I.J. Information Engineering and Electronic Business, **2016, 5, 9-17**
Published Online September 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2016.05.02

Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach

Olayemi M. Olaniyi, Taliha A. Folorunso, Aliyu Ahmed, Olugbenga Joseph
Federal University of Technology/Computer Engineering Department, Minna, P.M.B 65, Nigeria
Email: mikail.olaniyi@futminna.edu.ng;funso.taliha@futminna.edu.ng;aliyu.ahmed@futminna.edu.ng;
oluwagbemiga.joseph@st.futminna.edu.ng

***Abstract*—**The conventional voting scheme employs paper-based ballot to verify votes. This voting scheme is insecure due to the attributed shortcomings including ballot stuffing, ballot snatching and voter's impersonation. In this paper, we present the design and development of secure e-voting to ensure a free, fair and credible election where the preference of electorate counts. This proposed system solves the authentication, integrity and confidentiality security issues of e-voting in kiosk and poll site evoting scenarios using unimodal fingerprint biometrics and Advanced Encryption Standard based Wavelet based Crypto-watermarking Approach. The developed system solves: The possibility of blundering voter's authentication, integrity and confidentiality of vote stored in the server. The results after qualitative evaluation of the system with anti-watermarking detectors revealed that the developed secure e-voting system could serve as a platform for the delivery of credible e-election in developing countries with significant digital divides.

Index Terms—E-voting System, Fingerprint Biometric, Cryptography, Authentication, Integrity, Confidentiality, Watermarking.

I. Introduction

Democratic system of governance is based on election of representatives into position of authorities solely by populace. Democracy follows the rule of law where equal rights are awarded to all the electorates [1].Election is well-defined as a formal decision-making process by which a population chooses an individual to hold public office. Also, election is a process to affirm democracy [2]. Logically, the integrity of the voting process is central to the integrity of democracy [3]. The balloting framework needs to be sufficiently robust to tolerate diverse fraudulent activities and must be sufficiently straightforward such that voters and aspirants can acknowledge the outcomes of an election [4].

In customary voting system, the voting process embraces physical balloting of voters' choice [3]. The paper polls are perused and interpreted by voting authority. The outcomes for all contestants are separately arranged and showed. The physical presence of the voter is obliged because the fingerprint of specific registered electorate is utilized to vote. Even though, the configuration of a voting framework whether electronic, paper-based or mechanical designed must fulfill various contending criteria; these conditions are [1]: the privacy and alteration resistance of an electorate vote, aimed at guaranteeing electorate security when voting against a malicious contestant; and to ensure that voters have no proof that demonstrates which candidates they voted for. The presence of such proof would permit votes buying by a candidate [4]. The voting framework should also be robust enough to withstand various attacks, such as multiple voting by electorates and inaccurate counting by polling officers [5].

The conventional voting scheme has been linked to several elections irregularities including ballot stuffing, ballot snatching and voter impersonation which are linked to voter's ignorance and carelessness [3]. This voting scheme is insecure due to these attributed election irregularities. The most important issue about e-election is that, it depends on the accuracy, toughness, and security of the software in the polling station [6]. Due to high rate of electoral malpractices that can be perpetrated in e-voting system, secure electronic voting system is presented in this paper through fingerprint biometric of electorates and crypto-watermarking on electronic vote. Cryptography is the science of hidden communication from an adversary and watermarking is the science of embedding hidden information inside a multimedia data for secure communication. The synergistic combination of the two techniques symbolizes a well-organized technology for guaranteeing data veracity and data-origin genuineness [3, 15]. To improve voter authentication distinctiveness attribute to secure electorates from identity theft, fingerprint biometrics authentication has been adopted. Fingerprint authentication process reduces threats posed by identity theft, phishing, online fraud which dents confidentiality of democratic decision making process. So, voting schemes need to apply an operational authentication system to further make elections free, fair and reliable.

Electronic voting is a social information system for making electoral process, efficient and increasing trust in its administration. Properly executed e-voting solutions can speed up the processing of results and make voting stress-free [3]. However, challenges such as denial of service, increased vulnerability to security threats like malware and man-in the middle attacks make e-voting and e-voting system vulnerable to insecurity. If not carefully designed, e-voting can undermine the confidence in the whole electoral process as seen in manual ballot system. Information security has to do with safeguarding information and information systems from unapproved exposure, access, interference, modification, review, assessment, obliteration or recording [3, 7]. While trying to accomplish efforts to establish security in e-voting system, major security requirements to satisfy are Integrity, Non-repudiation, Confidentiality, and Authentication.

Voting is central to all democratic proceedings. Hence, the proficiency, dependability, and security of the technique employed are vital. In this work, we present the development of a crypto-watermarking model for a secured electronic voting system in an e-democratic stimulated nation where prominence in piloting fair, transparent and reliable elections is required [1, 3, 8]. The developed system is basically designed for securing electronic voting system by guaranteeing authentication, integrity and confidentiality of voters and vote during electoral process.

