For Authors (IOSR-JCE)

Governing Board (IOSR-JCE)

Contents (IOSR-JCE)

Downloads

Contact Us

Other Useful Journals

IOSR Journal of Computer Engineering (IOSR-JCE)

IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)

IOSR Journal of Mechanical and Civil Engineering (IOSR-JMCE)

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)

IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)

IOSR Journal of Environmental Science, Toxicology and Food Technology (JESTFT)

IOSR Journal of Humanities and Social Science (IOSR-JHSS)

IOSR Journal of Applied Chemistry (IOSR-JAC)

IOSR Journal of Applied Physics (IOSR-JAP)

IOSR Journal of Mathematics (IOSR-JM)

IOSR Journal of Business and Management (IOSR-JBM)

IOSR Journal of Pharmacy and Biological Sciences (IOSR-JPBS)

IOSR Journal of Dental and Medical Sciences (IOSR-JDMS)

IOSR Journal of Agriculture and veterinary Science (IOSR-JAVS)

IOSR Journal of Nursing and Health Science (IOSR-JNHS)

IOSR Journal of Computer Engineering (IOSR-JCE)

About IOSR-JCE List of Topics Submit an Article Publication Charges

Volume 17 - Issue 6 **Nov. – Dec. 2015**

Version 1 Version 2 Version 3 Version 4 Version 5 Version 6

Citation Abstract Reference Full PDF

Paper Type	:	Research Paper
Title	:	Q-JSON - Reduced JSON schema with high Data Representation Efficiency
Country	:	India
Authors	:	Pratik Tyagi

Citation Abstract Reference Full PDF

Paper Type	:	Research Paper
Title	:	Results for Web Graph Mining Base Recommender System for Query, Image and Social Network using Query Suggestion Algorithm and Heat Diffusion Method
Country	:	India
Authors	:	Asst. Prof. Sonal Patil || Ankush Mahajan

Citation Abstract Reference Full PDF

Paper Type	:	Research Paper
Title	:	Design and Implementation of Thresholding Algorithm based on MFR for Retinal Fundus Images
Country	:	India
Authors	:	S. A. Jameel || Dr. A. R. Mohamed Shanavas

Citation Abstract Reference Full PDF

Paper Type	:	Research Paper
Title	:	Home Automation Using Mobile Communication
Country	:	India
Authors	:	B. SRINIVASA RAO

Citation Abstract Reference Full PDF

Paper Type	:	Research Paper
Title	:	An Indepth Understanding of e-Procurement: A Case Study Approach
Country	:	India
Authors	:	Shaikh Imtiyaj || N.R Biswal || T.P Ray || Dr A.K Hota

IOSR Journal of Research & Method in Education (IOSR-JRME)

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	A Review on Software Fault Detection and Prevention Mechanism in Software Development Activities
Country	:	India
Authors	:	B.Dhanalaxmi || Dr.G.Apparao Naidu || Dr.K.Anuradha

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	A Compound Metric for Identification of Fault Prone Modules
Country	:	India
Authors	:	Ishleen Kaur

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Chaos Encryption and Coding for Image Transmission Over Noisy Channel
Country	:	Egypt
Authors	:	Noha Ramadan || HossamEldin H. Ahmed || Said E. Elkhamy || Fathi E. Abd El-Samie

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	A survey on recommendation system
Country	:	India
Authors	:	Gurpreet singh || Rajdavinder singh boparai

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Automated histopathological image analysis: a review on ROI extraction
Country	:	India
Authors	:	Rupesh Mandal || Mousumi Gupta

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Design of Mobile Robot Navigation system using SLAM and Adaptive Tracking Controller with Particle Swarm Optimization for Indoor Environment Monitoring
Country	:	India
Authors	:	Kapil Jajulwar || Dr.Amol Deshmukh

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Map-Reduce Synchronized and Comparative Queue Capacity Scheduler in Hadoop for Extensive Data
Country	:	India
Authors	:	Sukhmani Goraya || Vikas Khullar

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Data Compression using Multiple Transformation Techniques for Audio Applications.
Country	:	India

Authors	:	Arashpreet Kaur || Rajesh Mehra

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique
Country	:	Nigeria
Authors	:	Olaniyi Olayemi Mikail || Folorunso Taliha Abiodun || Abdullahi Ibrahim Mohammed || Abdulsalam Kayode Abdusalam

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Protocol Payment in M-commerce Transaction
Country	:	Morocco
Authors	:	K. Maazouz || H. Benlahmer || N. Achtaich

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Segmentation of the Blood Vessel and Optic Disc in Retinal Images Using EM Algorithm
Country	:	India
Authors	:	Shabana Mol S || Prof. Deepa Thomas || Dr.Jubilant J Kizhakkethottam

Citation | Abstract | Reference | Full PDF

Paper Type	:	Research Paper
Title	:	Design and Implementation of SOA Enhanced Semantic Information Retrieval web service using Domain Ontology, WCF and .NET Technologies for a Distributed Environment
Country	:	India
Authors	:	S. Meenakshi || Dr. R.M. Suresh

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. V (Nov – Dec. 2015), PP 86-97
www.iosrjournals.org

Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique

Olaniyi Olayemi Mikail[1], Folorunso Taliha Abiodun[2], Abdullahi Ibrahim Mohammed[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)*

Abstract: *Electronic decision making process has been adjudged as an alternative measure to address the flaws of ballot voting system for the delivery of free, fair, confident, credible and transparent elections. Electronic ballot spoofing, remote voter's masquerading, voter's coercibility and ballot integrity breach are some of the security issues in electronic voting system. In this paper, we proffer solution to the problem of authentication and verification of voters as well as the integrity and confidentiality of the casted electronic ballot. The developed e-voting system adopts two levels of security: authentication of voters for whom they are using Radio Frequency Identification Technique and protection of casted votes in transit using enhanced Least Significant Audio Steganographic for credible electronic decision making. The results obtained from the testing and qualitative evaluation using both human psychoacoustic and histogram analysis of the audio cover and stego audio of the system demonstrated an effective level of security from pre-election phase, election phase and post-election phase of the electioneering processes. When electoral processes are exercised with guaranteed security techniques, the electorates can have confidence in the conducted election for improved e-decision system of governance in developing countries with significant digital divide.*

Keywords: *Audio, Confidentiality, e-voting, Integrity, Steganography, Verifiability*

I. Introduction

One of the oldest forms of governance derived from two Latin words: *demo,* 'the people' and *kratein,* 'rule' is democracy [1]. Democracy is a type of governance where citizens are at liberty to choose the way and who governs them by means of election. Naturally, the integrity of electoral process is fundamental to the integrity of democracy [2]. The election system must be fair enough to guarantee credibility which is the ultimate goal of any electoral process.

