 Time elapsed: 0h 0m 0s

(b)

**Figure 8:** Attacking the stega file using (a) invisible secrete and (b) hopcrack software

## *3.1 Performance Comparison*

The performance of the developed scheme was compared with other relevant schemes from the literature as presented in Table 4. It can be clearly seen that the scheme developed in this paper provides countermeasures to meet fundamental e-Voting security objectives of Authentication, Confidentiality, Integrity and Vote Auditing threats peculiar to pre-electoral, electoral and post-electoral issues. The developed scheme is comparable to these baseline schemes and better in majority of some considered features.

**Table 4:** A comparison of secure electronic voting schemes

| Criteria | Enokela & Osuagwu (2011) | Osho *et al.* (2016) | Aminu *et al.* (2016) | Rura *et al.* (2017) | Proposed scheme |
|---|---|---|---|---|---|
| Security goal addressed by scheme | Authentication only | Confidentiality and Integrity only | Vote auditing and verification only | Authentication, confidentiality, integrity | Authentication, Confidentiality, Integrity and Vote Auditing |
| Countermeasure for voter's authentication | None | Fingerprint biometrics | None | None | Gabor's Filter enhanced Fingerprint biometrics |
| Countermeasure for vote confidentiality | None | RSA Asymmetric Algorithm | None | Hash scheme, visual cryptography and threshold decryption | Steganographic approach: Lifting Wavelet Transform |
| Countermeasure for post electoral ballot auditing integrity | None | None | None | None | Truncated SHA 256/512 |
| Proof of concept for the developed scheme | Yes | No | No | No | Yes |

## 4. Conclusion and Recommendations

This paper has successfully presented an essentially new perspective for addressing the authentication, confidentiality and integrity issues of a secure electronic voting system. It synergises the application Gabor filter based fingerprint biometrics, cryptographic hash function and steganography methods for the accomplishment of the predefined objectives. The strength of this paper lies on the integration of both cryptographic and stenographic procedure for high security assurance in e-democratic decision making. Seamless application of proposed techniques in secure electronic voting system will help encourage more participation of citizens in the electioneering process and also help makes vote casting credible and faster. The following observations are suggested for future research:

(a) integrating the system with other access control mechanism for physically challenged populace;

(b) exploration of linguistic Steganographic schemes for ballot confidentiality; and

(c) qualitative user acceptance evaluation of the developed proof of concept on pilot testing with large direct-recording, online poll-site, and remote e-voting scenarios.

## Conflict of Interests

Authors declare that there is no conflict of interests regarding the publication of this paper.

## References

Abdulhamid, S. M., Adebayo, O. S., Ugiomoh, D. O., & AbdulMalik. M. D. (2013). The design and development of real-time e-voting system in Nigeria with emphasis on security and result veracity. *International Journal of Computer Network and Information Security*, *5*(5): 9-18.

Abdulsalam, Y. S, Olaniyi O. M., & Ahmed A. (2017). Securing electronic health systems using enhanced transform domain image watermarking technique. *Computing, Information Systems, Development Informatics & Allied Research Journal, 8*(2): 103-118.

Aminu, F. E., Abdulmalik, A., & Zubairu, H. A. (2016). A framework for pre and post vote cast audit to enhanced electronic voting. *International Conference on Information and Communication Technology and Its Applications*, 28 – 30, Minna, Nigeria.

Aranuwa, F.O. & Oriola, O. (2012). Improved electoral fraud prevention mechanism for efficient.electronic voting. *African Journal of Computing & ICT, 5*(6): 70-77.

Dobraunig, C., Eichlseder, M., & Mendel, F. (2012). Analysis of SHA-512 / 224 and SHA-512 / 256. In: Iwata T., Cheon, J. (eds) Advances in Cryptology – ASIACRYPT 2015. *Lecture Notes in Computer Science, 9453. Springer, Berlin, Heidelberg.*

Enokela, J. A., & Osuagwu, C. C. (2011). An algorithm for the conduct of multiple simultaneous multi-party elections using a microcontroller. *Pacific Journal of Science and Technology*, *12*(2): 253-259.

Gabriel, J. A., Alese, K. B., Adetumbi, A. O., & Adewale, O. S. (2013). Post-quantum crystography: a combination post-quantum cryptography and steganography. *Proceedings of the IEEE 8th International Conference for Internet Technology and Secured Transactions,* USA, 449-552.

Ibeh. N. (2015). Premium Times. Retrieved from http://www.premiumtimesng.com/news/top-news/179447-3-cardreaders-fail-to-accredit-jonathan.html (March, 2015)

Kumar, S., & Singh, M. (2012). Security enhancement of e-voting system, *Global Journal of Computer Science and Technology*, *12*(5):1-7.

Mihir, H. R. (2012). Crystography-combination of cryptography and steganography with rapidly changing keys. *International Journal of Emerging Technology and Advanced Engineering, 2*(10): 329-332

Oke, B., Olaniyi, O. M., Aboaba, A. A., & Arulogun, O. T. (2017). Developing multifactor authentication technique for secure electronic voting system. In Misra, S. Matthews, V. O. & Adewumi, A. (Ed.), *IEEE International Conference on Computing, Networking and Informatics,* 48-53, Ota: Covenant University, Canaanland, Ota, Ogun State, Nigeria.

Okediran, O. O., & Ganiyu, A. A. (2015). Framework of electronic voting in Nigeria. *International Journal of Computer Applications*, *129*(3):12-16

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Adeoye O. (2013). Design of secure electronic voting system using multifactor authentication and cryptographic hash functions, *International Journal of Computer and Information Technology, 2*(6):1122-1130

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Okediran, O. O. (2014). Performance evaluation of modified stegano-cryptographic model for secured e-voting. *International Journal of Multidisciplinary in Cryptology and Information Security, 3*(1): 1-8.

Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Okediran, O. O. (2013). A Survey of cryptographic and stegano-cryptographic models for secure electronic voting system. *Covenant Journal of Informatics & Communication Technology*, *1*(2): 54–78.

Olaniyi, O. M., Arulogun, O. T., Omotosho, A., & Onuh, O. V. (2017). Securing clinic tele-diagnostic system using enhanced tiny encrypted radio frequency identification and image steganographic technique, *International Journal of Telemedicine and Clinical Practice, 2*(3): 242–266.

Olaniyi, O. M., Folorunso, T. A., Abdullahi, A. M., & Abdulsalam. A. 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,17*(6): 86-97.

Olaniyi, O. M., Folorunso, T. A., Ahmed, A., & Joseph, O., (2016). Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. *International Journal of Information Engineering and Electronic Business*, *5*, 9-17.

Osho, L, Abdullahi, M. B., & Osho, O. (2016). Framework for an e-voting system applicable in developing economies. *International Journal of Information Engineering and Electronic Business*, *8*(6): 9-21.

Osho, O., Yisa, V. L., & Jebutu, O. J. (2015). E-voting in Nigeria: a survey of voters perception of security and other trust factors,in cyberspace (CYBER-Abuja), *2015 International Conference*, 202–211.

Rura, L., Biju, I., & Haldar, M. K. (2017). Online voting system based on image steganography and visual cryptography. *Journal of Computing and Information Technology*, *25*(1): 47-61.