The remaining sections of the paper is organized into five: Section II presents the review of related works, Section III provides the system design philosophy, Section IV presents system development, the results of system qualitative evaluation were presented in Section V, while Section VI concluded and provided scope for future works.

II. Related Work

Numerous authors have proposed various secured electronic voting system using protocols, models and algorithms designed around biometrics, watermarking, cryptography and combination of any of these techniques for credible democratic e-governance. In [9], authors proposed and implemented secured electronic voting system using Identity Based Cryptography enhanced with Bilinear Pairings. The advantage of this method is the use of complexity assumptions rather than primitive protocols based on Public Key Infrastructure. This protocol does not require the entire infrastructure for implementation. Furthermore Private Key Generator (PKG) was used to develop bilinear maps to produce public, private, and shared keys to encrypt votes and advance the protocol development. The challenge of the proposition in [9] was that there exists an uneven distribution of private key among parties which gave rise to numerous trust authorities.

In [1], authors focused on rapid innovation in Information and Communication Technology (ICT) which created new systems that were unimaginable some years back. They formulated requirements, design and implementation of an all-purpose and secure electronic voting system using fingerprint biometric and Rivest, Sharma and Adelman (RSA) cryptographic technique that allows voting at anywhere, anytime through electronic devices that include: mobile phones, private computer networks and web. Furthermore, comparisons were made between electronic voting system and manual based voting systems; evaluated the defects noticed in manual voting system and proposed methods on how e-voting could eradicate perceived errors. Different possibilities of implementing electronic voting system on different platforms were also proposed.

In [8], detailed authentication approach in safeguarding transaction through use of multidimensional cryptographic systems was proposed and emphasis was laid on the use of both the financial institution authentication and mobile station authentication. Similarly in [10], a voting machine and fingerprint identification algorithm was used in e-voting system. Fingerprints are transformed into 64-byte format by applying a prescribed algorithm, the flash memory of the microcontroller was used as prints storage. The fingerprints were collected using fingerprint module and fingerprints were compared byte on byte with stored template in memory to verify their matching and identify the owner, thus aiding the microcontroller to voluntary make decisions as to confirm the individual's status whose fingerprint was read. The choice made is conveyed through interrupts to additional PIC18F2685 microcontroller that controls the package that coordinates the voting progression in the electronic voting machine. Fingerprints usage does not only permit the voters' privacy but also safeguards a one man one vote scheme. The method solved authentication, privacy and secrecy issues but do not solve the integrity security of vote and availability of data if there is failure in the voting machine.

Furthermore,[11] designed and implemented a secure voting system using Discrete Wavelet Transform (DWT) and a multi-layer security that evolves around fingerprint, Arnold transformation and Kekre's YCgCb colour spacing. The voting system provided a much secured and highly robust secured e-voting system as the PSNR value of 45.32 and NC of 1 were obtained which were substantially accepted values. The watermark and the cover image were decomposed at three (3) levels using 2D wavelet decomposition tool. The YCgCb colour space was separated relative to the traditional RGB colour space to get the values that relate Y, Cg, Cb mathematically. It was observed that the Cg component carries more of the low frequency component and provides more robust system. Hence, Cg component was selected as reference component. The key defect of their approach is that the administrative part required in e-voting system was not covered and the fingerprint authentication employed does not give room to be deployed on mobile platforms.

Also, a method using an ARM microcontroller based module and an android application to carry out online voting was proposed in [12]. At voter's end, there was a thumbprint terminal. The actual android program was developed based on the end-user location, ID of the electorate, ID of certified person and vote can be simultaneously delivered to a particular server. During voting process, data is encoded using ECC algorithm and the user's ID was deciphered and matched with records. If the authentication matches that in the database, then the server receives the vote and delivers it to ARM7 built EVM kit.

In this work, we present the design and development of a unimodal fingerprint biometrics and Advanced Encryption Standard (AES)-Wavelet based Crypto-Watermarking aimed at securing electronic voting system for e-democratic stimulated nations that emphasizes delivery of free, guaranteeing authentication, integrity, and confidentiality in data transfer over the network

III. System Design

The aim of system design is to formulate a procedural solution that can fulfill the functional requirements for secure scheme for e-democratic governance. The architecture that describes the components and interfaces of the entire system derived from system requirements are modeled to solve identified problem using unified process modeling technique in Unified Modeling Language.

A. Requirements Definition for the Secure E-voting System

Every voting system must fulfill some fundamental requirements to satisfy free, fair and dependable democratic decision making. According to [13,1] these requirements can be classified into functional and security requirements. Reviewing these requirements as they affect e-voting system, the important factors are:

Authentication: Only the authorized and certified electorates can cast vote.

Integrity: Ensure that the system cannot be re-configured during operation and ensure that each vote is recorded as intended and cannot be tampered with in any manner, once recorded.

Confidentiality: No one should be able to determine how any individual voted or make unauthorized disclosure.

Non-Coercibility: Voters should not be able to prove to others how they voted (which would facilitate vote selling or coercion).

Non-Repudiation: Ensure that votes can be verified against each voter.