Ballot system is the traditional voting system where voters cast their votes using ballot papers in view to express their interest for a particular candidate during electoral activities [3]. The result of ballot system of voting are recorded, tabulated and displayed in screen during collation to demonstrate transparency. This traditional method is always associated with several fallacious issues such as privacy-breach, unauthorised vote casting, falsification of results, election interruption, ballot snatching, impersonation and invalid votes [4]. Nevertheless, any voting system designed to effectively and efficiently carry out voting exercise must fulfill some specific criteria with which the system will be evaluated. The voting system must be secure enough to guarantee a secure election, protect votes' integrity and confidentiality to ascertain a free, fair and credible election [5].

These election malpractices in traditional voting have successfully made electorates to lose confidence in voting exercise being practiced. The security of any voting system is usually characterized by the techniques used in handling the casted votes [6]. In modern systems where biometrics were adopted for effective election; it was necessary for voters to enroll their smart cards or fingerprints [7]. The core insecurity issues in e-voting system can be addressed through hardware-software design methodology. In this work Radio Frequency Identification (RFID) technology was used to authenticate and validate electorate to and prove of identity while the developed enhanced Least Significant Bit (LSB) audio Steganographic technique is used for vote confidentiality and control in the design of secure electronic voting system.

Electronic voting system can be described as a referendum conducted by using electronic related equipment in electoral dispensation [8, 9]. The electorates cast their votes, these casted votes are recorded and stored electronically which will further be audited; the result will then be documented and announced by the electoral committee. Advancement in ICT world has penetrated into all facets of live without leaving behind voting system, thereby introducing the use of computer related technologies in voting [10]. The introduction of automation to voting could be a vehicle for fraudulent acts such as electronic ballot spoofing, vote falsification, vote rigging and invalid votes by erring administrators and eavesdroppers [4]. Information security techniques

have improved methods of protecting confidential information from eavesdroppers, hackers, attackers, disclosure, disruption, alteration, modification, perusal, inspection or destruction. In the view of solving the aforementioned security challenges of e-voting, there are specific criteria for e-voting to be adjudged secure. These criteria are authentication, verification, integrity, confidentiality and reliability [1, 4].

Since voting is a critical phase of democratic process, efficiency, effectiveness, reliability and security technologies adopted are of significant importance [4]. In this paper, we present the design and development of a secure electronic voting system using RFID technology and enhanced LSB audio steganographic technique for use in countries where there is significant digital bridge. In these countries, emphases are laid on transparent, trusted, confidence and credible election but the required ICT capacity to drive and provide backbone are inadequate. The designed and developed system mitigates on insecurity issues pervading different phases of electronic voting for efficient and effective information transmission towards the delivery of credible election in e-democracy.

The rest of the paper is organized into five sections: Section II provides rigorous review of related works and perceived gaps from literature; Section III provides system design to mitigate perceived gaps in Section II along system architecture as well as design considerations for both hardware and software subsystems; Section IV provides system development for both designed software and hardware techniques provided in Section III; Section V concludes and provide scope for future research endeavor in the design and development of secure e-voting system.

II. Related Works

There exist several literatures in the delivery of credible e-democracy decision making through secure voting models and systems based on audio steganography and RFID techniques. In [17], authors proposed a system that provided improved robustness and security using Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) for audio steganography. The model adopted an algorithm driven method for embedding message with sequence-mapping technique in the bit of cover-audio. The audio signal and message were read in binary, embedding an image file in it. A random key was generated in 8×8 block for every 16-bit data and store the image in the last 3bits of the audio file. There is low payload capacity of the proposed system as the perceptual transparency was not taken care of and the proposed LSB technique was relatively simple to avert rigorous processing from an eavesdropper.

An online and offline e-voting system implemented on embedded system for real time application was in proposed [8] . E-voting system was classified into two categories namely: Online using internet and offline using voting machine where RFID, facial and vein recognition can be implemented for the authentication of electorates. In the online scenario, a unique identification code was generated to identify individual voter. In offline mode on the other hand, authentication was implemented through facial recognition using Principal Component Analysis (PCA). There is no uniformity in the developed multidimensional voting system as biometrics and smart cards are used for authentication in offline voting while they cannot be implemented in online voting system.

A secure electronic voting system using multifactor authentication and cryptographic hash function was designed and developed in [4]. In [4], voters are registered during the pre-election phase of the electioneering process and casts vote during the election phase of the voting process. Short Message Service (SMS) technique was used for authentication by forwarding a unique identification number to the voter for verification. SHA256 hashing algorithm was used to process the votes where a 256 bit random numbers was generated. Encrypted votes are compared with the hashed votes in case of disparity and hence modification would be detected. Only two security issues were addressed, the authentication and integrity of the e-voting system. Truly secured e-voting system should provide countermeasures for confidentiality and verifiability security issues of electronic ballot during election phase and post-election phase of electioneering process respectively.

Authors in [13] presented a novel high bit rate audio watermarking method that reduces embedding distortion in audio host files. LSB audio steganography robustness was increased through reduction of distortion in LSB coding. A two-step algorithm was used through embedding watermarked bits in into higher LSB layer. The work was carried out in temporal domain having low robustness but high hiding capacity with little distortion on the audio.

In [14], authors carried out an extensive survey on steganographic techniques in real time audio signals and evaluation. General principles of hiding were addressed in audio domain of information hiding describing the major techniques that are being used conventionally. Authors in [9] worked on online voting system powered by biometrics using steganography. Cryptography was used along with steganography combined with biometrics to increase the security level of the system and prevent it from security breach.

Hiding text in audio using multiple LSB steganography and security using cryptography was carried out in [15] demonstrating multilevel security. In [16] steganography was described as the science of hiding the

existence of communication. Different techniques of steganography were discussed as regards the past, the present and the future of steganography. Audio steganography exploits the disadvantage of human auditory system thereby improving perceptual transparency and robustness as well as the payload capacity for better information security in an application area.

In this paper, we improve on the proposition in [4] and [17] by providing countermeasures for confidentiality and verifiability insecurities in[4] as well as providing further enhancement of underlying LSB audio steganographic technique in [17]. This was accomplished through the design and development of an enhanced LSB audio steganographic technique for a secure electronic voting system with RFID authentication and verification technique for voters in e-dispensation of democratic rule where free, fair, credible and confident elections are engendered.

III. System Design

The target of designing any voting system is to develop a system that can reasonably handle threat to at least a particular threshold standard in order to guarantee confident election process. The purpose of the designed system is to produce a proficient solution that caters for the basic functional and non-functional requirement of the system. The requirement specifications produced during system requirement analysis are transformed into a physical architecture through system modelling and database design.

a. Requirements Definition for the Secure E-voting System

The design of any voting system must meet up requirement standards to ensure the actual security of that voting system. According to [4], electronic voting system must satisfy a number of competing criteria for a credible, free and fair election to be assured. The criteria are either functional or non-functional which are further grouped by [6, 10] into generic and system requirement. With respect to these functional and non-functional requirements for e-voting, it can be analysed from the following point of view:

i. **Transparency:** The voters should understand in clear terms, the concept of the adopted voting system specified by the electoral committee prior the day of election. General knowledge of the electoral process would have been clearly stated and clarified in order to avoid confusion. Voters should be able to testify that votes were counted correctly so as to be able to testify to the transparency of the developed system.
ii. **Auditability:** The system should be designed in such a way that it makes provision for mechanism of audit trail. This guarantees and verifies that votes are being counted correctly in the database and hence maintain some level of security.
iii. **Convenience:** Voting process must not be too cumbersome for voters and hence should be able to cast their votes with minimal skill requirement and equipment. The system must be accompanied with a lot of ease for the voters to avoid discouragement.
iv. **Secrecy:** The number of voters voted must not be made known to voters and no one should know who another voter has voted for, not even the administrator
v. **Uniqueness:** The system must have specifications for the age, citizenship and eligibility of the voter in other to be able to vote. The attributes will be used to enforce single citizen single vote (SCSV) mechanism and therefore any vote can vote only but once.
vi. **Authentication:** The identity of all electorates must be verified for who they claim to be. This is the process of avoiding impersonation by imposters for efficient and effective voting process.
vii. **Verifiability:** The election process must be able to be subjected to efficient post-electoral ballot accountability for the establishment of confidence in the electoral officials and e-ballot.
viii. **Integrity:** The vote casted must be secured such that no single vote must be altered, modified, commuted, forged and deleted on transit from the database.
ix. **Confidentiality:** This is the process of ensure the fact that no one read, receive or have any access what so ever to the electronic ballot on transit except the intended recipient(voting administrators)

b. Architecture of Our Secure Model for E-voting System

The electronic voting system was designed kiosk based e-voting scenario peculiar to democratic climate of developing countries. This was primarily meant ensure maximum possible number of electorates cast vote, ensure accessibility and transparency by both the electorates and the administrator respectively. The goal of our system is to solve authentication and verification issues from the voters' point of view at the front end (pre-election phase) of the voting process. Also, the provision of integrity on vote casted after voting (post-election phase).Three distinct layers are adopted as in [4] for the pre-election phase, election phase and the post-election phase of the whole electioneering processes as shown in Figure 1.

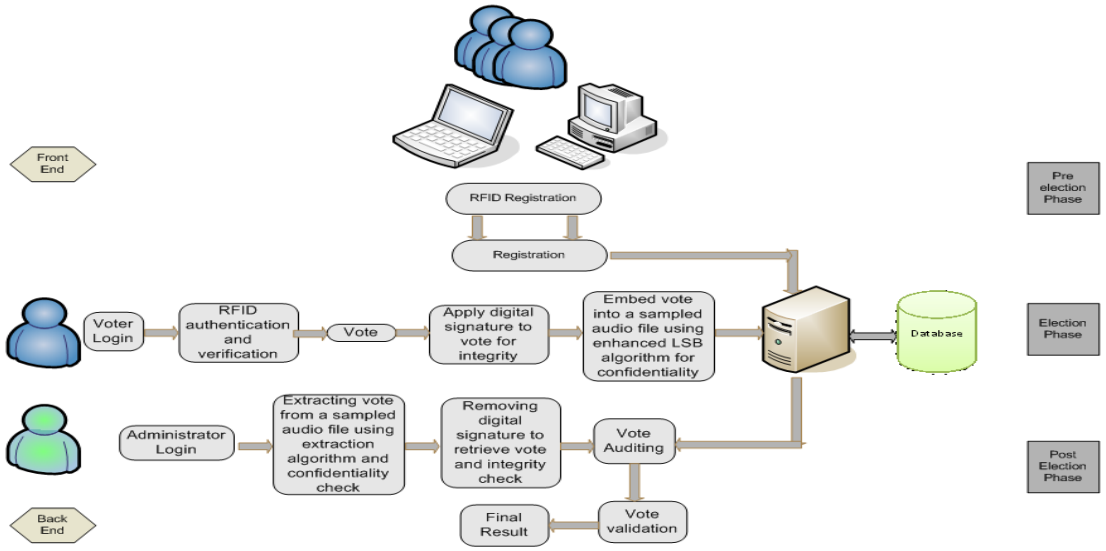


Figure 1: System Architecture of the Secured Electronic Voting System

The pre-election phase is the phase for eligible voters to register their identity that will be authenticated and verified during the execution of the voting phase. In pre-election stage of Figure 1, a unique RFID Tag was assigned to an individual voter to avoid impersonation, ensure transparency and convenience. No two voters will have the same tag for the purpose of achieving uniqueness and secrecy. The voter's information was recorded into the database along with the RFID unique code by the administrator during the registration phase during pre-election phase of the electioneering process. This assigned RFID tag to the voter must be brought to the polling unit before the voter can be licenced to cast his/her vote. The tag is used to gain access to the voting system which demonstrates the fact that 'no RFID card, not vote

In election phase of Figure 1, voters allowed for voting in the election. Only eligible voter is allowed to vote as authentication and verification of identity of voters is required for credible election. The RFID tag assigned to each voter is authenticated with the RFID reader and voter is verified to an eligible voter. After this level, the eligible voter is allowed to vote for desired candidate of whom the vote will now be digitally signed to protect its integrity. Digital signature embedded into the vote and then further embedded into the sampled audio cover file. The designed audio steganographic algorithm is used for this purpose and hence confidentiality is guaranteed. Figure 3.2 shows a pictorial view.