Simplicity: The system shall be designed to be extremely simple, as complexity is the enemy of security.

Accuracy: The system shall record and count all the votes and shall do so correctly.

Convenience: The system shall allow the voters to cast their votes quickly, in one session, and should not require many special skills or intimidate the voter (to ensure Equality of Access to Voters).

Flexibility: The system shall be flexible in that it allows a variety of ballot question formats including open-ended questions.

Uniqueness: No voter should be able to vote more than once.

Auditability: It should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records, in terms of physical, permanent audit trail (which should not reveal the user's identity in any manner).

Eligibility: Permits only registered voters to vote only once.

Transparency: Voters should be able to possess a general knowledge and understanding of the voting process.

B. Architecture of Secured Model for E-Voting System

The proposed electronic voting system was developed to allow the general public to vote via a desktop computer, the system is an open-ended type that accommodates both the administrator and the voter. The system architecture is adapted from the 3-layered Organization for the advancement of Structured Information Standards (OASIS): the pre-electoral phase, electoral phase and post-electoral phase as presented in [3]. The architecture is shown in Fig. 1:

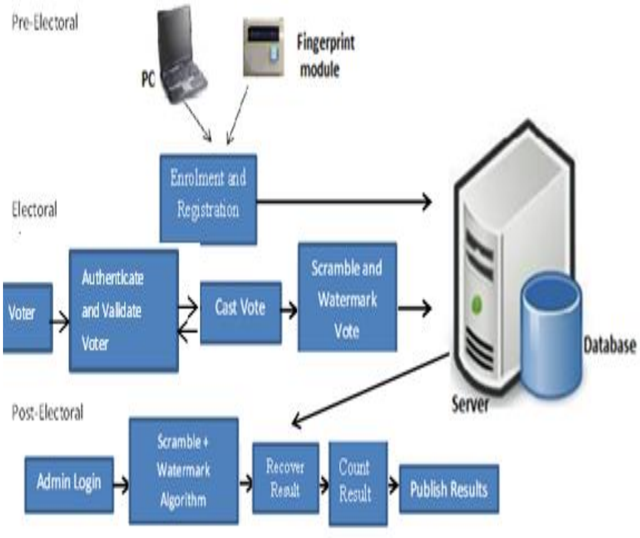


Fig.1. Secure Electronic System Architectural Diagram [14]

In the pre-electoral phase an intending voter fingerprint and personal data are captured and stored into the system. The procedure provides a platform for certified voters to input information and fingerprint registration follows swiftly. The system spontaneously assigns a serial ID to that voter in the system. Voters register in this phase by providing their personal details and fingerprint. Some fields such as surname, first name, and sex are compulsory parameters. After enrolment, a serial PIN is assigned to each user by the system. All registration details are saved in the database. At electoral phase, the voter is granted access into the voting system by

Copyright © 2016 MECS

fingerprint verification, and if valid he/she is allowed to vote. The vote once casted is encrypted with a private key. The encoded vote is embedded into a cover photo which is then directed into the database to be sorted at the post-electoral phase. The final phase is the post-electoral phase where votes casted are verified to satisfy they are unaltered during embedding process. The casted votes are retrieved and sorted, which is published for the electorate.

C. Underlying Voting Technique- Crypto-watermarking

By description, AES cryptographic system preserves assertion of data integrity with the concept of application of private key on the vote, while the wavelet based watermarking allows for confidentiality retention of vote, and any unauthorized modification can easily be tracked; integrity and confidentiality of vote can be assured. The cryptographic encryption algorithm applied to scramble the vote was that of the shared key infrastructure standard. The votes were separated into 128 bit. The Advanced Encryption Standard (AES) employed in this work provided greater “integrity” security as no successful attack have been recorded yet on this algorithm. The cipher generated from the encryption is embedded in the cover object.

D. Pseudocode for scrambling vote

```
Get the vote (V)
Transform the vote to bits
Apply AES to encrypt the vote by using a key $E_g$
Display Cipher vote
```

E. Scrambling Algorithm Formula

$$C = V \times E_g \tag{1}$$

$$V = C \times D_g \tag{2}$$

Where:

C = cipher ; V = vote ; E_g = Encryption key; D_g = Decryption key

The watermarking algorithm was employed to assure the “confidentiality” of the vote. This method is employed using the Haar wavelet and 3-level decomposition was performed on the cover object to improve the image quality and increase the imperceptibility of the watermark to be injected into the cover object.

F. Pseudocode of watermarking Algorithm

Three-level discrete wavelet transform watermarking was implemented on an Host image.

Vote (bit) is encrypted with a key having Mean = 0

G. Decomposition level

Step 1: Get Host image
Step 2: Coding of host image
Step 3: Perform decomposition on host image
Step 4: Coding of approximate host image (LL1)
Step 5: Perform decomposition on LL1
Step 6: Coding of approximate host image (LL2)
Step 7: Perform decomposition on LL2
Step 8: Pick HL3 components

H. Embedding process

Step 1: Read the decomposed Cover photo
Step 2: Convert cover photo to RGB image
Step 3: Read cipher (vote).
Step 4: Using contestant’s photo generate key k
Step 5: Initialize the weight of Watermark (vote)
Step 6: Obtain the filters associated with haar
Step 7: Compute 3-level wavelet transform on cover photo
Step 8: Scramble this watermark by using k.
Step 9: Perform the watermarking in HL3 sub band
Step 10: Display the Watermarked vote

I. Embedding Formula

$$WMI = (OM) * a + (WM) * b \tag{3}$$

WMI = watermarked image; OM= Original image WM = Watermark; a and b= scaling factors of original image and watermark.

J. Embedding Algorithm

These steps were transformed to embedding algorithm as:

```
Input: Cover photo C, Ciphered text T,
Output: Watermarked image W
Let text_len = 0xC0;
            int i;
for (int i=0; i = <text_len(input);i++)
input [i]^ = key;
cipheredtext =  msg.charactAt(i) ^ key
end for
   W = coverphoto + cipheredtext
End
```

K. Extraction process

Step 1: Consider ‘Watermarked vote’ in RGB color-space
Step 2: Consider watermarked image component in HL3 region using DWT transform up to 3 levels to give New_HL3 component.
Step 3: Apply extraction formula
Step 4: Apply De-scrambling algorithm to extract the watermark (vote).

L. Extraction Formula

$$RWM = WMI - LL3 * b \tag{4}$$

RWM = low frequency component approximation of recovered watermark

WMI= low frequency component approximation of watermarked image

LL3 = low frequency component approximation of original image

The extraction algorithm from above procedure thus is:

```
**Input**: Watermarked image W
**Output**: Ciphered Text T
*Begim*
*for i =1 to text_len(W) Do*
*IDWT ()*
*end for*
*Cipheredtext = Watermarkedimage - coverphoto*
End
```

The secured E-voting system architecture from Fig. 1 has unimodal fingerprint biometric system for voter's identity authentication. It comprises of fingerprint sensor, Arduino development board and the voting application software. To solve the "authentication" issue of electronic voting system the fingerprint biometrics was employed, the fingerprint sensor detects the fingerprint impression of the voter and sends signal to the controller unit. Fig. 2 shows the block diagram of authentication module in Fig.1 consisting of fingerprint sensor, database and controller unit. The on-board microcontroller checks the input of the sensor and compare with the stored template, if its matches then sends a signal (+6v) to grant access into the software application system. This process has a 5-25 seconds window gap before the voter cannot try again if the print is not validated. The system disables if no input is detected so as to reduce idle time through which an intruder can exploit.

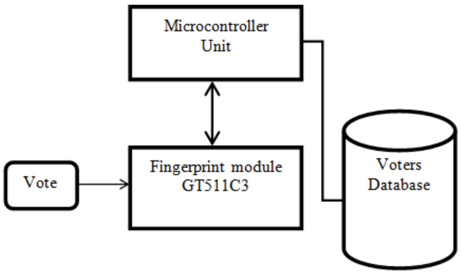


Fig.2. Block Diagram of authentication Module

The microcontroller unit consist ATMEGA 328 Arduino Microcontroller powered through the USB connector. The 5v direct current (DC) that powers the microcontroller unit was regulated to suit the power rating of the on-board ATmega328 (3.3v) chip and fingerprint sensor (3.2v). The regulation of voltage to 5v was achieved by implementing voltage divider theorem (VDR) in the circuit shown in Figure Fig. 3

Using VDR; given Et = 5v, R1 = 1kohm and R2 = 560ohm

$$V = E_t \cdot \frac{R_2}{R_1 + R_2} \qquad (5)$$

$$V = 5 \cdot \frac{1}{1 + 0.56}$$

V = 3.2v

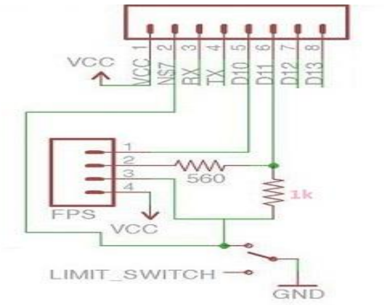


Fig.3. Step-Down Power Supply Circuit

M. System Modeling

Unified Modeling Language (UML) was used to model the e-voting system so as to give better understanding and show process workflow. It uses graphical representation like class diagrams, use-case diagram, and activity diagram to conceptualize the system behavior so as to improve its functionality [3].The use-case diagram of the proposed secure e-voting system is shown in Fig. 4.

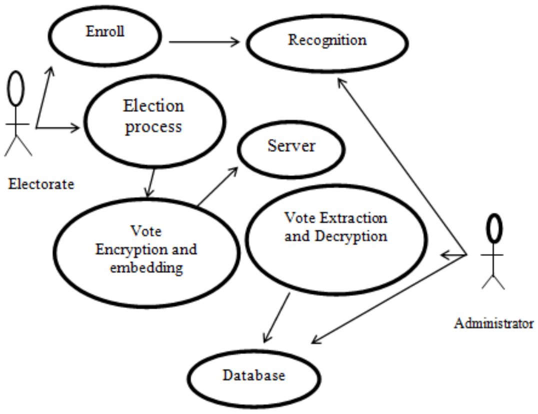


Fig.4. Use Case Diagram of proposed e-voting System

The object type employed in this system and their relationships is described in the class diagram shown in Fig. 5. How all the functions interact and what each actor does are shown in Fig. 5.