The post-election phase is the final stage, after the ballots have been casted; the vote is recorded and stored in the database for further processing. Here only the administrator can login to the system and query the database using query language. Inverse of the steganographic algorithm is applied and the vote is extracted. Digital signature check and extraction carried out in the database and auditing is done. Votes are validated and results are generated for declaration. This is shown in Figure 3.2.

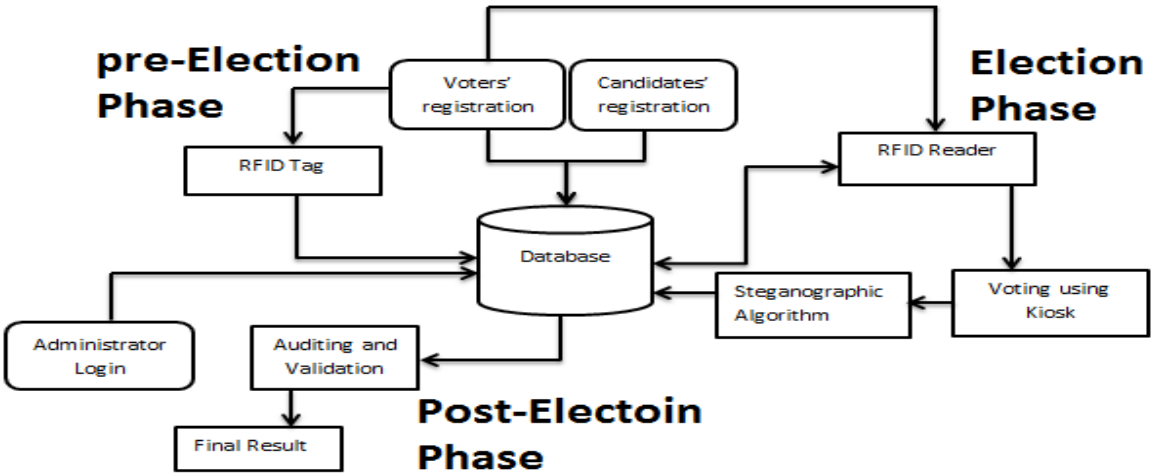


Figure 2: The system block diagram

Hardware design considerations for Voter's RFID Authentication

The major hardware component of the system is the RFID module. This module contains the RFID panel, RFID scanner and RFID tag. RFID is a non-contact technological device that communicates signals through radio wave in order to identify persons or objects. The device has a wide ranges of application amongst which are authentication, identification and tracking of devices and equipment. In most cases, the RFID tag contains a sequence of serial number of a microchip attached to an antenna that is used to identify/track a specific object. RFID transponder is used to describe the microchip and the antenna which work with RFID interrogator/reader [19, 11]. Figures 3, 4, 5 and 6 show the voter's RFID authentication system; the circuit diagram of the RFID scanner; the RFID authentication flowchart and overall RFID hardware module respectively.

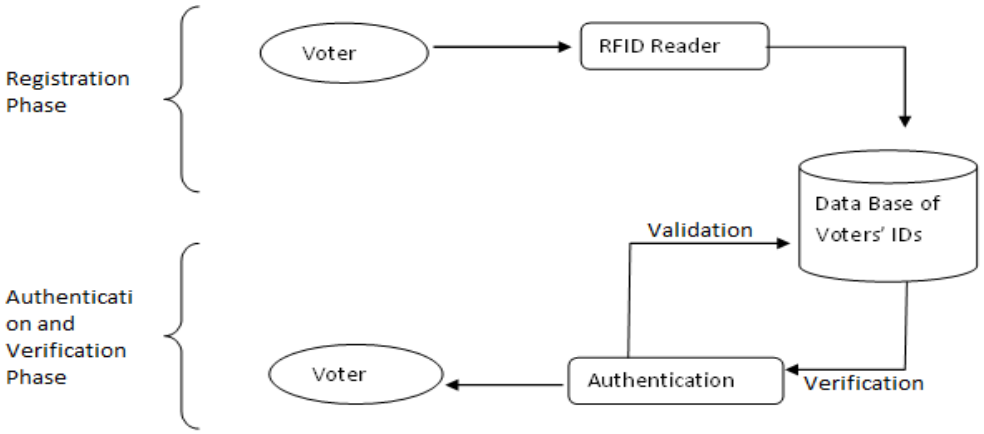


Figure 3: RFID System Architecture

The Voter's authentication Scanner/Reader from Figure 4 is an ID12-LA innovation series of spark fun scanner series. The series has a voltage range 2.8-5volts scanner module that supports ASCII, Wiegabd26 and Magnetic ABA Track2 data formats. It has a reading frequency of 125 KHz and with wide range of tags especially EM4001series

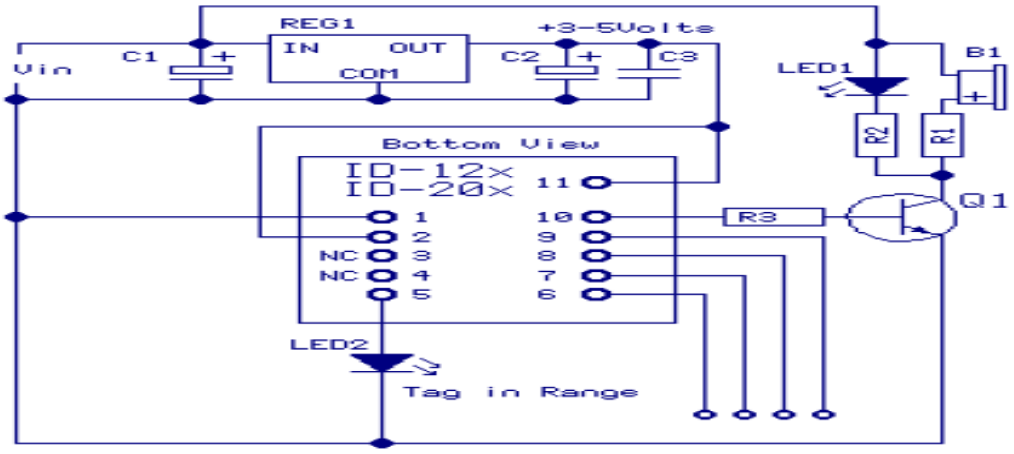


Figure 4: RFID Scanner Circuit Diagram (Source [19])

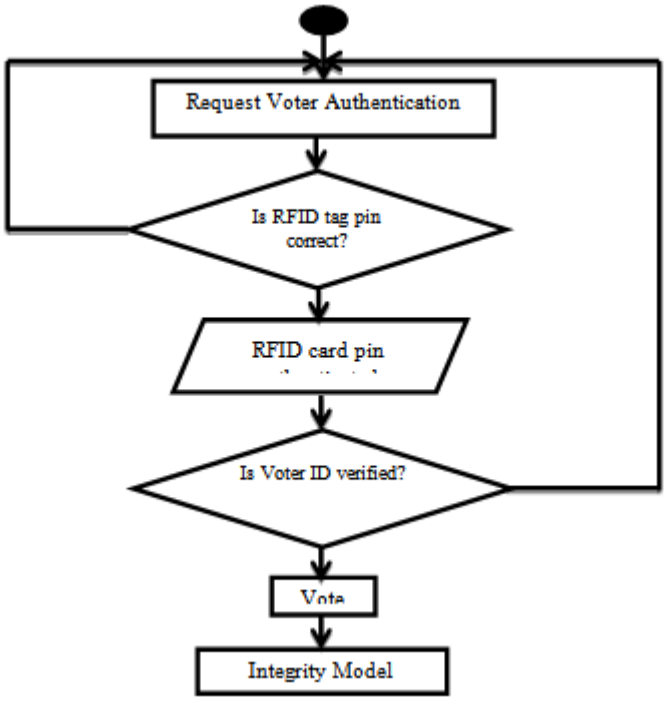


Figure 5: Secure E-voting Election Phase for Voter's Authentication and Verification

Figure 6: RFID authentication and verification hardware module

The study adopted electronic card type for EM4001 series of spark fun scanner/reader. Twenty electronic tags were mapped with selected student information (Name, Matriculation number, level and Department). For the Voters identity authentication RFID tag for six selected students are shown in Figure 7.

Figure 6: Voter's RFID Electronic Tag

c. Software design Consideration

In order to successfully hide information inside an audio file, authors in [18] proposed the following sequence of steps: alteration, modification, verification and reconstruction. An enhanced LSB audio Steganographic technique is adopted by substituting the least significant bits of the sampled audio with the bits of the secret message (voter's choice) envisaged to be hidden. The concept of our enhanced LSB method involves the improvement over the traditional LSB by advancing from the fourth bit of the sampled audio file to the sixth bit of the sampled audio file. The methodology espoused first converts the audio file into streams of bits called samples. Theses samples are divided into frames of audio bit stream and data hiding is eventually carried out.

Using the technique of this enhanced LSB audio Steganography in the election phase of Figure 1, the confidentiality of the casted vote was ensured on transit .To ensure the integrity of the vote on transit MD5 hash function was appended on the vote. The MD5 algorithm produces 128-bit hash value in form of 32-digit hexadecimal value. The idea behind this concept is to take the vote as an input and generate a fixed size hash value as an output. The output value is a fixed, "hash irreversible" value meant to verify vote integrity by the voting administrator.

The vote confidentiality was ensured by sampling and compressing the audio file into binary form of 0s and 1s. The least significant bits are always used for data embedding. In the work, an enhanced LSB method is adopted for the votes to be hidden into the sixth position of the digitized audio sample to unsure enhanced secrecy of information. This improvement was craved upon to guarantee more secure information mechanism over the existing method of hiding digital information into the 2nd and 4th position of audio file. Table 1 shows this mechanism. Figure 7 shows the Steganographic system, where the secret message (vote) and the cover audio are combined through algorithm to form a stego-audio file. The reverse mechanism involves extracting the hidden information using the extraction algorithm..

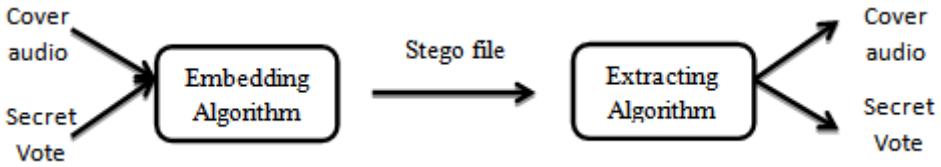


Figure 7: Basic Scheme for Audio Steganographic Process

Table 1: Description of Replaces Bits Positions Using Enhanced LSB technique at sixth position

Sampled Audio Stream (8bit)	Secret Message in Binary	Audio Stream in Encoded Message
10100101	1	10**1**10001
01010010	1	01**1**01010
10010111	0	10**0**01011
10101010	0	10**0**10110
10100011	1	10**1**10011
11001101	1	11**1**00101
01000011	0	01**0**00011
10101011	1	10**1**10111

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

The overall flow sequence of the voting process during election phase of electioneering exercise is shown in Figure 8. Voter authentication and verification of eligibility is achieved using RFID. This is followed by the integrity signature on vote using MD5 algorithm and eventually confidentiality check on signed votes using our enhanced LSB audio steganographic technique.