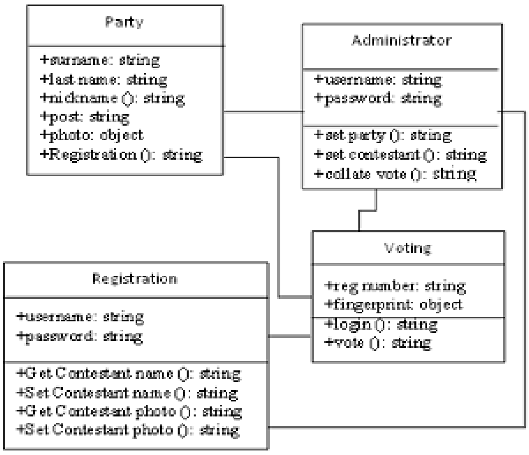


Fig.5. Class Diagram of proposed secure e-voting System

Copyright © 2016 MECS

The system's service like sequence diagram to show how an object in a system interacts; demonstrate the total control flow of the step by step actions and activities that defines an object is shown in Fig.6

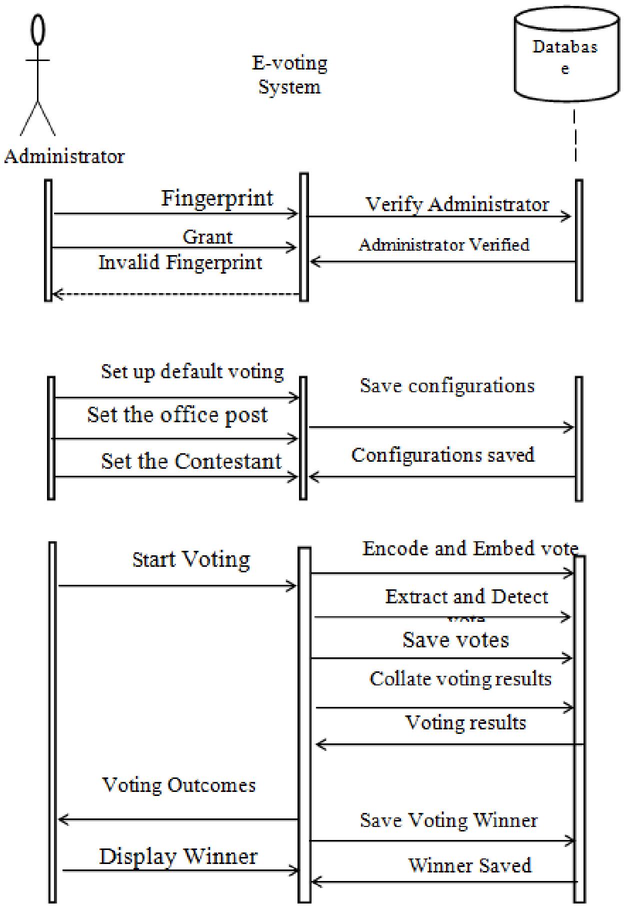


Fig.6. Sequence Diagram of the proposed secure e-voting System

IV. System Implementation

The underlying source code for the voting system was designed using PHP and HTML enabled the deployment of the software on a web platform. The software application permits two main users: the voter and the administrator. The administrator takes care of the entire operation that is carried out; he/she has the sole right to edit voter's information, register voter, set contestant profile, collate, display voting results and validates all voters and contestants. An Arduino based fingerprint module was interfaced with the system to cater for voter's authentication.

A. Authentication Module

The authentication module shown in Fig. 7 is a combination of the fingerprint sensor, Arduino with ATmega328 microcontroller. The interfacing of the system was enabled using a serial USB cable to communicate from the Computer system to the authentication module and vice versa.

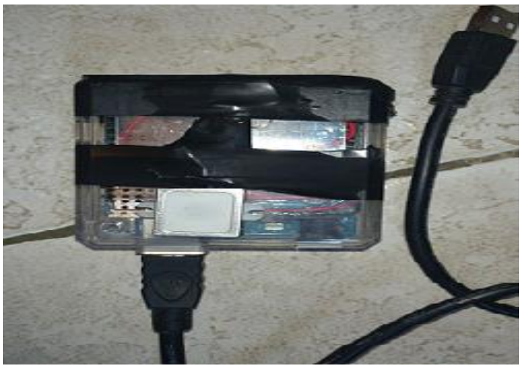
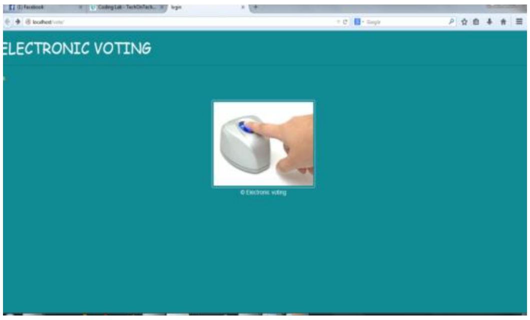


Fig.7. Authentication Module

B. Voting system

The voting interface in Fig. 8 appears to every user at login, requests for valid fingerprints impression on the fingerprint module so as to grant access into the registration or voting menu of the system as the case maybe.

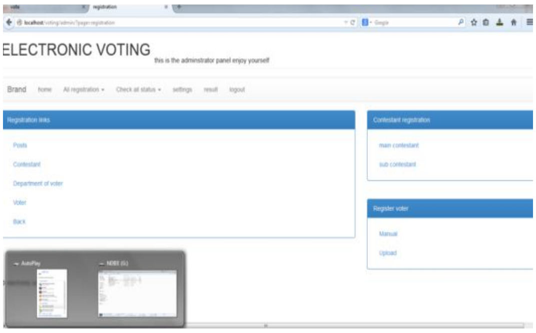


ELECTRONIC VOTING

Fig.8. Home Page of E-voting System

C. Registration Page

The registration interface in Fig. 9 permits voters to input their personal details for verification during voting. The voter fills in a form that contains field for serial number, full name, matric number and voter's department. As case study, the system is prototype around e-democratic decision making in campus scenario. Prospective voters are required to input mandatory matric number field. This field permits voters verification and validation during voting phase. The interface in Fig. 9 permits shows the fingerprint of verified and validated voter.



ELECTRONIC VOTING

this is the adminstrator panel enjoy yourself

Fig.9. Personal Details Registration Page of E-voting System

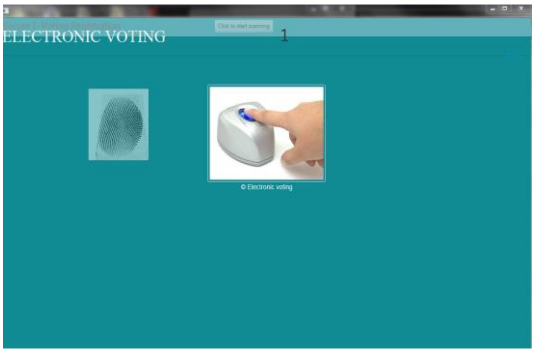


Fig.10. Fingerprint Registration Page of E-voting System

D. *Voting Page*

The voting interface in Fig. 11 provides the electorate an option to elect candidate of choice.

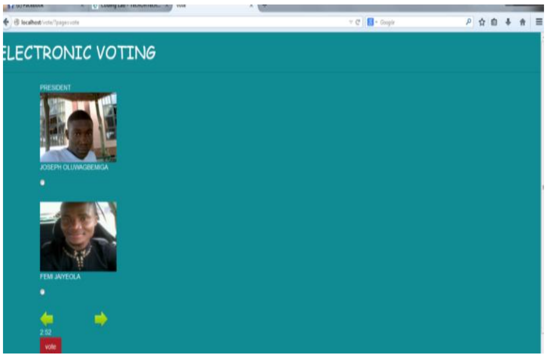


Fig.11. Voting Page of E-voting System

The system overall flowchart is shown in Fig. 12.

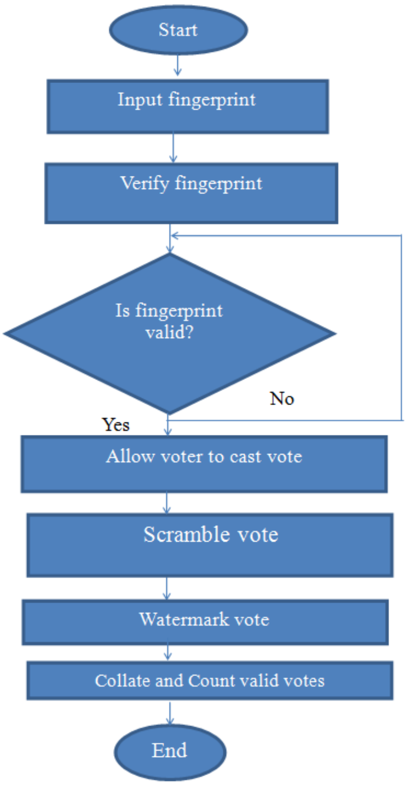
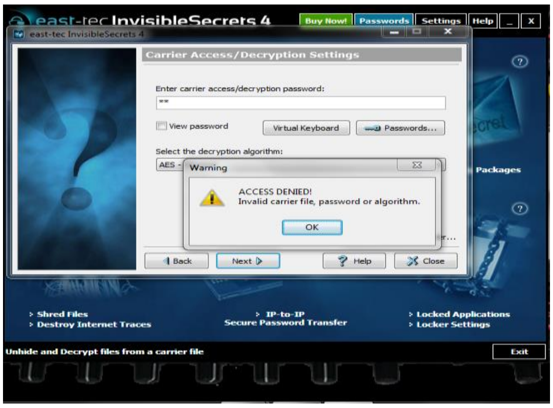