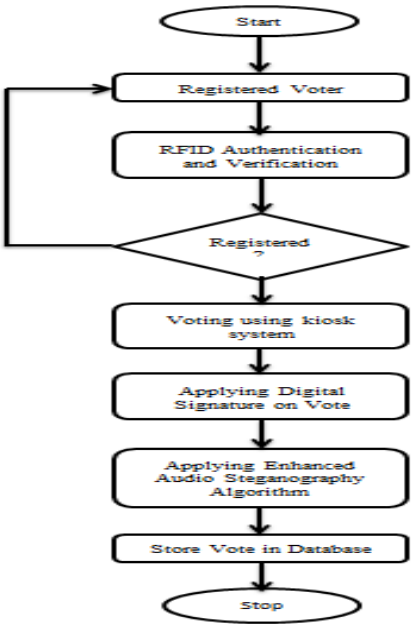


Figure 8: Overall System Flowchart

d. System Modelling

The secure electronic voting system was modelled using Unified Modelling Language (UML) standard. This was envisioned through different UML diagrams such as activity diagram, class diagram, use-case diagram, and sequence diagram. The various functional objects were depicted using the term actor. The use-case to represented goals and as well as the dependencies available is as shown in Figure 9.

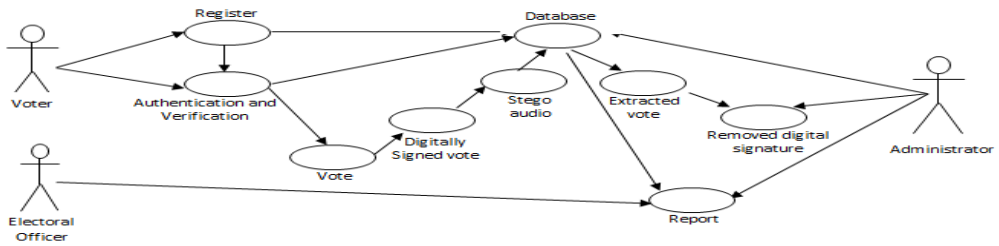


Figure 9: Secure E-voting System Use-Case Diagram

The static relationships between objects and their types are represented in Figure 10 class diagram. Figure 10 depicts interaction between each function of the objects, relationship types that exist between different actors, their functions and the kind of operation they can execute.

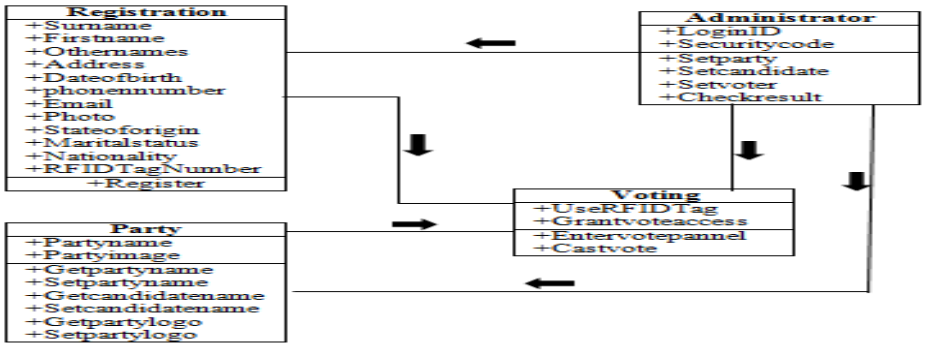


Figure 10: Secure E-voting System Class Diagram

IV. System Development

Both software and hardware design considerations were integrated into a system through appropriate system development with HyperText Markup Language(HTML), Cascading Style Sheet(CSS), Java Programming Language, Javascript, PHP (HyperText Pre-Processor), and SQL (Structured Query Language all integrated in Dreamweaver, MySQL, Apache and Netbeans development environment. There are two main users of the voting system: the electorate and the administrator. The administrator controls all the operations carried out on the secure e-voting system and assign privileges to voter. The administrative user has right to register voter and candidates, assign RFID tag to voters, edit information and check status/result. The administrator can also disqualify voter/candidate if found not worthy of voting or being voted for. The electorate can be registered and hence vote for his/her desired candidate. The following are the secure e-voting system environments:

a. Voter's Authentication

In the pre-election phase, the voters are registered and assigned RFID tags which are matched in the database for unique identification. Each voter must log into the system with his/her RFID tag, this helps to achieve single citizen single vote system. This also prevents voters without tag and unauthorized voters from voting as shown in Figure 11.

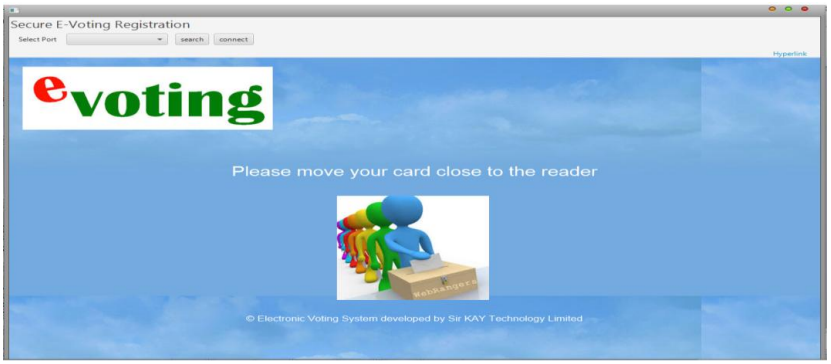


Figure 11: The Authentication and Verification Page using RFID Tag

b. Voting Phase

The login page is only accessible by the administrator in order to control the e-voting system. The page provides an interface to input the security code known only to the administrator and the administrator alone. This is in the view to control the privileges into the system and preventing unauthorized access and privileges. By inputting the passcode, the administrator can manage the entire system. Figure 12 shows the login page for the administrator.