Fig.12. Overall Secure E-Voting System Flowchart

V. System Qualitative Evaluation

The system was evaluated by using an anti-watermarking detection tool to test if there is any structural difference between the original image and watermarked image. An attempt was made to detect the presence of a hidden message in the watermarked object. East-tec invisible secret and invisible ink image processing software were used to confirm if hidden message (vote) is perceptible. From Fig. 13 and Fig. 14, it was observed that Invisible Secrets and Invisible Ink application were not able to decrypt or extract the watermark image. But, Invisible Ink successfully generated a series of cipher that could prove there exist a cipher in the watermarked object but does not correlate with that which was contained inside the carrier.



east-tec InvisibleSecrets 4

Carrier Access/Decryption Settings

Enter carrier access/decryption password: **

□ View password Virtual Keyboard Passwords...

Select the decryption algorithm: AES -

Warning

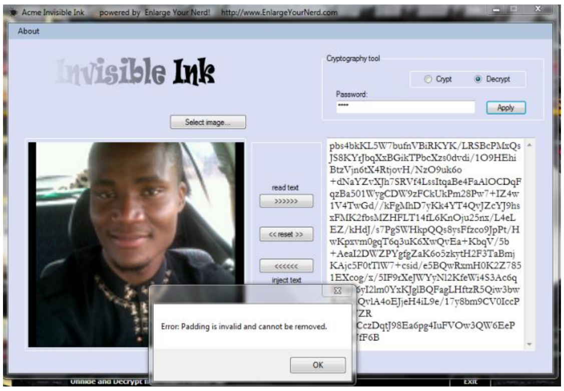
ACCESS DENIED!
Invalid carrier file, password or algorithm.

OK

Back Next Help Close

Unhide and Decrypt files from a carrier file

Fig.13. Attacking the Watermarked Image using Invisible Secrets



Cryptography tool

○ Crypt ● Decrypt

Password: ****

```
pbs4bkKL5W7bufnVBiRKYK/LRSBcPMxQs
JS8KYrJbqXxBGikTPbcXzs0dvdi/1O9HEhi
BtzVjn6tX4RtjovH/NzO9uk6o
+dNaYZvXJh7SRVf4LssItqaBe4FaAlOCDqF
qzBa501WygCDW9zFCkUkPm28Pw7+IZ4w
1V4TwGd//kFgMhD7yKk4YT4QvJZcYJ9hs
xFMK2fbsMZHFLT14fL6KnOju25nx/L4eL
EZ/kHdJ/s7PgSWHkpQQs8ysFfzco9JpPt/H
wKpxvm0gqT6q3uK6XwQvEa+KbqV/5b
+AeaI2DWZPYgfgZaK6o5zkytH2F3TaBmj
KAjc5F0tTlW7+csid/e5BQwRxmH0K2Z785
1EXcog/x/5IF9rXeJWYyNl2KfeWi4S3Ac6q
5yI2lm0YxKJglBQFagLHftzR5Qiw3bw
QvlA4oEJjeH4iL9e/17y8bm9CV0IccP
ZR
CczDqtJ98Ea6pg4IuFVOw3QW6EeP
fF6B
```

Error: Padding is invalid and cannot be removed.

OK

Unhide and Decrypt

Fig.14. Attacking the Watermarked Image using Invisible Ink

VI. Conclusion and Recommendation for Future Work

In this work, a new method for developing secured electronic voting systems have been designed and developed. The system combines fingerprint biometrics for authentication, AES cryptographic algorithm for integrity and wavelet watermarking for solving confidentiality security issues in e-voting. The unimodal fingerprint and AES-wavelet based crypto-watermarking secure electronic voting has been proposed as a secure method for enhancing citizens participation, transparency and trust in e-democratic decision making in future electoral process in developing countries with significant digital divides. The system is superior to other pre-existing methods in its dual layer of security against man in the middle attack or any other security breach mechanisms. In future, the performance of our technique will be quantitatively assessed using Image quality metrics and compared with similar models of secure e-voting systems. Also, a multi-platform authentication parameter will be adopted to enable integration with other electronic systems like tablets and mobile-phones. Consequently the following open issues can be addressed:

a. Exploring a complex multimedia objects such as video and audio for confidentiality in the election process: Video and Audio cover media can provide better payload capacity for improved secure electronic democratic decision making using the concept of crypto-watermarking.
b. Incorporating an audio/visual device to support persons with impaired sight. Future work could incorporate design considerations for disable electorate to exercise their democratic preference.
c. Enhancing the system to solve other security issues like non-repudiation and non-coercibility.: The addressed fundamental e-voting security requirements could be further complemented with post-electoral ballot verification and aversion of vote coercion as well as vote selling prior to voting.
d. Implementing the secure e- voting system based on template-free system to eliminate the threat of compromising the fingerprint template database: Future research could also investigate a template free system for improved model performance.

References

[1] Okediran O. O., Omidiora E. O. Olabiyisi S. O., Ganiyu R. A. and 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.

[2] Howard, M. (2001) E-Government across the globe: How will "e" change government? Government Finance Review, Vol. 17(4), pp. 6-9.

[3] Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. (2012), " Design of A Secured Model For Electronic Voting System Using Stegano-Cryptographic Approach ", Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89

[4] Kohno T., Stubblefield A., Rubin A. and Wallach D. S, (2004), "Analysis of an Electronic Voting System", In Proceedings of IEEE Symposium on Security and Privacy, pp. 1-23.

[5] Sanjay, K.., and Singh, M. (2013). "Design A Secure Electronic Voting System Using Fingerprint Technique" International Journal of Computer Science Issues Vol. 10(4), pp 192-199.

[6] Linu P, and Anilkumar M. N. (2012), "Authentication for Online Voting Using Steganography and Biometrics", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Vol. 5(10), pp. 26-32.

[7] Shafi'í, M, Adebayo, O. S, Damian, O., Mohammed,D. (2013). "The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity, International Journal of Network and Computer Security. MECS (http://www.mecs-press.org/) Vol. 5, pp 9-18

[8] D. Akinmosin D., G.G.O. Egbedokun G.G.O. and Ibitowa F.O (2011),"An Extended Multifactor Authentication in Mobile Financial Transaction Using User Authentication Module with Multilayered Encryption Algorithms", African Journal of Computer and Information Technology ICT (Journal of IEEE Nigeria Computer Section),Vol. 4 (2), pp 17-24.

[9] Gallegos G., Gomez R., and Sanchez G, (2010), "Electronic Voting using Identity Based Cryptography", Fourth International Conference on Digital Society, pp 31-36.

[10] Enokela, J. A. (2010), "Security of Programs and Data for an Electronic Voting System", Pacific Journal of Science and Technology, Vol. 11(2), pp. 283-287.

[11] Gunjal B., and Mali S, (2013). "Secure e-voting system with Biometric and Wavelet Based Watermarking Technique in Ycgcb color space." IEEE International Conference on Information Technology, pp 1-6

[12] Sable, S. and Bombale U. L. (2014), "Cryptography Based Secured E-voting System Using ARM for Cell Phone and Internet Application", International Journal of Computer Engineering and Applications, Vol. 7 (1), pp. 1-6.

[13] Prashanth P., and Swaroop S, (2012), "Requirements for an Electronic Voting System." Department of Computer Science The Johns Hopkins University, pp. 1-2.

[14] Olaniyi, O.M, Folorunso, T. A.,Abdullahi I.M.,Joseph O (2015)," Performance Evaluation of an Enhanced Crypto-Watermarking Model for Secure Electronic Voting ", Open Journal of Information Security and Applications (OJISA),USA, In press Available at: http://www.scipublish.com/journals/ISA/papers/1322

[15] Mohanty S. M. and Bhargava, B. K. (2008). Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP), Vol. 5(2). Pp1-22

Authors' Profiles

Olayemi Mikail Olaniyi is a Senior Lecturer in the Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria. He obtained his B. Tech and M.Sc. in Computer Engineering and Electronic and Computer Engineering respectively. He had his PhD in Computer Security from the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He has published in reputable journals and learned conferences. His areas of research includes: Computer Security, Intelligent Systems, Embedded Systems, Telemedicine and Precision Farming. He can be contacted at mikail.olaniyi@futminna.edu.ng

Folorunso Taliha is an Assistant Lecturer in the Department of Mechatronics Engineering Federal University of Technology Minna. He completed in Bachelor Degree of Engineering in Electrical/Electronics Engineering at the Prestigious Ladoke Akintola University of Technology Ogbomoso Nigeria and proceeded to the famous Universiti Teknologi Malaysia for his Master’s Degree in Mechatronics and Automatic Control Engineering. He has published in reputable journals and learned conferences. His areas of research includes: Control system, systems identification and estimation, Embedded Systems and Precision Agriculture. He can be contacted at funso.taliha@futminna.edu.ng

Aliyu Ahmed had his B. Eng (Electrical and Electronic Engineering) from the Federal University of Technology Minna and his MSc in Computer Networking from the University of Bedfordshire, UK. He is currently a Lecturer II at the Department of Computer Engineering, Federal University of Technology, Minna, Niger state, Nigeria. His areas of research includes: Computer Security, Intelligent Systems, Embedded Systems and Wireless Sensor Networks. He can be contacted at ahmed.aliyu @futminna.edu.ng

Joseph Olugbenga had his Bachelor of Engineering in Computer Engineering from the Department of Computer Engineering, Federal University of Technology, Minna, Niger State, Nigeria in 2014. He is a promising Computer and Network Security Specialist. His areas of research includes: Computer and Network security; Intelligent Systems.

How to cite this paper: Olayemi M. Olaniyi, Taliha A. Folorunso, Aliyu Ahmed, Olugbenga Joseph,"Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.8, No.5, pp.9-17, 2016. DOI: 10.5815/ijieeb.2016.05.02