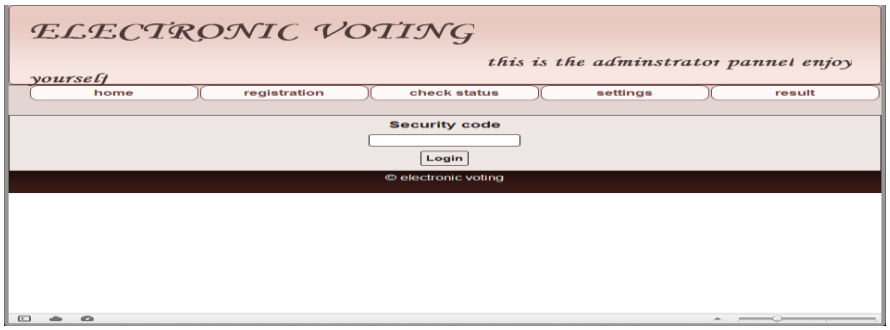
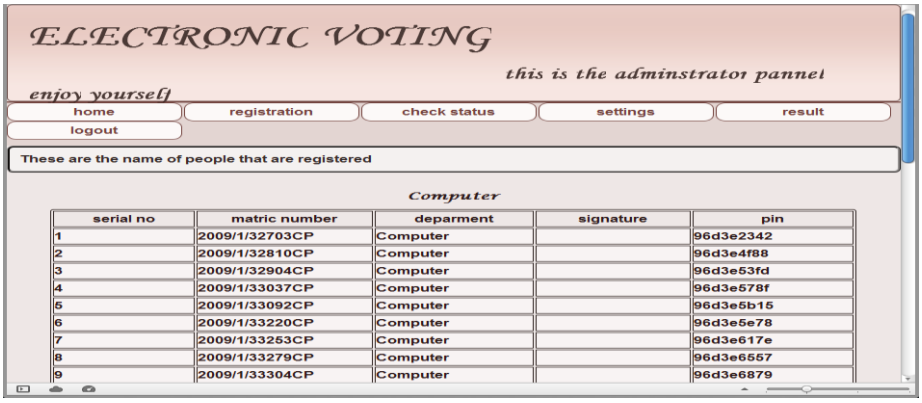


Figure 12: The Login Page for the Administrator

c. Registered Voter's ,Voting and Candidate Environments

This is a view from the database, presenting the list of registered voters in a tabular form of relational database. The administrator can check the list of registered voter, edit the content and eliminate non-eligible voter from the list. Figure 13 represents the pictorial view of the database list of registered voters. The voting environment is the page presented to the voter in order to cast his/her vote for any intended candidate. The pictures of these candidates are also presented along with their respective names so as to make voting exercise easy for the voter. Figure 14 shows the pictorial view of the voting page. The candidate development environment contains the list of registered candidate that can be voted for in the election process. Candidates for various post are displayed in the database for the administrator to manage, cross-check and nullify if found not eligible to be voted for. Figure 15 shows the pictorial view for candidates' page in the database



serial no	matric number	deparment	signature	pin
1	2009/1/32703CP	Computer		96d3e2342
2	2009/1/32810CP	Computer		96d3e4f88
3	2009/1/32904CP	Computer		96d3e53fd
4	2009/1/33037CP	Computer		96d3e578f
5	2009/1/33092CP	Computer		96d3e5b15
6	2009/1/33220CP	Computer		96d3e5e78
7	2009/1/33253CP	Computer		96d3e617e
8	2009/1/33279CP	Computer		96d3e6557
9	2009/1/33304CP	Computer		96d3e6879

Figure 13: Database View of the Registered Voters of Computer Engineering Department

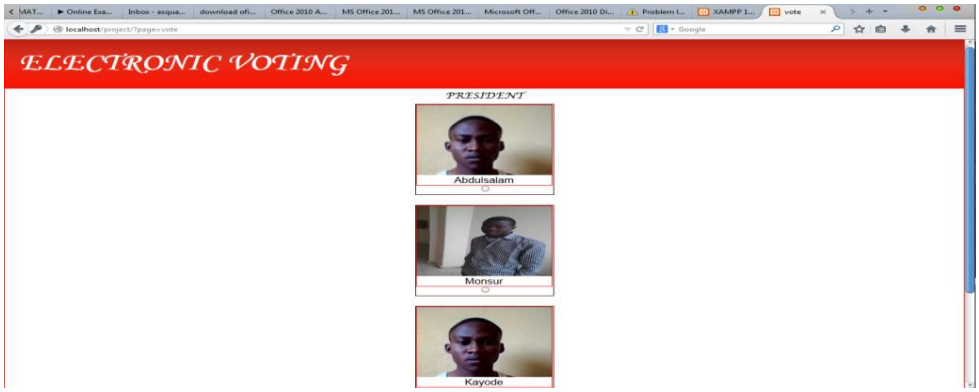


Figure 14: Voting Interface Displayed to the Voter

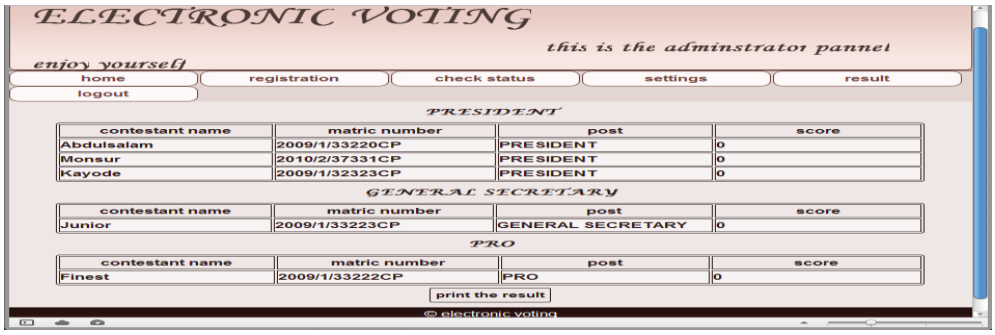


Figure 15: Relational Database View of the Result

V. System Performance Evaluation

The system performance was evaluated both subjectively and objectively. It was evaluated subjectively through perceptual evaluation of audio quality by human psychoacoustic method. The stego audio and cover audio were both subjected to listening ears by various persons and neither was found distorted as it was difficult to identify any irregularities or distortion in any of them. It was realized that the Human Auditory System (HAS) could not detect any variation through their listening ability. The stego audio was also tested using Invisible Secret software to detect any hidden information in the stego audio file but could not identify any thing and rather returned an error message. Figure 16 shows the Invisible Secret software test.

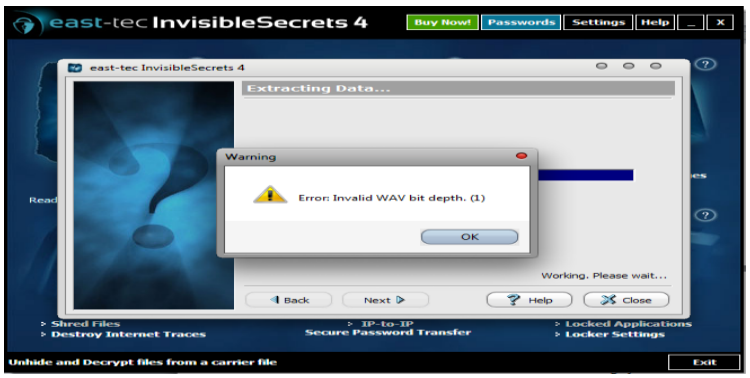


Figure 16: Invisible Secret Test for Hidden Information

Preliminary evaluation with wave audio file on the cover audio and stego audio showed that there was no detectable difference in both audio considering the histogram shown in Figure 17. One of the stego audio file used was sampled and Figure 17 depicts the wave plot of pledge audio file.

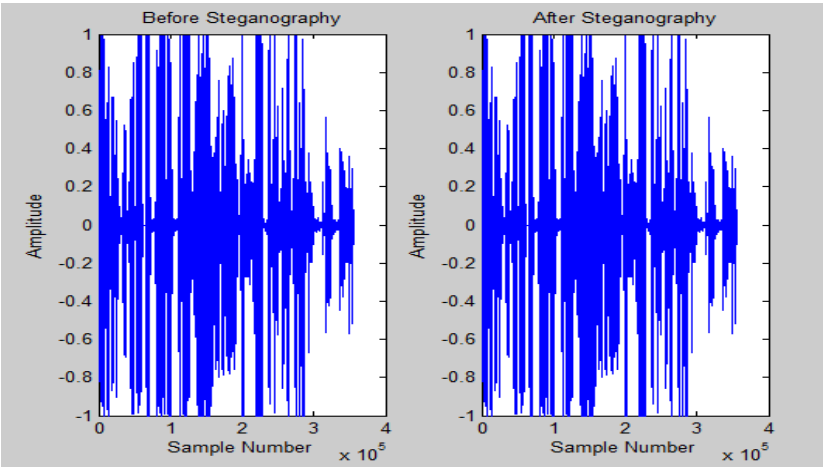


Figure 17: The Wave Plot of Pledge Audio before and after Steganography

VI. Conclusion And Recommendations For Future Work

This paper has successfully presented a secure electronic voting system with countermeasures against authentication, confidentiality and integrity/verifiability fundamental security requirements. The developed

secured voting system was evaluated against the set security goals of developing the system and it was found effective and efficient. The electronic voting system employs computerized equipment over the traditional ballot voting system. Security issues such as authentication and verification of electorates were tackled with RFID technology while integrity check was achieved using cryptographic hash functions. Confidentiality of the system was accomplished using enhanced LSB audio steganographic technique. The system was evaluated using both subjective human psychoacoustic and histogram analysis of the audio cover and stego audio. In future, an extensive quantitative performance evaluation of the enhanced LSB audio Steganographic technique would be carried out using metrics such as: Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and embedding capacity. The technique would also be benchmarked with related techniques in literature.

The following recommendations are suggested for future researchers for further improvement on the developed secured electronic voting system for better e-governance in e-democratic administration:

i. Privacy risks between the RFID tag and Reader could be addressed with appropriate light weight cryptographic techniques.
ii. Audio steganography can also be combined with other security technologies to increase security ability.
iii. Integration of speech processing for visually impaired is also recommended.

References

[1]. Olaniyi O. M., Adewumi D. O., Oluwatosin E. A., Bashorun M. A. and Arulogun O. T. (2011). Framework for Multilingual Mobile E-Voting Service Infrastructure for Democratic Governance. *African Journal for Computer and Information Communication Technology. 4:3(2): 23-32.*

[2]. 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*

[3]. Abdulhamid S. M., Adebayo O. S., Ugiomoh D. S. and 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 For Computer Network and Information Security. 5(5). 9-18.*

[4]. Olaniyi O. M., Arulogun O. T. and Omidiora E. A. (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.*

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

[6]. 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). 72-82*

[7]. Alok K. and Atul K. (2011). A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme. *International Journal of Technology and Engineering System*. *2(1), 8-11.*

[8]. Alaguvel R. and Gnanavel G. (2013). Offline and Online E-Voting System with Embedded Security for Real Time Application. *International Journal of Engineering Research*. *2(2). 76-82.*

[9]. Katiyar S., Meka K. R., Barbhuiya F. A. and Nandi S. (2011). Online Voting System Powered By Biometric Security Using Steganography. *Second International Conference on Emerging Applications of Information Technology*.*IEEE Computer Society:288-291*

[10]. 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*. *1(4). 135-142.*

[11]. Garfinkel S. L., Juels A. and Pappu R. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Computer Society*: *34-43*

[12]. Alaguvel R. and Gnanavel G. (2013). Offline and Online E-Voting System with Embedded Security for Real Time Application. *International Journal of Engineering Research*.

[13]. Cvejic N. and Tapio S. (2003). Increasing Robustness of LSB Audio Steganography by Reduced Distortion LSB Coding. *MediaTeam, Information Processing Laboratory, University of Oulu, Finland*.

[14]. Al-Othmani A. Z., Abdul Manaf A. and Zeki A. M. (2012). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation. *International Journal of Computer Science Issues. 9(1).30-37*

[15]. Divya S. S., Ram M. (2012). Hiding Text In Audio Using Multiple Lsb Steganography And Provide Security Using Cryptography. *International Journal Of Scientific & Technology Research 1(6): 68-70.*

[16]. Amirtharajan R. and Rayappan J. B. B. (2013). Steganography-Time to Time: A Review. Reseearch Journal of Information Technology. *5(2). 53-66.*

[17]. Gupta N. and Sharma N. (2013). Hiding Image in Audio using DWT and LSB. *International Journal of Computer Applications 81(2).1-14*

[18]. 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). 62-65.*

[19]. Sparkfun (2015).RFID starter Kit Retreived online at https://www.sparkfun.com/products/13198 on 14th January,2015.